Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

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

Nr. 3 **MEMORIE VAN TOELICHTING**

INHOUDSOPGAVE MEMORIE VAN TOELICHTING **blz.**

kst-34372-3
ISSN 0921 - 7371
's-Gravenhage 2015

I ALGEMEEN DEEL

1. Inleiding

Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te versterken en vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer alsmede van het in het regeerakkoord van het kabinet-Rutte-Asscher. Het wetsvoorstel sluit aan bij de snelle ontwikkelingen van de technologie, het internet en computercriminaliteit en zet de lijn voort die is ingezet met de Wet computercriminaliteit (inwerkingtreding 1 maart 1993) en de Wet computercriminaliteit II (inwerkingtreding 1 september 2006). Daarmee zijn voor de bestrijding van computercriminaliteit wijzigingen aangebracht in het Wetboek van Strafvordering en het Wetboek van Strafrecht. Met de Wet computercriminaliteit II is het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290), ook bekend als het Cybercrime Verdrag, geïmplementeerd.

Dit wetsvoorstel vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer. Bij brief van 23 december 2011 (Kamerstukken II 2011/12, 26 643, nr. 220) is de Tweede Kamer conform de toezegging in het algemeen overleg met de Tweede Kamer over nationale veiligheid van 1 juni 2011 (Kamerstukken II 2010/11, 28 684, nr. 323) geïnformeerd over een juridisch kader voor cybersecurity en de juridische knelpunten. In vervolg hierop heb ik de Tweede Kamer bij brief van 15 oktober 2012

(Kamerstukken II 2012/13, 28 684, nr. 363) geïnformeerd over voorstellen om, binnen de kaders van de rechtsstaat en de vereisten van proportionaliteit en subsidiariteit, een aantal onderwerpen in wetgeving uit te werken om daarmee de bevoegdheden op het gebied van de opsporing en de vervolging van computercriminaliteit te versterken. Voorts wordt met dit wetsvoorstel invulling gegeven aan het in het regeerakkoord (Bruggen slaan, Regeerakkoord VVD–PvdA, 29 oktober 2012, blz. 28) opgenomen voornemen om de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. Daartoe wordt voorgesteld te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen.

Dit wetsvoorstel bevat voorstellen tot wijziging van het Wetboek van Strafvordering (Sv) en het Wetboek van Strafrecht (Sr). In de eerste plaats wordt voorgesteld een nieuwe bevoegdheid voor de daartoe aangewezen opsporingsambtenaren te creëren om onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Deze doelen betreffen de uitoefening van reeds bestaande bevoegdheden. Voor de uitoefening daarvan is het heimelijk binnendringen in geautomatiseerd werk noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens. Daarbij kan de beveiliging worden doorbroken of kunnen technische handelingen worden verricht om toegang te verschaffen tot het geautomatiseerde werk. Ook kan heimelijk software worden geïnstalleerd met behulp waarvan op specifieke punten de beveiliging wordt doorbroken of omzeild en waarmee de versleuteling van gegevens ongedaan kan worden gemaakt. Deze bevoegdheid kan onder omstandigheden ook worden toegepast ten aanzien van gegevens die zich wellicht niet op het Nederlandse grondgebied bevinden, terwijl de gevolgen van het strafbare feit zich in Nederland voordoen. Indien duidelijk is in welk land het geautomatiseerd werk zich bevindt, is rechtshulp – behoudens uitzonderlijke omstandigheden – aangewezen. Tevens wordt voorgesteld de omschrijving van het begrip «geautomatiseerd werk» te verruimen.

In de tweede plaats wordt voorgesteld om de regeling van de bevoegdheid van de officier van justitie om, met machtiging van de rechter-commissaris om, te bevelen dat gegevens op internet ontoegankelijk worden gemaakt, aan te passen. Deze bevoegdheid is thans geregeld in het Wetboek van Strafrecht (artikel 54a Sr). De voorgestelde aanpassing heeft ten doel te komen tot een betere toepassing van de bestaande regeling, zodat de samenleving beter kan worden beschermd tegen strafbare feiten die op internet worden begaan. Verruiming van het toepassingsbereik van de bestaande bevoegdheid tot het ontoegankelijk maken van gegevens wordt niet beoogd. Dit betreft een aangepast voorstel op basis van een voorstel tot herziening van de regeling van het ontoegankelijk maken van gegevens, dat eerder in consultatie is gegeven.

In de derde plaats wordt voorgesteld het wederrechtelijk overnemen van gegevens en het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens strafbaar te stellen. Daardoor worden gedragingen strafbaar die kunnen worden beschouwd als «heling» van gegevens. Hiermee wordt in een betere strafrechtelijke bescherming van computergegevens voorzien. Ook dit betreft een aangepast voorstel op basis van een voorstel tot strafbaarstelling van heling van gegevens, dat eerder in consultatie is gegeven.

In de vierde plaats wordt voorgesteld de strafbaarstelling van het verleiden van minderjarigen tot ontucht en «grooming» (artikelen 248a en 248e Sr) te verruimen. Met de term grooming wordt gedoeld op het ongewenst benaderen van kinderen op het internet, bijvoorbeeld in chatrooms, met het oogmerk om ontuchtige handelingen met hen te plegen. Om deze maatschappelijk zeer schadelijke verschijnselen beter te kunnen bestrijden is het wenselijk opsporingsambtenaren in te zetten («lokpubers») die zich als minderjarige voordoen.

In de vijfde plaats wordt voorgesteld de zogenaamde online handelsfraude strafbaar te stellen. Met deze term wordt gedoeld op het via het internet aanbieden van goederen of diensten, zonder de intentie die goederen of diensten te leveren, zodat de kopers worden gedupeerd. Zodra de koper merkt dat hij is bedrogen is de website doorgaans uit de lucht gehaald en is de verkoper niet meer te achterhalen. Hiermee wordt de mogelijkheid geboden strafrechtelijk op te treden tegen personen die een beroep of gewoonte maken van het aanbieden van goederen of diensten op het internet, zonder de intentie om die goederen of diensten daadwerkelijk te leveren.

Ten slotte zijn in dit wetsvoorstel enkele wijzigingen van meer technische aard opgenomen, waarmee eerdere omissies worden hersteld.

Het oorspronkelijke conceptwetsvoorstel is in consultatie gegeven aan het College van procureurs-generaal, de korpschef van de politie, de Raad voor de rechtspraak (Rvdr), de Nederlandse Vereniging voor Rechtspraak (NVvR), de Nederlandse Orde van Advocaten (NOvA), het College bescherming persoonsgegevens (Cbp) en Bits of Freedom (BoF)[1]. Tevens heeft een internetconsultatie plaatsgevonden. In een later stadium zijn de voorstellen rond de strafbaarheid van grooming en verleiding van minderjarigen tot ontucht en van de online handelsfraude aan het oorspronkelijke conceptwetsvoorstel toegevoegd. Over deze voorstellen is afzonderlijk advies gevraagd van het College van procureurs-generaal, de korpschef van de politie, Rvdr, de NVvR, de NOvA en het Cbp[2].

Het College van procureurs-generaal heeft met grote instemming kennis genomen van het voornemen om heling van gegevens strafbaar te tellen en van het voorstel om een bevoegdheid te creëren voor opsporingsambtenaren om heimelijk op afstand een geautomatiseerd werk binnen te kunnen dringen ten behoeve van de opsporing van ernstige strafbare feiten. Het College kan zich grotendeels vinden in het beoogde doel van de voorgestelde wijzigingen rond de strafbaarheid van grooming en verleiding van minderjarigen tot ontucht en van de online handelsfraude.

De Rvdr stelt vast dat de inzet van de voorgestelde opsporingsbevoegdheden een vergaande inbreuk op de grondrechten van burgers kan opleveren. Het is van groot belang dat een dergelijke inbreuk zo beperkt mogelijk wordt gehouden en dat de burger wordt beschermd tegen willekeurige inmenging door de overheid in zijn privéleven. De Raad acht de keuze dat deze bevoegdheden slechts kunnen worden toegepast na een schriftelijke machtiging door de rechter-commissaris wenselijk en verstandig. Wat betreft de online handelsfraude adviseert de Rvdr de nieuwe strafbaarstelling te heroverwegen, vanwege de stand van de jurisprudentie rond de oplichting door middel van het internet.

---

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

De korpschef van de politie is verheugd met dit wetsvoorstel. De wet wordt daarmee aangepast aan de eisen van deze tijd. De toenemende omvang en ernst van computercriminaliteit, en high tech crime in het bijzonder, noodzaakt tot aanpassing van de wet.

De NVvR stelt vast dat de voortschrijdende technologische ontwikkelingen en de daarmee samenhangende ontwikkeling van de mogelijke vormen van criminaliteit maken dat de reeds bestaande bevoegdheden van politie en justitie soms tekort schieten. De NVvR is van mening dat de inbreuk op de grondrechten, die uit het wetsvoorstel kan voortvloeien, zo beperkt mogelijk moet worden gehouden. De voorgestelde eis van een schriftelijke voorafgaande machtiging van de rechter-commissaris vormt volgens de NVvR een voldoende waarborg voor zorgvuldig gebruik van de ingrijpende bevoegdheden. De NVvR meent dat met de voorgestelde wetwijziging voor wat betreft de strafbaarheid van grooming en verleiding van minderjarigen tot ontucht ook de intentie strafbaar wordt gesteld en adviseert deze wijziging niet door te voeren.

De NOvA heeft fundamentele bezwaren tegen de invoering van de bevoegdheid om heimelijk op afstand in een geautomatiseerd werk binnen de kunnen dringen en het voorgestelde decryptiebevel aan de verdachte. Met betrekking tot de invoering van de nieuwe bevoegdheden van het ontoegankelijk maken van gegevens en de strafbaarstelling van het overnemen en de heling van gegevens stelt de NOvA concrete wijzigingen voor. De NOvA stelt vast dat in het wetsvoorstel zonder voldoende grond of doordenking zeer vergaande en zeer ingrijpende bevoegdheden in het leven worden geroepen, en maakt zich zorgen over de kritiekloze houding die de toenmalige Minister van Veiligheid en Justitie ten aanzien van de digitalisering van de opsporing zou innemen. De verregaande digitalisering van het leven van burgers vraagt volgens de NOvA niet om uitbreiding van het strafrecht maar juist om terughoudendheid en zorgvuldiger proportionaliteitsafwegingen dan in het voorliggende wetsvoorstel zichtbaar zijn gemaakt. De NOvA maakt bezwaar tegen de aanpassing van het materiele strafrecht om de inzet van een zogenaamde lokpuber mogelijk te maken bij de bestrijding van grooming.

Het Cbp heeft zijn advies beperkt tot de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk. Het Cbp is van oordeel dat het ingrijpende karakter van de voorgestelde bevoegdheid en de uitgebreide kring van personen die de inzet ervan kan betreffen, hierbij onvoldoende zijn onderkend. De overwegingen worden in belangrijke mate gebaseerd op een aantal concrete situaties dat de invoering van de beoogde bevoegdheid op zichzelf onvoldoende kan rechtvaardigen. De dringende noodzaak als bedoeld in artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) behoeft daarnaast ook een zelfstandige beschouwing en onderbouwing. Gelet hierop adviseert het Cbp om bij de gronden en afwegingen die de noodzaak van aanpassing van de huidige wettelijke bepalingen moeten onderbouwen, nadere aandacht te besteden aan de door artikel 8 EVRM gestelde voorwaarden.

De voorstellen zijn voor BoF onacceptabel. Ten aanzien van het onderzoek van een geautomatiseerd werk en het decryptiebevel aan de verdachte zijn de bezwaren zo fundamenteel van aard dat deze voorstellen in hun geheel moeten worden afgewezen. De bezwaren tegen de andere voorstellen zijn zodanig dat deze op essentiële onderdelen moeten worden herzien.

Het conceptwetsvoorstel is voor advies voorgelegd aan de Afdeling advisering van de Raad van State (hierna ook te noemen: Afdeling advisering). Naar aanleiding van het advies van de Afdeling advisering is het voorstel voor het decryptiebevel aan de verdachte geschrapt (dit betrof de artikelen I, onderdeel G en II, onderdelen D en M, van het oorspronkelijke conceptwetsvoorstel dat in consultatie is gegeven). Tevens is de voorgestelde bevoegdheid van een mondelinge vordering van gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker geschrapt (artikel II, onderdelen G en I, van het oorspronkelijke conceptwetsvoorstel dat in consultatie is gegeven). Ditzelfde geldt door de voorgestelde bevoegdheid van een mondelinge vordering ter zake van de zogenaamde NAW-gegevens (naam, adres, woonplaats) van een gebruiker van een communicatiedienst (artikel II, onderdelen H en J, van het oorspronkelijke conceptwetsvoorstel dat in consultatie is gegeven). De voorstellen met betrekking tot de mondelinge vorderingen zijn overgeheveld naar het voorstel van wet tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering in verband met de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare telecommunicatiediensten.

De opbouw van de memorie van toelichting is als volgt. In hoofdstuk 2 komt de bevoegdheid om een geautomatiseerd werk op afstand heimelijk binnen te dringen met het oog op bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten aan de orde. Dit betreft de voorgestelde nieuwe artikelen 126nba, 126uba en 126zpa Sv (artikel II, onderdelen G, L en Q) en de voorgestelde wijziging van artikel 80sexies Sr (artikel I, onderdeel B). In hoofdstuk 3 wordt ingegaan op de aanpassing van de bevoegdheid tot het geven van een bevel aan de aanbieder van een communicatiedienst tot het ontoegankelijk maken van bepaalde gegevens die worden opgeslagen of doorgegeven. Dit betreft de voorgestelde wijziging van artikel 54a Sr (artikel I, onderdeel A) en het voorgestelde nieuwe artikel 125p Sv (artikel II, onderdeel D). In hoofdstuk 4 wordt de strafbaarstelling van het wederrechtelijk overnemen van gegevens en het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens behandeld. Dit betreft het voorgestelde nieuwe artikel 138c Sr (artikel I, onderdeel C) en artikel 139g Sr (artikel I, onderdeel E). Hoofdstuk 5 is gewijd aan het voorstel tot verruiming van de strafbaarstelling van het verleiden van minderjarigen tot ontucht en «grooming» (artikel I, onderdelen F en G). In Hoofdstuk 6 wordt het voorstel tot strafbaarstelling van de online handelsfraude toegelicht (artikel I, onderdeel I). Hoofdstuk 7 bevat de financiële paragraaf. In hoofdstuk 8 volgt de behandeling van de adviezen. Deel II bevat de artikelsgewijze toelichting.

2. Onderzoek in een geautomatiseerd werk

2.1. De noodzaak van de voorgestelde bevoegdheid

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

noodzakelijk is geworden, vanwege de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

Het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen wordt in deze memorie van toelichting aangeduid als: onderzoek in een geautomatiseerd werk. Het onderzoek bestaat uit verschillende onderdelen die hieronder, in onderdeel 2.5, nader worden toegelicht. Het eerste onderdeel betreft het binnendringen van het geautomatiseerde werk. Dit onderdeel omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel (met behulp waarvan gegevens kunnen worden vastgelegd). Dit onderdeel wordt hierna ook aangeduid als: binnendringen. Het tweede onderdeel betreft het verrichten van bepaalde handelingen in het geautomatiseerde werk waarin is binnengedrongen. Als dit onderdeel wordt bedoeld, dan wordt dit omschreven als: het verrichten van onderzoekshandelingen.

Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. Via een verbinding, zoals een intern netwerk, het internet of een Wi-Fi-verbinding, kan op afstand toegang worden verkregen tot een geautomatiseerd werk. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) beschikken reeds over een dergelijke bevoegdheid voor de uitvoering van hun wettelijke taak. Op grond van de WIV 2002 zijn de diensten bevoegd tot het binnendringen in een geautomatiseerd werk. Daarbij zijn de diensten bevoegd tot het doorbreken van een beveiliging, tot het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens ongedaan te maken en tot het overnemen van opgeslagen of verwerkte gegevens (artikel 24 WIV 2002). Enkele andere Europese landen, zoals België, Duitsland en Frankrijk, kennen een wettelijke regeling voor het heimelijk doorzoeken van informatiesystemen ten behoeve van de opsporing van strafbare feiten. De wettelijke regelingen van deze landen worden in paragraaf 2.7 nader toegelicht.

De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een leemte in de bestaande wettelijke bevoegdheden. Met de introductie van de bestaande wettelijke bevoegdheden in de Wet computercriminaliteit (Stb. 1993, 33), de Wet computercriminaliteit II (Stb. 2006, 300) en de Wet bevoegdheden vorderen gegevens (Stb. 2005, 390) zijn destijds specifieke bevoegdheden opgenomen in het Wetboek van Strafvordering, ter bestrijding van computercriminaliteit en andere delicten die met behulp van computers worden gepleegd. Computercriminaliteit kan worden omschreven als het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk. De bestaande opsporingsbevoegdheden schieten echter in toenemende mate tekort om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen. Deze ontwikkelingen kunnen als volgt worden geschetst:

1. De versleuteling van elektronische gegevens
De versleuteling (of: encryptie) van elektronische gegevens vormt in toenemende mate een probleem voor de opsporing van strafbare feiten. Bij versleuteling worden leesbare data omgevormd in onleesbaar materiaal door middel van een wiskundig algoritme. Op internet worden speciale programma's aangeboden voor het versleutelen van gegevens-

bestanden. Het versleutelen van gegevensbestanden vereist steeds minder technische kennis. Het programma TrueCript vormt hiervan een goed voorbeeld. Dit betreft een gratis, open source-programma waarmee onder andere containers op de harde schijf worden aangemaakt, waarin een grote hoeveelheid bestanden versleuteld kunnen worden opgeslagen. Ook kan de harde schijf volledig worden versleuteld. Daarnaast zijn informatiesystemen en software dikwijls standaard ingesteld op versleutelde vormen van communicatie. Deze standaardinstellingen worden door de gebruikers vrijwel nooit gewijzigd, waardoor zij – dikwijls zonder dat zelf te weten of na te streven – steeds beter zijn beveiligd tegen het aftappen en opnemen van hun communicatie. Diensten als Gmail en Twitter zijn standaard van versleuteling voorzien en andere populaire diensten zoals Facebook en Hotmail bieden versleuteling als optie aan. Bepaalde smartphones versleutelen standaard de communicatie van de gebruiker (Justitiële verkenningen 3/12 (WODC), Tappen en infiltreren, blz. 29). Ook de communicatie die via het internet verloopt kan eenvoudig worden versleuteld. Voorbeelden hiervan zijn de algemeen verkrijgbare communicatiesoftware (bijvoorbeeld Skype, WhatsApp, VPN-diensten) die op computers of smartphones kan worden geïnstalleerd. E-mailverkeer kan worden versleuteld, bijvoorbeeld met de plug-in Pretty Good Privacy (PGP) of soortgelijke toepassingen. Op het internet wordt voorts de mogelijkheid geboden om door middel van bepaalde internetdiensten het transport van gegevens te anonimiseren. Een voorbeeld hiervan is het Tor-netwerk (The Onion Router), dat bestaat uit een wereldwijd netwerk van door vrijwilligers aangeboden servers waarbinnen communicatie versleuteld wordt gerouteerd.

De bestaande bevoegdheden op het gebied van de opsporing van strafbare feiten voorzien niet in de mogelijkheid om de versleuteling van gegevens adequaat het hoofd te bieden. Als het gaat om opgeslagen gegevens dan voorziet de wet in de mogelijkheid van een doorzoeking van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn vastgelegd (artikel 125i Sv). Als gegevens versleuteld zijn dan kan een bevel tot ontsleuteling worden gericht tot degene die kennis draagt van de wijze van versleuteling van de gegevens (artikel 125k, tweede lid, Sv). Ondanks de mogelijkheid van een ontsleutelbevel kan de aanbieder de opgeslagen gegevens meestal niet ontsleutelen omdat de data door tussenliggende diensten zijn versleuteld. De tussenliggende diensten hoeven dikwijls niet aan een tapbevel te voldoen en daarmee ook niet aan de ontsleutelplicht (Justitiële verkenningen 3/12 (WODC), Tappen en infiltreren, blz. 29). Een dergelijk decryptiebevel kan evenmin tot de verdachte worden gericht (artikel 125k, derde lid, Sv). Ook voorziet de wet in de mogelijkheid om gegevens te vorderen van degene van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens. Een dergelijke vordering kan worden gericht tot de aanbieder van een dienst voor de opslag van gegevens (artikel 126ng, tweede lid, Sv). De aanbieder is echter dikwijls in een ander land gevestigd, waardoor hij niet onder de Nederlandse rechtsmacht valt en niet kan worden verplicht aan de vordering te voldoen. Alsdan kunnen de Nederlandse instanties op basis van het Cybercrime Verdrag een rechtsreeks verzoek doen tot het afgeven van gegevens (artikel 32 onder b van het Cybercrime Verdrag). Bovendien, en deze weg wordt meer gekozen, kan een verzoek om rechtshulp worden gedaan. Het Cbp heeft gewezen op de mogelijkheid van een rechtshulpverzoek met betrekking tot e-mails en bestanden die worden opgeslagen op de servers van Google, Skype of Facebook. Het Openbaar Ministerie (OM) doet geregeld rechtshulpverzoeken aan de Verenigde Staten om opgeslagen gegevens van deze bedrijven te verkrijgen. Een dergelijk verzoek dient door de Amerikaanse autoriteiten bij een Amerikaanse rechtbank te worden aangebracht en getoetst, onder andere aan het

vereiste aan de «probable cause». Daarnaast is het op basis van de Amerikaanse privacywetgeving mogelijk dat de in de VS gevestigde aanbieders op basis van een door de Amerikaanse autoriteiten uitgebrachte subpoena die is gebaseerd op een Nederlands verzoek, uit eigen beweging informatie verstrekken. De aanbieders kunnen evenwel besluiten niet te verstrekken, er is geen verplichting tot medewerking. Ook moet worden benadrukt dat een dergelijk verzoek op grond van de Nederlandse wetgeving uitsluitend opgeslagen gegevens kan betreffen terwijl ook behoefte bestaat aan informatie over stromende gegevens (gegevens die worden verwerkt of overgedragen). De door bedrijven als Google en Microsoft tegenwoordig uitgebrachte transparancyreports leveren onvoldoende inzicht op om een goed beeld te vormen van de bereidheid van bedrijven om mee te werken en zijn niet naar herkomst en specifieke juridische basis uitgesplitst. Er is een beperkte kans van slagen bij een verzoek aan een buitenlandse aanbieder tot het verstrekken van informatie over hun klanten en er wordt in ieder geval geen informatie over stromende gegevens verstrekt. Daar komt bij dat het gehele proces veel tijd kost.
Bovendien kunnen criminelen op het internet gemakkelijk hun fysieke locatie versluieren. Het is dan onbekend in welk land, of welke landen, de door criminelen gebruikte geautomatiseerde werken zich bevinden. Het vaststellen van de locatie van een geautomatiseerd werk of verschillende geautomatiseerde werken waar (delen van) gegevens zijn opgeslagen is in theorie mogelijk, maar dit is tijdrovend en gaat gepaard met diverse inbreuken op de persoonlijke levenssfeer.
Op grond van het bovenstaande kan worden geconcludeerd dat de opsporing dringend behoefte heeft aan een mogelijkheid om de sleutels van een encryptieprogramma of encryptiedienst te achterhalen, opdat de versleuteling ongedaan kan worden gemaakt en toegang kan worden verkregen tot de elektronische gegevens ten behoeve van de opsporing van strafbare feiten.

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

betekent dat de communicatie wordt afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden verzonden of nadat deze ontvangen zijn en de communicatie door de software op het geautomatiseerde werk van de ontvanger is ontsleuteld. Daardoor verschuift de oriëntatie van het aftappen van de verbinding, door middel waarvan de communicatie tussen de deelnemers wordt overgedragen, naar het aftappen op de bron of het doel van de communicatie, te weten de computer of de mobiele telefoon met behulp waarvan de communicatie wordt gecommuniceerd («aftappen op het apparaat»).

2. Het gebruik van draadloze netwerken
Draadloze verbindingen zijn in Nederland wijdverbreid beschikbaar. Gedacht kan worden aan het Wi-Fi-netwerk van buurtbewoners of gratis aangeboden onbeveiligde netwerken in restaurants, treinen of hotels (hotspots). Wanneer een internetgebruiker gebruik maakt van verschillende hotspots dan is de communicatie niet goed aftapbaar. Slechts bij de aanbieder waar een tapbevel wordt afgegeven wordt het communicatieverkeer afgetapt. Voor het aftappen van alle communicatie van de verdachte die gebruik maakt van meerdere toegangspunten tot het internet moet een tap worden geplaatst op alle netwerk- en dienstenaanbieders waarvan hij gebruik maakt. Dit is in de praktijk echter onmogelijk en vanuit het oogpunt van de proportionaliteit minder wenselijk (Justitiële verkenningen 3/12 (WODC), Tappen en infiltreren, blz. 31).

Niet alleen in een woning, maar ook op andere plaatsen, zoals hotels of campings, kan ten behoeve van particuliere gebruikers een draadloos netwerk worden ingericht door middel waarvan de geautomatiseerde werken, die onderdeel vormen van het netwerk, gegevens kunnen uitwisselen. Met behulp van een router kan vanuit het netwerk verbinding met het internet worden gelegd. Achter een router kunnen meerdere geautomatiseerde werken, zoals een computer, tablet of smartphone, worden gebruikt zonder dat van buitenaf kan worden nagegaan welke apparaten gebruik maken van de router en welke gegevens met welk apparaat worden opgehaald of verzonden.

Op grond van de bestaande wettelijke bevoegdheden kan communicatie worden afgetapt en opgenomen. Hierbij kan gebruik worden gemaakt van een zogenaamde internettap. Als echter gebruik wordt gemaakt van verschillende toegangspunten tot het internet, wat in toenemende mate het geval is, dan is het aftappen van de volledige communicatie van een verdachte vrijwel onmogelijk. Bovendien biedt de internettap geen soelaas als de gegevens zijn versleuteld. Als een internettap op een router wordt geplaatst, dan kan uitsluitend de in- en uitgaande communicatie worden afgetapt en opgenomen. Dit betekent dat de interne communicatie op het netwerk, waarbij geen gebruik wordt gemaakt van internet, niet kan worden onderschept. Daar komt bij dat als een internettap op een router wordt geplaatst, alle in- en uitgaande gegevensverkeer via de router wordt getapt en opgenomen, ook de gegevens van personen in wie de politie niet is geïnteresseerd. Bij actief internetgebruik betreft dit naast inloggegevens, e-mails en chatgesprekken ook ingetypte zoektermen, films en muziekbestanden. Deze data dienen te kunnen worden doorzocht op voor de opsporing relevant materiaal (Justitiële verkenningen 3/12 (WODC), Tappen en infiltreren, blz. 15 en 21). Het vereiste van de proportionaliteit bij de toepassing van ingrijpende opsporingsbevoegdheden, zoals het aftappen en opnemen van telecommunicatie, strekt tot beperking van de inzet van de bevoegdheid tot de communicatie van de persoon wiens communicatie in het belang van het onderzoek dient te worden afgetapt en opgenomen. De bescherming van de persoonlijke levenssfeer van derden dient daarbij zoveel mogelijk te worden gewaarborgd. De opsporing heeft behoefte aan een mogelijkheid om op afstand

heimelijk binnen te kunnen dringen in een geautomatiseerd werk met het oog op de identificatie van een geautomatiseerd werk of van de gebruiker. Dit kan onder meer een computer of een smartphone betreffen. Op basis van de identificerende gegevens kan dan, meer gericht, een geautomatiseerd werk worden onderzocht.

3. Cloudcomputingdiensten
Tegenwoordig worden gegevens door particulieren en bedrijven niet altijd meer op de harde schijf van een computer in het eigen netwerk opgeslagen, maar wordt in toenemende mate gebruik gemaakt van zogenaamde «webbased» toepassingen. Hierbij moet worden gedacht aan de (al dan niet verspreide) opslag van gegevens in de «Cloud», wat wil zeggen dat voor de opslag van gegevens gebruik wordt gemaakt van servers die zich elders in Nederland of in het buitenland bevinden. Cloudcomputingdiensten bestaan uit een veelheid van al dan niet verbonden of geïntegreerde toepassingen. Verschillende aanbieders bieden diensten aan op het gebied van Cloud computing. Voorbeelden zijn Hotmail, Dropbox, Googledocs en Mega upload. De gegevens worden langs geautomatiseerde weg door de aanbieder van de desbetreffende dienst op verschillende servers opgeslagen, zonder dat de gebruiker daarop invloed heeft. De locatie van de servers en de daarop bewaarde gegevens is soms ook voor de aanbieder niet te achterhalen. Voor de aanbieders is de plaats van opslag vanuit bedrijfseconomisch perspectief vooral van belang in verband met de kosten daarvan en de zekerheid van verbindingen. Met behulp van het internet is gewaarborgd dat de gegevens voor de belanghebbenden toegankelijk zijn. Doordat de bestanden doorgaans in gedeelten worden opgeslagen over meerdere servers worden verspreid, betekent dit dat gegevens van één gebruiker zich in verschillende landen kunnen bevinden.
Als het nodig is om gegevens die op een geautomatiseerd werk of een gegevensdrager zijn opgeslagen vast te leggen, dan biedt het Wetboek van Strafvordering, zoals eerder is opgemerkt, de mogelijkheid van een doorzoeking van de plaats waar de gegevensdrager zich bevindt ter vastlegging van die gegevens. Deze bevoegdheid wordt ook aangeduid als doorzoeking ter vastlegging van gegevens. Vervolgens kan vanaf de plaats waar de doorzoeking plaatsvindt ook onderzoek worden gedaan in een elders aanwezig geautomatiseerd werk, voor zover vanaf die plaats toegang kan worden verkregen tot dat geautomatiseerde werk (artikel 125j, eerste lid, Sv). Deze bevoegdheid wordt ook wel aangeduid als de netwerkzoeking. Deze bevoegdheden gaan er in belangrijke mate van uit dat de gegevens die voor de opsporing van belang zijn, zich bevinden op een bepaalde gegevensdrager die zich op een vaste plaats bevindt, die ter verkrijging van de gegevens alleen nog hoeft te worden binnengedrongen. Zoals hierboven is aangegeven, spoort dit niet meer met de werkelijkheid in gevallen waarin smartphones en laptops worden gebruikt.
Belangrijk bezwaar van deze bevoegdheden is voorts dat de verdachte doorgaans op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Dat kan strijdig zijn met het belang van het onderzoek. Ook kan, op grond van de bestaande wettelijke bevoegdheden, de aanbieder van de opslagdienst worden aangesproken op de verstrekking van de opgeslagen of vastgelegde gegevens (artikel 126ng Sv). Hierboven is reeds aan de orde gekomen dat dit in de praktijk minder eenvoudig is, omdat de aanbieder zich vaak in het buitenland bevindt.

Als het gaat om communicatie dan kan, op grond van de bestaande wettelijke bevoegdheden, communicatie worden afgetapt en opgenomen, al dan niet met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst (artikelen 126m, 126t en 126zg Sv). Ook kan van een aanbieder worden

gevorderd gegevens te verstrekken (artikelen 126n, 126na, 126ng, 126u, 126ua, 126ug, 126zh, 126zi en 126zl Sv). Het gebruik van Cloudcomputingdiensten kan echter tot onduidelijkheid leiden over de vraag wie als aanbieder van een telecommunicatiedienst in de zin van de Telecommunicatiewet kan worden aangemerkt. Dit kan aan de orde zijn bij webdiensten die geen diensten verlenen op het gebied van communicatie. Hierbij moet ook worden gedacht aan zogenaamde «bulletproof hosting providers» die hun klanten de mogelijkheid bieden om volledig anoniem, en vaak in resell constructies, illegale activiteiten te ontplooien. Daarbij kan gedacht worden aan het hosten van een nagebouwde bankwebsite om financiële transacties af te vangen, het aanbieden van diensten waarmee op anonieme wijze betaaltransacties kunnen plaatsvinden of het onderbrengen van tijdelijke phishingwebstes op een server. Wanneer de verleners van webdiensten niet als aanbieder van een communicatiedienst in de zin van de wet kunnen worden aangemerkt, kan aan hen geen bevel tot medewerking worden gegeven. Ook als dit wel het geval zou zijn dan valt deze aanbieder niet onder de Nederlandse rechtsmacht, zodat een rechtshulpverzoek nodig is. De ervaring leert dat het karakter van deze webdiensten veelal onlosmakelijk is verbonden met het feit dat de aanbieder ervan in een land is gevestigd, waarmee Nederland niet of nauwelijks een rechtshulprelatie onderhoudt. Anonimisering en afscherming van de gegevens voor politie en justitie vormen een essentiële elementen van het bedrijfsmodel van deze aanbieders. De opsporing heeft behoefte aan de mogelijkheid om heimelijk toegang te kunnen verkrijgen tot gegevens die in de Cloud zijn opgeslagen, zonder dat de verdachte of de aanbieder daarbij is betrokken.
Het Cbp heeft opgemerkt dat aan de gevolgde redenering, dat effectieve middelen ingeval van bulletproof hostingproviders ontbreken, niet de conclusie kan worden verbonden dat de opsporing heimelijk toegang dient te krijgen tot alle in de Cloud opgeslagen gegevens. Het is voor de opsporing echter van essentieel belang dat toegang kan worden verkregen tot gegevens die in de Cloud zijn opgeslagen. Dit betekent niet dat een onderzoek in een geautomatiseerd werk aangewezen is, als ook langs andere weg toegang tot die gegevens verkregen kan worden. Het vereiste van het «dringende opsporingsbelang» brengt met zich mee dat een dergelijk onderzoek uitsluitend aan de orde is als andere opsporingsbevoegdheden tekort schieten. Het is aan de officier van justitie om in het bevel de feiten en omstandigheden op te nemen, op grond waarvan de rechter-commissaris kan afwegen of aan dit vereiste is voldaan.
De bovenbeschreven, verouderde wetgeving vormt in toenemende mate een belemmering voor de effectiviteit en het welslagen van het opsporingsonderzoek naar ernstige strafbare feiten. De opsporingsbevoegdheden die zijn gericht op het vastleggen van elektronische gegevens of het aftappen en opnemen van communicatie, voldoen niet langer omdat gebruik wordt gemaakt van versleuteling, de geautomatiseerde werken onderdeel vormen van een netwerk of de gegevens worden opgeslagen in de Cloud. Een alternatief is om andere (bestaande) opsporingsbevoegdheden in te zetten, maar hieraan zijn zwaarwegende bezwaren verbonden. Deze worden hieronder geschetst.

In de eerste plaats biedt de bevoegdheid tot het opnemen van vertrouwelijke communicatie (artikelen 126l, 126s en 126zf Sv) de mogelijkheid om door middel van een technisch hulpmiddel, zoals een «bug» (een kleine microfoon die opgenomen signalen draadloos verzendt) of een richtmicrofoon, heimelijk vertrouwelijke communicatie op te nemen. Ter uitvoering van de bevoegdheid kan een besloten plaats of een woning worden betreden, zodat het technische hulpmiddel kan worden geplaatst. Uit de wetsgeschiedenis blijkt dat de wetgever daarbij heeft gedacht aan het in een kantoor plaatsen van een bug op het toetsenbord en de muis van een computer. Daardoor kunnen alle toetsaanslagen en muisklikken

van de computer worden geregistreerd (Kamerstukken II 1996/97, 25 403, nr. 3, blz. 35). Niet is voorzien in de mogelijkheid om een bug te plaatsen door middel van software die van buitenaf, dus online, op de computer wordt geplaatst. De noodzaak van fysieke toegang tot de plaats van het geautomatiseerde werk zich bevindt, vormt echter in veel gevallen een grote belemmering voor de opsporing zowel in de gevallen waarin de locatie van het geautomatiseerde werk niet bekend is (terwijl de technische ontwikkelingen het op afstand plaatsen van een «bug» wel mogelijk maken) als in gevallen waarin die locatie wel bekend is, maar de kans bestaat op ontdekking of op onvoorziene omstandigheden ter plaatse. Het is dan niet nodig een woning te betreden om een technisch hulpmiddel te plaatsen, zodat er geen inbreuk wordt gemaakt op het grondwettelijke beschermde recht van onschendbaarheid van de woning (artikel 12 Grondwet).

De inzet van andere opsporingsbevoegdheden dan de bevoegdheden die zien op het vergaren of vorderen van gegevens, zoals de observatie (artikelen 126g, 126o en 126zd, eerste lid, onderdeel a Sv), het stelselmatig inwinnen van informatie (artikelen 126j, 126qa en 126zd, eerste lid, onderdeel c Sv) of de inkijkoperatie (artikelen 126k, 126r en 126zd, eerste lid, onderdeel d Sv) bieden evenmin soelaas. De inzet van deze bevoegdheden is niet gericht op de toegang tot gegevens die langs elektronische weg worden verwerkt en biedt dan ook weinig kans op kennisneming van de inhoud van de gegevens die door de verdachte zijn ontvangen of verzonden, of van de communicatie waarbij hij is betrokken.

Voorts bestaat de mogelijkheid om een geautomatiseerd werk of een gegevensdrager in beslag te nemen. Inbeslagneming van een voorwerp is mogelijk bij aanhouding van de verdachte (artikel 95, eerste lid, Sv), in geval van ontdekking op heterdaad van een strafbaar feit (artikel 96, eerste lid, Sv) of ingeval van verdenking van een ernstig strafbaar feit (artikelen 96c, eerste lid, 97 eerste lid, 98, eerste lid, en 99, eerste lid, Sv). Het laatste geval betreft de doorzoeking van een plaats zoals een voertuig of een woning. Met de inbeslagneming van een voorwerp komen de gegevens, die op een geautomatiseerd werk of de gegevensdrager zijn opgeslagen, in het bezit van de opsporing. Een belangrijk bezwaar van inbeslagneming is echter dat de verdachte hierdoor op de hoogte kan komen van het feit dat politie en justitie in hem zijn geïnteresseerd. De inzet van deze bevoegdheid brengt met zich mee dat politie en justitie kunnen beschikken over alle gegevens die op het geautomatiseerde werk of de gegevensdrager zijn opgeslagen. Voor de waarheidsvinding mag onderzoek worden gedaan aan inbeslaggenomen voorwerpen teneinde gegevens voor het strafrechtelijk onderzoek ter beschikking te krijgen (HR 29 maart 1994, NJ 1994, 577 en Rb Haarlem 23 september 2010, NJFS 2010, 327, LJN BN8648). Het kennisnemen van een grote hoeveelheid persoonsgegevens met het oog op het selecteren van voor de opsporing relevante gegevens zal veelal als disproportioneel moeten worden aangemerkt in de gevallen waarin een voorwerp in beslag wordt genomen uitsluitend om bepaalde gegevens vast te leggen (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 19). Het oogmerk van de Wet vorderen gegevens was juist om de grootte van de inbreuk te beperken. Van de bevoegdheden tot inbeslagneming van een voorwerp en tot het bevelen van de uitlevering van een voorwerp mag geen gebruik worden gemaakt indien met toepassing van de bevoegdheden rond het vorderen van gegevens kan worden volstaan. Alleen indien er omstandigheden zijn die ertoe nopen dat de gehele gegevensdrager wordt verkregen, kunnen de inbeslagnemingsbevoegdheden worden toegepast (Kamerstukken II 2001/02, 28 366, nr. 1, blz. 28 en 2003/04, 29 441, nr. 3, blz. 12).

Daarom wordt voorgesteld in het Wetboek van Strafvordering een specifieke bevoegdheid op te nemen tot het op afstand heimelijk binnendringen van een geautomatiseerd werk dat bij een verdachte in gebruik is. Deze bevoegdheid is essentieel voor de bestrijding van ernstige criminaliteit, waarbij gebruik wordt gemaakt van een geautomatiseerd werk. Het binnendringen kan uitsluitend worden verricht met het oog op het verrichten van bepaalde onderzoekshandelingen. Met behulp van deze bevoegdheid kan het geautomatiseerde werk of de gebruiker worden geïdentificeerd ten behoeve van een meer gericht bevel tot het aftappen en opnemen van communicatie. Ook kunnen gegevens worden vastgelegd die in de Cloud zijn opgeslagen zonder dat de verdachte of de aanbieder daarbij is betrokken of kunnen sleutels worden onderschept zodat de versleuteling van gegevens ongedaan kan worden gemaakt dan wel toegang kan worden verkregen tot gegevens. Voorts kunnen gegevens ontoegankelijk worden gemaakt, kan communicatie worden afgetapt en opgenomen voordat deze wordt versleuteld of kan de precieze locatie van het geautomatiseerde werk – en daarmee van de persoon die het werk in gebruik heeft – nauwkeurig worden vastgesteld. In het belang van het onderzoek kunnen de gegevens worden vastgelegd.

Het binnendringen kan met behulp van verschillende methoden worden gerealiseerd. In onderdeel 2.5. van deze memorie wordt hier nader op ingegaan. Het binnendringen is voorbehouden aan bepaalde, daartoe aangewezen opsporingsambtenaren die over gespecialiseerde kennis beschikken op het gebied van de informatie- en communicatietechnologie. Deze ambtenaren vormen onderdeel van het zogenoemde technische team, en zijn niet betrokken bij het operationele onderzoek.

Het verrichten van onderzoekshandelingen vindt in beginsel plaats met behulp van een technisch hulpmiddel. Dit is echter niet per se noodzakelijk. Indien gebruik wordt gemaakt van een technisch hulpmiddel, zal dit hulpmiddel vooraf moeten zijn gekeurd. Het plaatsen en verwijderen van een technisch hulpmiddel is voorbehouden aan daartoe aangewezen opsporingsambtenaren van het technische team. De resultaten van de onderzoekshandelingen worden ter beschikking gesteld aan de opsporingsambtenaren die zijn betrokken bij het operationele onderzoek, ook wel aangeduid als het tactische team.

Alle onderzoekshandelingen die al dan niet met behulp van een technisch hulpmiddel ter uitvoering van een bevel van de officier van justitie worden verricht, worden geautomatiseerd vastgelegd. Dit wordt ook wel logging genoemd. Hierdoor zal steeds inzichtelijk zijn welke handelingen in dat kader zijn verricht.

De opsporingsambtenaren die kunnen worden aangewezen voor het doen van onderzoek in een geautomatiseerd werk zijn de opsporingsambtenaren van de politie, de Koninklijke marechaussee en de bijzondere opsporingsdiensten, bedoeld in artikel 141 van het Wetboek van Strafvordering, evenals de buitengewone opsporingsambtenaren, bedoeld in artikel 142 van dat wetboek. De politie heeft behoefte aan de bevoegdheid tot het onderzoek in een geautomatiseerd met het oog op de uitvoering van de politietaak, bedoeld in artikel 3 van de Politiewet 2012, namelijk de opsporing van ernstige vormen van computercriminaliteit. Dit kan ook vormen van commune criminaliteit betreffen, waarbij gebruik wordt gemaakt van een geautomatiseerd werk om gegevens op te slaan of over te dragen, zoals ernstige vormen van drugshandel, fraude of levensdelicten. Bij de Koninklijke marechaussee bestaat de behoefte aan deze bevoegdheid met het oog op de uitvoering van de politietaak op de luchthaven Schiphol en op en nabij de daartoe aangewezen grensdoorlaatposten, bedoeld in artikel 4, eerste lid, onderdelen c en f, van de

Politiewet 2013, namelijk het opsporingsonderzoek naar mensenhandel en mensensmokkel. Bij de FIOD/ECD bestaat behoefte aan deze bevoegdheid met het oog op de strafrechtelijke handhaving van de rechtsorde op bepaalde beleidsterreinen, bedoeld in artikel 3 van de Wet op de bijzondere opsporingsdiensten, namelijk de opsporing van ernstige vormen van fraude en witwassen. Vanwege de behoefte aan specifieke expertise op het gebied van de informatie- en communicatietechnologie, benodigd voor het onderzoek in een geautomatiseerd werk, kunnen personen die niet beschikken over algemene opsporingsbevoegdheid als buitengewoon opsporingsambtenaar worden ingezet. Dit betreft de opsporingsambtenaren, bedoeld in artikel 142, eerste lid, onderdeel b, van het Wetboek van Strafvordering. De aan te wijzen opsporingsambtenaren moeten voldoen aan de eisen op het gebied van de deskundigheid en samenwerking. Dit wordt in paragraaf 2.4. nader toegelicht.

Vanwege de reikwijdte van de bevoegdheid en de mate van inbreuk op de persoonlijke levenssfeer van de betrokkene, is het van groot belang dat de inzet van de bevoegdheid met strikte waarborgen is omgeven. Dit wordt eveneens in paragraaf 2.4. nader toegelicht.

2.2. De reikwijdte van de voorgestelde bevoegdheid en de plaatsing in het Wetboek van Strafvordering

Met de verwijzing naar een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, wordt tot uitdrukking gebracht dat het toepassingsbereik van onderzoek in een geautomatiseerd werk, zich niet beperkt tot specifieke gevallen van computercriminaliteit, zoals computervredebreuk of het gebruik van botnets voor het platleggen van vitale infrastructuur door verstikkingsaanvallen (de zogenaamde «DDoS-aanvallen»). De bevoegdheid kan ook ten aanzien van andere misdrijven worden toegepast waarvoor op grond van artikel 67, eerste lid, Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. Bij het voorbereiden en plegen van meer traditionele misdrijven is het gebruik van moderne ICT-voorzieningen een steeds belangrijker component geworden, bijvoorbeeld als het gaat om (versluierde) communicatie tussen criminelen, of het raadplegen van informatie over bijvoorbeeld gebouwen, het vervaardigen van explosieven of het gebruik van toxische stoffen. Het kan gaan om misdrijven als moord, handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel, maar ook ernstige financiële misdrijven, zoals omvangrijke ernstige fraude. De opsporingspraktijk heeft ook in die gevallen de behoefte aan de voorgestelde bevoegdheid, zodat het mogelijk is in voorkomende gevallen een geautomatiseerd werk binnen te dringen en te onderzoeken met het oog op bijvoorbeeld de vastlegging van gegevens. Wel wordt de bevoegdheid binnen de kring van de misdrijven waarvoor voorlopige hechtenis mogelijk is nader ingekaderd, afhankelijk van de aard van de te verrichten onderzoekshandelingen. Dit naar aanleiding van het advies van de Afdeling advisering van Afdeling advisering. Hierop wordt in paragraaf 2.4. nader ingegaan.

Voor de regeling rond het binnendringen van het geautomatiseerde werk is aangesloten bij de regeling van de computervredebreuk in het Wetboek van Strafrecht. Op grond van deze regeling is van binnendringen in ieder geval sprake indien de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid (artikel 138ab, eerste lid, Sr).

Vanwege de nauwe samenhang met de bestaande bevoegdheid van de doorzoeking ter vastlegging van gegevens, zoals geregeld in artikel 125i Sv, was de voorgestelde bevoegdheid aanvankelijk in de zevende afdeling van Titel IV («Enige bijzondere dwangmiddelen») van het Wetboek van Strafvordering opgenomen. In deze afdeling is de doorzoeking ter vastlegging van gegevens geregeld. De Afdeling advisering heeft opgemerkt dat de voorgestelde bevoegdheid heimelijk wordt uitgeoefend, dus zonder dat de verdachte daar kennis van krijgt, en dat deze bevoegdheid daarom in de kern samenhang vertoont met de bijzondere opsporingsbevoegdheden die zijn vervat in Titel IVA van het Eerste Boek. Bij de toepassing van bijzondere opsporingsbevoegdheden op grond van Titel IVA zijn meer rechtswaarborgen van toepassing dan bij Titel IV het geval is, de Afdeling wijst op de ruimere notificatieplicht, de voeging van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen die verschoningsgerechtigden raken. Indien niet dragend gemotiveerd kan worden waarom de voorgestelde bevoegdheid opgenomen dient te worden in Titel IV van het Eerste Boek adviseert de Afdeling deze bevoegdheid op te nemen in de regeling van bijzondere opsporingsbevoegdheden (Titel IVA van het Eerste Boek).

Naar aanleiding van dit advies kan worden opgemerkt dat aanvankelijk was gekozen voor plaatsing van de voorgestelde bevoegdheid in titel IV van het Eerste Boek vanwege de overeenkomsten van het binnendringen in een computer op afstand en de doorzoeking in een geautomatiseerd werk, evenals de met die onderzoeking verband houdende bevoegdheden zoals de regels voor de ontsleuteling van gegevens (artikel 125k, tweede lid, Sv), de beperkte kennisneming van gegevens die betrekking hebben op verschoningsgerechtigden (artikel 125l Sv), de mededeling van de vastlegging of ontoegankelijkmaking van gegevens (artikel 125m Sv), de vernietiging van vastgelegde gegevens (artikel 125n Sv) en de ontoegankelijkmaking van gegevens (artikel 125o Sv). Met de Afdeling advisering ben ik van oordeel dat plaatsing in de titel IVA voor de hand ligt vanwege de omstandigheid dat de voorgestelde bevoegdheid heimelijk wordt toegepast, zonder dat de betrokkene daar weet van heeft, en inhoudelijk overeenkomsten vertoont met de bijzondere opsporingsbevoegdheden van Titel IVA van het Eerste Boek. Daarom wordt, in navolging van het advies van de Afdeling advisering, voorgesteld de bevoegdheid in titel IVA op te nemen. De plaatsing in deze afdeling impliceert dat de rechtswaarborgen waar de Afdeling advisering op heeft gewezen, ook van toepassing zijn op het onderzoek in een geautomatiseerd werk.

Titel V van het Eerste Boek bevat bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband. Deze bevoegdheden strekken tot onderzoek naar de georganiseerde criminaliteit. Titel VB van het Eerste Boek bevat bijzondere bevoegdheden tot opsporing van terroristische misdrijven. Het is van belang dat de bevoegdheid van het onderzoek in een geautomatiseerd werk ook kan worden toegepast bij het onderzoek naar de georganiseerde criminaliteit en terroristische misdrijven. Daarom wordt voorgestelde deze bevoegdheid tevens op te nemen in de desbetreffende titels van het Eerste Boek.

De verhouding tussen de voorgestelde bevoegdheid en de bestaande bevoegdheid van artikel 125i Sv is als volgt. De bevoegdheid van artikel 125i Sv betreft de doorzoeking van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn vastgelegd. Indien deze bevoegdheid wordt uitgeoefend in een plaats die bij de verdachte in gebruik is, dan kan deze op de hoogte raken van het opsporingsonderzoek. Een belangrijk kenmerk van de voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk is dat op

afstand heimelijk een geautomatiseerd werk wordt onderzocht, zonder dat de verdachte daar kennis van krijgt. Het doel van de bevoegdheid van de doorzoeking is het vergaren van voor de waarheidsvinding relevante gegevens die op de plaats van de doorzoeking (of op daarmee via een computernetwerk verbonden plaatsen) reeds aanwezig zijn en niet het onderscheppen van gegevens die in een proces zijn van verwerking of overdracht tussen computers (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 49). Anders dan de bevoegdheid van artikel 125i Sv is de voorgestelde bevoegdheid niet beperkt tot de vastlegging van reeds aanwezige gegevens. Deze kan ook betrekking hebben op gegevens die na de afgifte van het bevel worden verwerkt. Daarnaast kan de bevoegdheid worden ingezet met het oog op de toepassing van bepaalde doelen op het gebied van de opsporing van ernstige strafbare feiten. Op deze punten is de voorgestelde bevoegdheid ruimer. Overigens is nauw aangesloten bij de bestaande wettelijke regeling voor de doorzoeking ter vastlegging van gegevens.

De Rvdr is van mening dat de toepassing van de regeling voor de beperkte kennisneming van gegevens die betrekking hebben op verschoningsgerechtigden (artikel 125l Sv) op het onderzoek in een geautomatiseerd werk nadere toelichting zo niet regeling verdient. Zo is het de vraag op welke wijze communicatie met een verschoningsgerechtigde (bijvoorbeeld een advocaat) zal kunnen worden ontdekt en tijdig worden vernietigd conform artikel 126aa Sv. Ook de NOvA wijst op het ontbreken van een regeling over de wijze waarop moet worden omgegaan met informatie en documenten die ook voor de opsporing geheim behoren te blijven, zoals de correspondentie tussen de verdachte en zijn raadsman, die op de computer wordt aangetroffen en mogelijk wordt «overgenomen». Een uitdrukkelijk in de wet voorgeschreven procedure voor dit soort situaties kan veel juridische procedures en mogelijk mislukte vervolgingen door niet-ontvankelijkverklaringen voorkomen. Het Nederlands Uitgeversverbond, de Nederlandse Vereniging van Journalisten, het Nederlands Genootschap van Hoofdredacteuren en het Persvrijheidsfonds wijzen in hun gemeenschappelijke reactie op de mogelijkheid om in computer van journalisten binnen te dringen, waardoor journalistieke bronnen achterhaald kunnen worden.

Naar aanleiding van deze adviezen kan worden opgemerkt dat de regeling rond de toepassing van bijzondere opsporingsbevoegdheden in een speciale procedure voorziet voor mededelingen gedaan door of aan een verschoningsgerechtigde. Dit betreft de regeling van het bestaande artikel 126aa, tweede lid, Sv. Deze regeling heeft betrekking op gegevens die ter kennis van de opsporingsambtenaren komen in het kader van de uitoefening van bijzondere opsporingsbevoegdheden jegens anderen dan de verschoningsgerechtigden (de zogenaamde «bijvangst»), en is ook van toepassing op het onderzoek in een geautomatiseerd werk. Anders dan bij de regeling van artikel 125l Sv bij de doorzoeking ter vastlegging van gegevens, waarbij de verdachte in beginsel op de hoogte is van de uitvoering van die doorzoeking, voorziet de regeling van artikel 126aa, tweede lid, Sv in de verplichting tot vernietiging van de processen-verbaal en andere voorwerpen mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 Sv zou kunnen verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd. In de jurisprudentie worden de arts, de geestelijke, de notaris en de raadsman als verschoningsgerechtigde in de zin van deze bepaling erkend. Ook andere geneeskundige beroepsbeoefenaren dan de arts kunnen verschoningsgerechtigd zijn, zoals de apotheker of de verpleegkundige. Dit betekent dat zodra bij het onderzoek in een geautomatiseerd werk met het technische hulpmiddel gegevens worden vastgelegd die betrekking hebben op communicatie tussen de verdachte en zijn

raadsman of tussen de verdachte en zijn arts wordt, de opgenomen en vastgelegde gegevens worden vernietigd voor zover deze onder de geheimhoudingsplicht vallen. In de gevallen waarin de geheimhouder verdachte is, wordt het oordeel van een gezaghebbend lid van de betreffende beroepsgroep ingewonnen over de vraag welke gegevens dergelijke mededelingen behelzen. De procedure voor de vernietiging van de vastgelegde gegevens is uitgewerkt in het Besluit bewaren en vernietigen niet gevoegde stukken. Dit besluit voorziet eveneens in een regeling van nummerherkenning voor advocaten. Indien bij het aftappen en opnemen van telecommunicatie een nummer is betrokken dat door de NOvA bij de politie is aangemeld, dan wordt het opnemen van de communicatie onmiddellijk beëindigd. Indien communicatie is opgenomen voordat het nummer is herkend, worden de gegevens van de communicatie onmiddellijk langs geautomatiseerde weg vernietigd (artikel 4a Besluit bewaren en vernietigen niet gevoegde stukken). In reactie op de wens van de NOvA, dat de procedure van nummerherkenning ook wordt gewaarborgd bij het onderzoek in een geautomatiseerd werk, kan worden bevestigd dat dit inderdaad het geval is voor het aftappen en opnemen van telecommunicatie.

Wat betreft de positie van journalisten kan worden gewezen op het wetsvoorstel bronbescherming in strafzaken, dat in 2014 bij de Tweede Kamer der Staten-Generaal is ingediend (Kamerstukken II 2014/14, 34 032, nr. 1). Dit wetsvoorstel voorziet in wettelijke verankering van een recht op bronbescherming. Daartoe wordt voorgesteld een nieuw artikel 218a in het Wetboek van Strafvordering op te nemen. Tevens wordt voorgesteld in het eerdergenoemde artikel 125l Sv een verwijzing naar artikel 218a Sv op te nemen, zodat dit recht onverkort zal gelden bij een onderzoek in een geautomatiseerd werk. Verder wordt, naar aanleiding van het advies van de Afdeling advisering, voorgesteld de voorwaarde voor de inzet van de bevoegdheid van het op afstand heimelijk betreden van een geautomatiseerd werk van aan te scherpen voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens. Voor het verrichten van deze onderzoekshandelingen zal een misdrijf zijn vereist dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld of een misdrijf dat bij algemene maatregel van bestuur is aangewezen. De misdrijven die raakvlakken hebben met de vrijheid van meningsuiting, zoals de belediging (art. 137c Sr), het aanzetten tot haat (art. 137d Sr), of de openbaarmaking van beledigende uitlatingen (art. 137e Sr) zullen niet worden niet worden aangewezen. Overigens geldt thans, op grond van de Aanwijzing toepassing dwangmiddelen tegen journalisten, een toetsingskader voor de toepassing van dwangmiddelen tegen journalisten (Stcrt. 2012, 3656). Uitgangspunt daarbij is dat in de praktijk slechts dan sprake kan zijn van de toepassing van strafvorderlijke dwangmiddelen, als dit het enig denkbare effectieve middel is om een zeer ernstig delict op te sporen of te voorkomen. In het licht van de uitspraak van het EHRM in de zaak Sanoma (EHRM 14 september 2010, nr. 38224/03, Sanoma Uitgevers BV vs Nederland) is het van belang dat er slechts wordt opgetreden op basis van een voorafgaande rechterlijke afweging van enerzijds het recht op vrije meningsuiting en anderzijds het opsporingsbelang.

In het Wetboek van Strafvordering wordt onderscheid gemaakt tussen de bevoegdheden met betrekking tot opgeslagen gegevens en de bevoegdheden met betrekking tot stromende gegevens. Met het eerste wordt gedoeld op gegevens die in een computer zijn opgeslagen. Met het tweede wordt gedoeld op gegevens die in een proces zijn van verwerking of overdracht tussen computers (Kamerstukken II 1998/99, 26 671, nr. 3,

blz. 3). Destijds is voor dit onderscheid gekozen om de strafbepalingen en strafvorderlijke bevoegdheden rond het gebruik van gegevens voldoende precies te kunnen omschrijven (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 27). Het onderscheid tussen de bevoegdheden met betrekking tot opgeslagen gegevens en stromende gegevens is in de praktijk echter aan het vervagen. Ook zijn de diensten van de verschillende aanbieders in elkaar over gaan lopen. Zo zijn er aanbieders van internetdiensten die opslagdiensten in de Cloud aanbieden (Google Docs, Dropbox, Skydrive). Webmaildiensten worden niet alleen gebruikt om berichten te versturen naar andere e-mailadressen maar ook voor interne communicatie binnen criminele groeperingen. Een bericht wordt dan in de concepten box geplaatst waarna verschillende personen op de dienst (Gmail of Hotmail) waarmee de inloggegevens worden gedeeld, kunnen inloggen en kennis kunnen nemen van de inhoud van het bericht zonder dat dit als e-mailbericht naar de ontvanger wordt verzonden. Een e-mailbericht dat via een openbaar telecommunicatienetwerk naar een andere computer wordt verzonden, kan worden aangemerkt als communicatie. De inhoud van het bericht kan worden achterhaald door middel van toepassing van de bevoegdheid van het aftappen en opnemen van communicatie (artikelen 126m, 126t en 126zg Sv). Als het bericht bij de aanbieder is opgeslagen, dan kunnen de gegevens worden verkregen door middel van een vordering aan de aanbieder tot het verstrekken van opgeslagen persoonsgegevens (artikelen 126ng, 126ug en 126zo Sv). Het is dan ook niet noodzakelijk om de verhouding tussen de bevoegdheden rond de doorzoeking van een geautomatiseerd werk ter vastlegging van gegevens, in Titel IV van het Wetboek van Strafvordering, en de bijzondere bevoegdheden tot opsporing, in Titel IVA van het Wetboek van Strafvordering, te herzien maar te volstaan met een aanvulling van de bestaande bevoegdheden. Met dit wetsvoorstel wordt daarin voorzien.

2.3. De doelen van het onderzoek in een geautomatiseerd werk

Het onderzoek in een geautomatiseerd werk kan uitsluitend plaatsvinden met het oog op het verrichten van bepaalde onderzoekshandelingen. Deze handelingen zijn de volgende:

2.3.1 De vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan

Ter voorbereiding van het inzetten van andere opsporingsbevoegdheden of het bepalen van de richting van het opsporingsonderzoek kan het noodzakelijk zijn om bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, vast te stellen. Voor de inhoud van de bevoegdheid is nauw aangesloten bij de eerdergenoemde bevoegdheid tot het opnemen van een besloten plaats. Kenmerk is dat heimelijk toegang wordt verkregen tot het geautomatiseerde werk teneinde informatie te vergaren die ten grondslag kan worden gelegd aan beslissingen over het verdere optreden rond het geautomatiseerde werk. Er is als het ware sprake van een virtuele plaatsopneming of inkijkoperatie, waarbij bepaalde kenmerken van het geautomatiseerde werk worden vastgesteld, ter voorbereiding van het binnendringen met het oog op het verrichten van bepaalde onderzoekshandelingen, zoals de uitvoering van een bevel tot het aftappen van communicatie of het veiligstellen van gegevens die in het geautomatiseerde werk zijn of worden verwerkt. Met de term vastlegging van gegevens wordt gedoeld op het overnemen (of: kopiëren) van opgeslagen gegevens. Anders dan bij de bijzondere opsporingsbevoegdheid van het opnemen van een besloten plaats, die jegens de rechthebbende kan worden ingezet, is de bevoegdheid van onderzoek in het geautomatiseerde werk beperkt tot een geautomatiseerd werk dat bij de verdachte in gebruik is.

De bevoegdheid kan worden toegepast ten behoeve van de verkrijging van een nummer of van andere gegevens ter identificatie van het geautomatiseerde werk of de gebruiker. Dit betreft identificerende gegevens, zoals een IP-, IMEI- of IMSI-nummer, aan de hand waarvan een apparaat of de gebruiker kan worden geïdentificeerd. Dit kan van belang zijn voor de afgifte van een bevel tot het aftappen en opnemen van communicatie of voor het vorderen van gegevens van een aanbieder van een telecommunicatiedienst of het vorderen van gegevens van andere derden (artikelen 126nd, 126ud en 126zl Sv). De bepaling van de locatie van het geautomatiseerde werk kan ook van belang zijn voor de mogelijkheid om tactisch op te treden, bijvoorbeeld door een verdachte aan te houden of voorwerpen in beslag te nemen.

Voorbeelden:
1. Het binnendringen van een router zodat kan worden achterhaald wat het identificerende kenmerk van de laptop van de verdachte is zodat de toepassing van onderzoekshandelingen (bijvoorbeeld de vastlegging van opgeslagen of vastgelegde gegevens) of de inzet van opsporingsbevoegdheden (bijvoorbeeld het aftappen en opnemen van communicatie) selectiever kan plaatsvinden.
2. Het binnendringen van een computer, waarvan alleen het Tor-adres bekend is, om het IP-adres vast te stellen teneinde een bevel tot het aftappen en opnemen van communicatie aan de aanbieder te kunnen afgeven.
3. Het binnendringen van een smartphone van een persoon, die criminele contacten onderhoudt met een verdachte, om zijn identiteit vast te kunnen stellen.
4. Het in kaart brengen van de software die in het geautomatiseerde werk aanwezig is (o.a. welke versie het betreft).

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

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

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

deze weg kunnen inlogcodes en wachtwoorden, die toegang geven tot versleutelde gegevens, worden verkregen. Voor het vastleggen van de gegevens kan gebruik worden gemaakt van een «keylogger», die de toetsaanslagen op een toetsenbord vastlegt.

Voorbeelden:
1. De verdachte maakt veelvuldig gebruik van cryptocontainers of complete versleuteling van de harde schijf. Nadat in het geautomatiseerde werk is binnengedrongen kan het wachtwoord worden afgevangen zodat bij latere vastlegging van de gegevens de cryptocontainer kan worden geopend.
2. De verdachte heeft zijn gegevens via het Tor-netwerk in de Cloud opgeslagen. De aanbieder kan niet worden vastgesteld of bereikt. Het veiligstellen van de gegevens is uitsluitend mogelijk als de verbinding met de Clouddienst open is. Daarvoor is het noodzakelijk om de gegevens van het geautomatiseerde werk over te nemen als de verbinding met de Clouddienst in werking is.

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

2.3.3 De ontoegankelijkmaking van gegevens
Worden tijdens het onderzoek in een geautomatiseerd werk op grond van de voorgestelde bevoegdheid gegevens aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, dan kan de officier van justitie bepalen dat deze gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Met de voorgestelde regeling wordt aangesloten bij de bestaande wettelijke regeling van de ontoegankelijkmaking van gegevens, in artikel 125o Sv. Onder ontoegankelijkmaking van gegevens wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van een geautomatiseerd werk of derden verder van de gegevens kennis nemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen van de gegevens uit het geautomatiseerde werk, met behoud van de gegevens ten behoeve van de strafvordering (artikel 125o, tweede lid, Sv). De definitie van ontoegankelijkmaking laat echter ook andere maatregelen toe, mits die kunnen strekken ter voorkoming van de verdere kennisneming van die gegevens. Met behulp van hardware kan een ingang van een computer (tijdelijk) onbruikbaar worden gemaakt. Met behulp van software kunnen gegevens worden versleuteld of gewist (met behoud van een kopie voor justitie). In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is, rekening houdend met de eisen van proportionaliteit en subsidiariteit (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 21).
Uit het voorgaande vloeit voort dat de voorgestelde bevoegdheid ook kan worden ingezet ter bestrijding van botnets. Een «bot» is een geautomatiseerd werk van een willekeurige gebruiker die als gevolg van een infectie met een bepaalde malware door de «inbreker» kan worden gecontroleerd

en waaraan de inbreker buiten de gebruiker om opdrachten kan geven. Een botnet is een grootschalig en wereldwijd netwerk van semiautonoom werkende softwarerobots op «zombiecomputers», die op afstand kunnen worden bediend om illegale acties uit te voeren, zoals het versturen van spam, het verzamelen van (bedrijfs)geheimen en andere vertrouwelijke informatie zoals creditcardgegevens en wachtwoorden, het uitvoeren van DDoS-aanvallen en het verspreiden van malware zoals ransomware (een infectie die de computer blokkeert en pas vrijgeeft nadat losgeld is betaald). Na een succesvolle besmetting kan ongemerkt meer kwaadaardige software worden geïnstalleerd, waaronder sniffers (computerprogramma waarmee het dataverkeer op het netwerk kan worden bekeken en geanalyseerd) en keyloggers (het vastleggen van toetsaanslagen).
Om een botnet onschadelijk te kunnen maken, is het noodzakelijk om toegang te verkrijgen tot de servers die onderdeel vormen van het botnet. Zo heeft de Nationale Recherche in 2010 het Bredolab-botnet offline gehaald, door een groot aantal «command and control» servers af te sluiten die bij een Nederlandse hosting provider stonden. Vanuit dit botnet zijn vanaf 2009 naar schatting dagelijks 3,6 miljard e-mails verstuurd. Het botnet werd daarnaast ook verhuurd aan andere cybercriminelen voor onder meer DDoS-aanvallen en het verspreiden van malware. Met de voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk wordt voorzien in een expliciete wettelijke grondslag voor de bestrijding van botnets.

Niet uitgesloten is dat de behoefte bestaat aan de vastlegging van gegevens, ten behoeve van het opsporingsonderzoek. De vastlegging van gegevens is mogelijk op basis van het voorgestelde artikel 126nba, eerste lid, onderdeel d. Dit dient dan te worden vermeld in het bevel van de officier van justitie, zodat de rechter-commissaris hiermee rekening kan houden bij de beslissing over het verlenen van de machtiging.

De kennelijke veronderstelling van de Afdeling advisering in het advies dat de voorgestelde bevoegdheid tot binnendringen van een geautomatiseerd werk met het oog op tot ontoegankelijkmaking dient om botnets waarbij gebruik gemaakt wordt van netwerken zonder centrale aansturing (peer-to-peer) uit te schakelen en dat de bevoegdheid van artikel 125p Sv van het wetsvoorstel kan worden ingezet om botnets met een centrale aansturing uit te schakelen is niet correct. De regeling van het voorgestelde artikel 125p Sv betreft de bevoegdheid tot het vorderen dat gegevens door een aanbieder van een telecommunicatiedienst ontoegankelijk worden gemaakt. Deze bevoegdheid laat de mogelijkheid onverlet dat de officier van justitie besluit de strafbare feiten te beëindigen door middel van een onderzoek in een geautomatiseerd werk. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest aangewezen is.

Met de Afdeling ben ik van mening dat een opsporingsbevoegdheid ten behoeve van grootschalige opruimacties weinig effectief zou zijn. Bij brief van 7 juli 2014 heb ik de Voorzitter van de Tweede Kamer geïnformeerd over de aanpak van botnets in Nederland (Kamerstukken II 2013/14, 26 643, nr. 320). Het Nationaal Cyber Security Centrum van mijn ministerie heeft een taak bij het verstoren van de werking van botnets. Ook Internet Service Providers (ISP's) spelen hierbij een rol.

De ontoegankelijkmaking van gegevens betreft een voorlopige maatregel. Bij de einduitspraak over het strafbaar feit of bij afzonderlijke beschikking neemt de rechter een beslissing over de ontoegankelijk gemaakte gegevens (artikelen 354 en 552fa Sv). Dit komt in paragraaf 3.3. aan de orde.

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

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

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

Het aftappen van communicatie kan zonder de medewerking van de aanbieder plaatsvinden indien dit niet mogelijk is of het belang van strafvordering zich daartegen verzet. Deze mogelijkheid is opgenomen naar aanleiding van het Cybercrime Verdrag. Dit verdrag gaat ervan uit dat de opsporingsdiensten beschikken over eigen bevoegdheden en dat daarnaast een medewerkingsplicht komt te rusten op de serviceproviders. Teneinde te voldoen aan de eisen van het verdrag is, met de Wet computercriminaliteit II, artikel 126m Sv gewijzigd zodat het opnemen van telecommunicatie ook zonder medewerking van de aanbieder kan plaatsvinden (artikelen 126m en 126t, derde en vierde lid, en 126zg, vierde lid, Sv). Vereist is dat een technisch hulpmiddel wordt gebruikt, dat voldoet aan bij algemene maatregel van bestuur te stellen eisen (artikel 126ee, onderdeel a, Sv). Deze eisen zijn vastgelegd in het Besluit technische hulpmiddelen strafvordering. In de artikelen 126m en 126t, tweede lid, Sv zijn destijds een nieuw onderdeel e. respectievelijk f. toegevoegd, die bepalen dat in het bevel de aard van het technische

hulpmiddel moet worden aangeduid waarmee de communicatie zal worden opgenomen.

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

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

In de tweede plaats kunnen stromende gegevens met betrekking tot communicatie heimelijk worden opgenomen op grond van het eerdergenoemde bevel tot het opnemen van vertrouwelijke communicatie (het direct afluisteren). Een voorbeeld betreft een gesprek dat op een openbare plaats of in een woning tussen personen plaatsvindt. Het is ook mogelijk dat er wel sprake is van communicatie maar niet van een communicatiedienst in de zin van de Telecommunicatiewet, zoals bij communicatie via het internet (Skype). Deze bevoegdheid kan eveneens uitsluitend worden ingezet in geval van verdenking van een ernstig misdrijf, waarvoor voorlopige hechtenis is toegelaten, en dat een ernstige inbreuk op de rechtsorde oplevert. In een dergelijk geval kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een ambtenaar van politie of van de Koninklijke marechaussee vertrouwelijke communicatie opneemt met een technisch hulpmiddel (artikelen 126l, 126s en 126zf, eerste lid, Sv). Hiervoor is eveneens een afzonderlijk bevel van de officier van justitie en een afzonderlijke schriftelijke machtiging van de rechter-commissaris vereist (artikelen 126l en 126s, vierde lid, en 126zf, eerste lid, Sv). Het technische hulpmiddel dat gebruikt wordt kan een keylogger zijn, die op het geautomatiseerde werk wordt aangebracht en die aanslagen op

een toetsenbord vastlegt, of een richtmicrofoon, met behulp waarvan op grote afstand vertrouwelijke communicatie kan worden afgeluisterd en opgenomen. Ook kan worden gedacht aan het op afstand aanzetten van een microfoon van een computer, zodat bijvoorbeeld VOIP-gesprekken kunnen worden afgeluisterd die worden gevoerd met de betreffende computer.

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

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

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

2.3.5 De uitvoering van een bevel tot stelselmatige observatie
De voorgestelde bevoegdheid biedt de mogelijkheid om de locatie van het geautomatiseerde werk zeer nauwkeurig te bepalen. Dit is van belang bij het gebruik van mobiele apparaten, zoals een laptop of een smartphone. Met de locatie van het apparaat wordt eveneens een indruk verkregen van de locatie van de bezitter, omdat het aannemelijk is dat deze het apparaat bij zich draagt (in de kleding of in een tas). Daardoor kunnen de bewegingen van die persoon worden gevolgd. Net als bij het aftappen van communicatie is het onderzoek in het geautomatiseerde werk beperkt tot het gebruik van het geautomatiseerde werk ten behoeve van het inzetten van de bevoegdheid van de stelselmatige observatie en is er geen sprake van onderzoek naar de gegevens, anders dan die met betrekking tot de plaatsbepaling, die in het geautomatiseerde werk worden opgeslagen.

Er kan op afstand software op een smartphone worden geïnstalleerd waardoor de GPS-functie kan worden geactiveerd. Vervolgens kunnen, bijvoorbeeld door een softwareapplicatie op de smartphone te installeren, de locatiegegevens via internet aan de ontvanger worden doorgegeven waardoor het mogelijk is een plaatsbepaling te doen. Een dergelijke plaatsbepaling (op basis van de GPS-gegevens) biedt de mogelijkheid om de plaats van de smartphone veel nauwkeuriger te bepalen dan met behulp van de zogenaamde mastgegevens mogelijk is. De mastgegevens kunnen worden verkregen door middel van het aftappen van communicatie of de verzending van zogenaamde stealth-sms berichten. Aan de hand daarvan kan worden bepaald met welke zendmast een mobiele telefoon in verbinding is geweest. De plaatsbepaling op basis van GPS-gegevens kan nuttig zijn in gevallen waarin de observatie met behulp van een observatieteam (OT) niet tot resultaat leidt. Ook kan dit nuttig zijn in gevallen waarin het van belang is dat de verdachte wordt aangehouden, maar zijn verblijfplaats niet bekend is.

Voorbeelden:
1. De verdachte is bekend met observatietechnieken en weet het observatieteam voortdurend af te schudden. Hij heeft wel een smartphone met een data-abonnement bij zich. In plaats van gebruik te maken van het observatieteam kan op afstand heimelijk toegang worden verkregen tot de smartphone, waarna via de GPS-locatie kan worden nagegaan waar de smartphone zich bevindt.
2. De verdachte gebruikt een smartphone en een GPS-jammer, zodat zijn locatie niet te bepalen is aan de hand van mastgegevens. De verdachte gebruikt zijn smartphone wel op plekken waar gratis Wi-Fi beschikbaar is. Op het moment dat de verdachte gebruik maakt van Wi-Fi worden de zichtbare Wi-Fi-netwerken doorgegeven, zodat een locatiebepaling kan worden verricht.

De bevoegdheid van de observatie is afzonderlijk geregeld in de Titels IVa en V van het Wetboek van Strafvordering. De inzet van deze bevoegdheid vereist een afzonderlijk bevel, op grond van de artikelen 126g, 126o, 126zd, eerste lid, onder a, Sv. Bij het op stelselmatige wijze waarnemen van personen gaat het om die vormen van observatie die tot resultaat kunnen hebben dat een min of meer volledig beeld wordt verkregen van bepaalde aspecten van iemands leven. Betreft het observatie van een persoon met behulp van een technisch hulpmiddel, dat over een kortere of langere periode signalen registreert, dan moet dit in beginsel worden beschouwd als stelselmatige observatie. Dit kan ook aan de orde zijn bij de observatie van een zaak die zich steeds in samenhang met de persoon verplaatst, zoals een koffer of mobiele telefoon (Kamerstukken II 1996/97, 25 403, nr. 3, blz. 27/29). Mede op grond van de jurisprudentie kan worden aangenomen dat een eenmalige of incidentele locatiebepaling bezwaarlijk is aan te merken als het volgen of stelselmatig waarnemen van de aanwezigheid of het gedrag van een persoon. Het gedurende een langere periode met een zekere frequentie vastleggen van de plaats van een geautomatiseerd werk kan echter mogelijk worden aangemerkt als een vorm van stelselmatige observatie, waarvoor een bevel van de officier van justitie is vereist. Te dien aanzien kan de inzet van deze bevoegdheid worden vergeleken met de inzet van een peilbaken.

Naar aanleiding van het advies van de Afdeling advisering wordt ingegaan op de verhouding tussen de voorgestelde bevoegdheid tot het onderzoek doen in een geautomatiseerd werk en het verbod tot het betreden – ter uitvoering van een bevel tot observatie – van een woning zonder toestemming van de rechthebbende. Uit de verwijzing naar de bestaande bepalingen over de stelselmatige observatie in het

wetsvoorstel vloeit voort dat het verbod op de stelselmatige observatie in de woning (artikelen 126g, tweede lid en 126o, tweede lid Sv) onverminderd blijft gelden. Het permanent waarnemen wat zich in een woning afspeelt via het op afstand aanzetten van een webcam van bijvoorbeeld een smartphone of een laptop, moet als even ingrijpend worden aangemerkt als het betreden van een woning; dat is in het kader van de opsporing niet toegestaan. Zie in dit verband ook: Kamerstukken II 1996/97, 25 403, nr. 3, p. 71 (wat betreft het plaatsen van een camera in een woning).

In de wettelijke regeling van de bevoegdheid van de stelselmatige observatie is voorzien in de mogelijkheid van het gebruik van een technisch hulpmiddel, voor zover daarmee geen vertrouwelijke communicatie wordt opgenomen (artikelen 126g, derde lid, en 126o, derde lid, en 126zd, vierde lid, Sv). Een softwareapplicatie die wordt ingezet met het oog op de opsporing van strafbare feiten kan worden aangemerkt als een technisch hulpmiddel. In het Besluit technische hulpmiddelen strafvordering zijn eisen opgenomen voor technische hulpmiddelen (artikel 126ee Sv). Dit besluit zal worden aangevuld met eisen voor het gebruik van een dergelijke softwareapplicatie.

Voor een bevel tot observatie als bedoeld in de artikelen 126g, 126o en 126zd Sv is geen machtiging van de rechter-commissaris vereist. Vanwege de inbreuk op de persoonlijke levenssfeer die is verbonden aan de bevoegdheid van onderzoek in een geautomatiseerd werk, wordt voorgesteld in artikel 126nba Sv de mogelijkheid van stelselmatige observatie door middel van deze bevoegdheid te binden aan een voorafgaande machtiging van de rechter-commissaris.
In de wet is bepaald dat een technisch hulpmiddel niet op een persoon wordt bevestigd, tenzij met diens toestemming (artikelen 126g, derde lid, en 126o, derde lid, Sv). In de memorie van toelichting bij de Wet bijzondere opsporingsbevoegdheden is destijds aangegeven dat bevestiging op een persoon inhoudt: op of aan het lichaam of de kleding. Daaronder valt ook plaatsbepalingsapparatuur die wordt aangebracht in een aansteker of pen die in of op de kleding wordt gedragen (Kamerstukken II 1996/97, 25 403, nr. 3). Op advies van de Afdeling advisering is nader ingegaan op de verhouding tussen de voorgestelde bevoegdheid en het verbod om een technisch hulpmiddel op de persoon te bevestigen. De huidige techniek maakt het mogelijk om op afstand software te plaatsen op een geautomatiseerd werk, zoals een smartphone, en hiermee de gps-functie aan te zetten. Op deze wijze kunnen signalen worden opgevangen over de locatie waarop het toestel, en de bezitter, zich bevindt. Plaatsbepaling op basis van GPS-gegevens is nuttig in die gevallen waarin andere observatiemogelijkheden niet of niet voldoende tot resultaat leiden of wanneer de verblijfplaats van de verdachte onbekend is.
De ontwikkeling van de techniek leidt ertoe dat de reikwijdte van het verbod om een technisch hulpmiddel op een persoon te bevestigen minder strikt dient te worden uitgelegd dan voorheen. Voorgesteld wordt om de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel tot binnendringen van een geautomatiseerd werk melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt. Dit kan een technisch hulpmiddel betreffen dat reeds op de persoon aanwezig is (zoals een mobiele telefoon in de kleding) of dat op de persoon wordt bevestigd (zoals een peilzender in de kleding). Op deze wijze kan de rechter-commissaris hiermee rekening houden bij de beoordeling van de rechtmatigheid van het bevel.

Hierboven is een overzicht gegeven van de onderzoekshandelingen in het kader van het onderzoek in een geautomatiseerd werk. Niet uitgesloten is dat naar aanleiding van het resultaat van het onderzoek wordt gekozen voor de toepassing van andere opsporingsbevoegdheden, waarvoor het niet nodig is om op afstand heimelijk in het geautomatiseerde werk binnen te dringen. Daarvoor kan worden gedacht aan bevoegdheden als de inbeslagneming van voorwerpen (artikel 94 Sv), de stelselmatige observatie (artikelen 126g, 126o en 126zd, eerste lid, onderdeel a, Sv.), de pseudokoop of -dienstverlening (artikelen 126i, 126q en 126zd, eerste lid, onderdeel b, Sv) of het aftappen van communicatie, met medewerking van de aanbieder (artikelen 126m, 126t en 126zg Sv).

De voorgestelde bevoegdheid is essentieel om de bevoegdheden van politie en justitie in evenwicht te brengen met de ontwikkelingen binnen de digitale wereld. Burgers en bedrijven hebben in korte tijd de beschikking gekregen over een breed scala aan hulpmiddelen waarmee zij ICT toepassingen kunnen integreren in het dagelijks leven, zoals netbooks, tablets en smartphones. Veel mensen hebben niet meer één maar verschillende van deze hulpmiddelen in bezit en gebruiken die vaak successievelijk of zelfs simultaan. Daardoor is het eenvoudig om informatie buiten het bereik van de politie te houden, waardoor de betrokkenheid van personen bij strafbare feiten niet kan worden vastgesteld. Op basis van de huidige bevoegdheden zijn politie en justitie onvoldoende in staat strafrechtelijk effectief hiertegen op te treden. De belangrijkste oorzaken daarvoor zijn beschreven in paragraaf 2.1. Dit betreft de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en het gebruik van web applicaties en Cloudcomputingdiensten.
Met de voorgestelde bevoegdheid kan toegang worden verkregen tot een zeer grote hoeveelheid gegevens van burgers. Dit betreft niet alleen de gegevens die reeds op het geautomatiseerde werk aanwezig zijn maar ook de gegevens die gedurende de looptijd van het bevel worden opgeslagen. Er dienen dan ook afdoende waarborgen te gelden voor een zorgvuldige toepassing van de bevoegdheid, waarbij de inbreuk op de privacy van burgers zoveel mogelijk wordt beperkt. Dit wordt in de volgende paragrafen nader toegelicht.

2.4. De juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid

Gelet op het indringende en heimelijke karakter van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk zijn aan de inzet ervan strikte voorwaarden verbonden. Om in een geautomatiseerd werk binnen te kunnen dringen moet sprake zijn van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Hiermee wordt tot uitdrukking gebracht dat het een zeer ingrijpende bevoegdheid betreft. Dit vereiste geldt ook voor de inzet van bijzondere opsporingsbevoegdheden als de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s en 126zf Sv), het aftappen van communicatie (artikelen 126m, 126t en 126zg Sv) of het vorderen van gevoelige persoonsgegevens, zoals betreffende iemands godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv).

De Afdeling advisering stelt vast dat de voorwaarden om van de voorgestelde bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk gebruik te maken niet differentiëren naar de mate waarin een inbreuk wordt gemaakt op de persoonlijke levenssfeer. Ingeval sprake is

van bijvoorbeeld het bepalen van de identiteit of van de locatie van een geautomatiseerd werk of van de gebruiker, zijn de voorgestelde waarborgen naar het oordeel van de Afdeling passend. Bij het binnendringen met het oog op het aftappen van communicatie of stelselmatige observatie kan eveneens worden volstaan met de voorwaarden zoals voorgesteld. Voor het binnendringen dat het meest ingrijpend is voor de persoonlijke levenssfeer, zoals het doorzoeken van alle gegevens in het geautomatiseerde werk en het overnemen daarvan, acht de Afdeling evenwel aansluiting bij de voorwaarden voor de toepassing van de bijzondere opsporingsbevoegdheid tot opnemen van vertrouwelijke communicatie waarbij een woning wordt binnengedrongen, aangewezen.

Naar aanleiding van het advies van de Afdeling advisering is de voorwaarde voor de inzet van deze bevoegdheid aangescherpt voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens. Daarbij kunnen de gegevens worden doorzicht die in het geautomatiseerde werk worden verwerkt. Voor het verrichten van deze onderzoekshandelingen is de verdenking van een misdrijf vereist waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen, en dat een ernstige inbreuk op de rechtsorde oplevert.
De misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld betreft delicten als de deelneming aan een terroristische organisatie (artikel 140a Sr), het maken van een beroep of gewoonte van het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b, tweede lid, Sr), mensenhandel (artikel 273f, eerste lid, Sr), opzettelijke vrijheidsberoving (artikel 282 Sr), gijzeling (artikel 282a Sr), doodslag (artikel 287 Sr) of moord (artikel 289 Sr).
De bij algemene maatregel van bestuur aan te wijzen misdrijven betreffen misdrijven waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Er is dan vaak geen ander aangrijpingspunt voor de opsporing. Dit betreft misdrijven als het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) de «grooming» (artikel 248e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.

Een belangrijke voorwaarde voor de inzet van de voorgestelde bevoegdheid is dat de officier van justitie een bevel tot onderzoek in een geautomatiseerd werk kan geven na een voorafgaande schriftelijke machtiging van de rechter-commissaris. Het vereiste van een voorafgaande rechterlijke toetsing biedt de burger bescherming tegen willekeurige inmenging door de overheid in zijn privéleven. Tijdens het opsporingsonderzoek zal niet altijd meteen duidelijk zijn of in een geautomatiseerd werk privégegevens zijn opgeslagen, zoals financiële administratie of vakantiefoto's. Net als op fysieke plaatsen kunnen ook in een geautomatiseerd werk veel verschillende soorten gegevens zijn opgeslagen. Het is niet uitgesloten dat tijdens de toepassing van de bevoegdheid kennis wordt genomen van de inhoud van vertrouwelijke communicatie. Het recht op vertrouwelijke communicatie wordt beschermd door artikel 8 van het EVRM en artikel 13 van de Grondwet. Voor een inbreuk op dit recht is een voorafgaande rechterlijke toets

noodzakelijk. De rechter-commissaris dient bij de beoordeling van de vordering van de officier van justitie tot afgifte van een machtiging te toetsen of het bevel aan alle wettelijke eisen voldoet. De machtiging strekt zich dan ook uit over alle onderdelen van het bevel.

Het vereiste van een «dringend onderzoeksbelang» brengt tot uitdrukking dat de inzet van de bevoegdheid voldoet aan de vereisten van proportionaliteit en subsidiariteit. De toetsing van de proportionaliteit hangt af van de concrete omstandigheden van het geval. Daarnaast moet de rechter-commissaris kunnen vaststellen dat de gegevens niet op een minder ingrijpende wijze kunnen worden verkregen, waarbij rekening moet worden gehouden met de gevolgen van de toepassing van de bevoegdheid voor het desbetreffende geautomatiseerde werk en de betrokken personen.

Het bevel van de officier van justitie tot onderzoek in een geautomatiseerd werk dient aan een aantal nauwkeurig omschreven inhoudelijke eisen te voldoen. Deze eisen komen voor een groot deel overeen met de eisen aan het bevel tot de inzet van andere bijzondere opsporingsbevoegdheden. Doel van deze eisen is om de rechter-commissaris in staat te stellen de proportionaliteit en subsidiariteit van de inzet van de bevoegdheid te toetsen. Het is immers van groot belang dat de inbreuk op de persoonlijke levenssfeer van een verdachte of derden zo beperkt mogelijk wordt gehouden. In het bevel van de officier van justitie moeten bepaalde gegevens worden opgenomen. Dit betreft onder meer het misdrijf en de feiten en omstandigheden die ten grondslag liggen aan de verdenking. Zo mogelijk wordt tevens een aanduiding opgenomen met het oog op de identificering van het geautomatiseerde werk. Dit betreft gegevens als het IP-adres, het MAC-adres, het IMEI-nummer, de hardware ID of de User Agent. Van belang is dat het object van het binnentreden voldoende precies kan worden vastgesteld. In de gevallen waarin dit aan de orde is dient ook te worden vermeld dat de gegevens niet in Nederland zijn opgeslagen of vastgelegd of dat dit niet bekend is. Verder moet het technische hulpmiddel worden aangeduid dat wordt ingezet ter uitvoering van de bevoegdheid, zodat kan worden gecontroleerd of deze voorziening aan de eisen voldoet. Voorts dient de tijdsduur van de inzet van de bevoegdheid te worden vermeld en dient zo nauwkeurig mogelijk te worden aangegeven ten aanzien van welk deel van het geautomatiseerde werk aan het bevel uitvoering wordt gegeven. Als het bevel betrekking heeft op de inzet van een afzonderlijke bijzondere opsporings-bevoegdheid, te weten het direct afluisteren, het aftappen van communicatie of de stelselmatige observatie, kunnen in het bevel tevens de gegevens worden opgenomen die in een afzonderlijk bevel voor de toepassing van een dergelijke bevoegdheid moeten worden opgenomen. Er is dan slechts één bevel nodig voor de toepassing van de vorenbedoelde bevoegdheden, waarbij een geautomatiseerd werk op afstand heimelijk is binnengedrongen. In de artikelsgewijze toelichting wordt nader ingegaan op de specifieke eisen waaraan het bevel van de officier van justitie moet voldoen.

Het onderzoek in een geautomatiseerd werk dient tevens te voldoen aan bepaalde procedurele eisen. In de eerste plaats is het binnendringen ter uitvoering van het bevel van de officier van justitie beperkt tot de daartoe aangewezen opsporingsambtenaren van het technische team. Dit betreft de door de korpschef aangewezen en ter zake deskundige opsporings-ambtenaren die over specialistische kennis beschikken op het gebied van de informatie- en communicatietechnologie. Een en ander wordt nader geregeld bij algemene maatregel van bestuur. Dit betreft het Besluit technische hulpmiddelen strafvordering. Aldus kan de kwaliteit en professionaliteit van die inzet worden gewaarborgd.

De opsporingsambtenaren van het technische team behoren niet tot het opsporingsteam dat het tactische onderzoek verricht. Deze functiescheiding, die ook bij de plaatsing van een telefoon-, of internettap gebruikelijk is, vermindert het risico op tunnelzicht. De opsporingsambtenaren van het technische team zijn niet betrokken bij het operationele onderzoek en kunnen daardoor niet worden beïnvloed bij het maken van afwegingen ter zake van de haalbaarheid en de wijze van uitvoering van de onderzoekshandelingen. In het eerdergenoemde Besluit technische hulpmiddelen strafvordering zullen tevens eisen worden gesteld aan de samenwerking met de ambtenaren die zijn belast met de opsporing van strafbare feiten, voor het geval waarin een opsporingsdienst zelf niet beschikt over een technisch team. Wanneer in opsporingsonderzoeken de behoefte bestaat om de bevoegdheid tot onderzoek in een geautomatiseerd werk toe te passen, is de advisering van de officier van justitie omtrent de afweging om in het concrete geval daadwerkelijk een onderzoek in een geautomatiseerd werk te verrichten voorbehouden aan de opsporingsambtenaren van het technische team.
In de tweede plaats zullen nadere eisen worden gesteld aan het technische hulpmiddel (de software) met behulp waarvan onderzoekshandelingen in een geautomatiseerd werk kunnen worden verricht. Hiervoor zal worden aangesloten bij de algemene regeling over technische hulpmiddelen die worden ingezet bij de toepassing van bijzondere opsporingsbevoegdheden, zoals camera's en richtmicrofoons, en de eisen waaraan die hulpmiddelen moeten voldoen. Dit betreft de regeling van artikel 126ee Sv. Deze nadere eisen zijn uitgewerkt in het eerdergenoemde Besluit technische hulpmiddelen strafvordering. Dit besluit zal worden aangevuld met eisen inzake het technische hulpmiddel dat wordt gebruikt voor het verrichten van handelingen in een geautomatiseerd werk. Hierbij moet worden gedacht aan technische eisen waaraan de software moet voldoen, de beveiligingseisen voor het transport van signalen, de controle op het technische hulpmiddel en de verwijdering ervan.
In de derde plaats dient te allen tijde te kunnen worden gecontroleerd welke handelingen al dan niet met behulp van een technisch hulpmiddel in het desbetreffende geautomatiseerde werk hebben plaatsgevonden, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel. Dit betreft de geautomatiseerde vastlegging (logging) van gegevens over de verwerking van gegevens bij het verrichten van handelingen in een geautomatiseerd werk. De eisen die aan de geautomatiseerde vastlegging worden gesteld worden eveneens nader geregeld in Besluit technische hulpmiddelen strafvordering.

Tot slot wordt opgemerkt dat, voor zover het doel van het onderzoek is gelegen in het ontoegankelijk maken van gegevens (artikel 126cc, vijfde en zesde lid Sv), het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie (artikelen 126l, 126m, 126s, 126t, 126zf, 126zg Sv) en de stelselmatige observatie (artikelen 126g, 126o, 126zd Sv), de bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden van toepassing zijn. Hieruit volgt dat de wettelijke voorwaarden waaronder deze bevoegdheden kunnen worden ingezet onverminderd gelden.

2.5. De inzet van de bevoegdheid

In deze paragraaf wordt een feitelijke beschrijving gegeven van de wijze waarop de voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk zal kunnen worden ingezet. De inzet laat zich onderscheiden in verschillende fasen: een verkennende fase waarin het onderzoek in het geautomatiseerde werk wordt voorbereid en eventuele reeds bestaande wettelijke bevoegdheden worden toegepast, de fase waarin het geauto-

matiseerde werk op afstand heimelijk wordt binnengedrongen en (eventueel) een technisch hulpmiddel wordt geplaatst, de fase waarin onderzoekshandelingen in het geautomatiseerd werk worden verricht en een eindfase waarin de inzet van de bevoegdheid wordt beëindigd en het technische hulpmiddel wordt verwijderd.

I De verkennende fase
In een opsporingsonderzoek is het, voorafgaand aan eventuele daadwerkelijke inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk nodig om een goed beeld te verkrijgen van de mogelijkheden om daadwerkelijk toegang te verkrijgen tot het geautomatiseerde werk en de daaraan verbonden risico's. Voor het beoordelen van de risico's is het van groot belang dat de kenmerken van het geautomatiseerde werk zo goed mogelijk in kaart worden gebracht. Hierin verschilt de voorgestelde bevoegdheid niet ten opzichte van andere (bijzondere) opsporingsbevoegdheden. Wanneer bijvoorbeeld de bevoegdheid tot het verrichten van een inkijkoperatie (artikel 126k Sv) of het fysiek plaatsen van een technisch hulpmiddel ter vastlegging van vertrouwelijke communicatie (artikel 126l Sv) wordt ingezet, dan wordt ter voorbereiding van de inzet van die bevoegdheid getracht een zo volledig mogelijk beeld te krijgen van de besloten plaats of woning die moet worden betreden om de bevoegdheid te kunnen toepassen. Voor de daadwerkelijke uitvoering van het onderzoek in een geautomatiseerd werk is het van belang dat bekend is welke programma's zijn geïnstalleerd, welke bestandsmappen er zijn (zodat een technisch hulpmiddel onopvallend kan worden geplaatst), of er meerdere gebruikers zijn, hoe het beheer verloopt, welk besturingsprogramma van toepassing is en wat de risico's zijn. Aan de hand van deze informatie kan een globale inschatting worden gemaakt van de barrières voor het onderzoek in het geautomatiseerde werk, in het bijzonder op het gebied van de beveiliging. Bij de inzet van de voorgestelde bevoegdheid zal dikwijls maatwerk nodig zijn om, afhankelijk van de concrete situatie, de juiste en meest doelgerichte methode ten aanzien van het desbetreffende geautomatiseerde werk te kunnen toepassen. Hierbij wordt informatie verzameld uit open bronnen. Ook kunnen bijzondere opsporingsbevoegdheden worden ingezet, bijvoorbeeld om te proberen inloggegevens te achterhalen.

In de eerste plaats kan het nodig zijn het geautomatiseerde werk of de persoon die van het geautomatiseerde werk gebruik maakt, te identificeren zodat zeker kan worden gesteld dat de voorgestelde bevoegdheid wordt uitgeoefend ten aanzien van het juiste geautomatiseerde werk of de juiste persoon. Dit kan bijvoorbeeld een privécomputer, een smartphone of een server bij een hosting provider betreffen. Ieder geautomatiseerd werk beschikt over eigen technische kenmerken die kunnen worden gebruikt om het te onderscheiden van andere geautomatiseerde werken. Voor het identificeren van het geautomatiseerde werk of van de gebruiker kan gebruik worden gemaakt van de bevoegdheid tot het vorderen van verkeersgegevens (artikelen 126n, 126u en 126zh Sv) of van de bevoegdheid tot het opvragen van gebruikersgegevens (artikelen 126na, 126ua en 126zi Sv). De bevoegdheid tot het aftappen van communicatie (artikelen 126m, 126t en 126zg Sv) kan worden gebruikt om door middel van een internettap in kaart te brengen welk verkeer met het internet via een router van een thuisnetwerk of een zogenaamde openbare «hotspot» is waar te nemen.

De Afdeling advisering heeft opgemerkt dat de voorgestelde bevoegdheid tot binnendringen niet zonder risico is. Het door een verdachte gebruikte geautomatiseerd werk zou een vitale functie kunnen vervullen binnen bijvoorbeeld een ziekenhuis, bank of cruciaal beveiligingssysteem. Zou deze functie bekend zijn dan zou dit waarschijnlijk tot de conclusie leiden

dat de risico's van binnendringen in het desbetreffende werk onaanvaardbaar groot zijn, binnendringen dus achterwege moet blijven. In reactie hierop moet worden opgemerkt dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig zijn in te schatten. Wel komen de risico's soms vollediger in beeld in beeld nadat is binnengedrongen, waarbij uiteraard zoveel mogelijk wordt vermeden dat het functioneren van het betreffende werk wordt belemmerd. De technische risico's die zijn verbonden aan het onderzoek in een geautomatiseerd werk kunnen ook aan de orde komen in het kader van de toetsing van de noodzaak en de proportionaliteit van het onderzoek. Bedacht moet echter worden dat de officier van justitie en de rechter commissaris niet bij uitstek deskundig zijn om de technische risico's te beoordelen. Voor de inschatting, beheersing en beperking van deze risico's is de deskundigheid van de opsporingsambtenaren die worden belast met het binnendringen van essentieel belang.

Voordat een geautomatiseerd werk wordt binnengedrongen kan de geografische locatie daarvan op verschillende manieren worden vastgesteld, bijvoorbeeld door het nagaan van de gegevens van een IP-adres in de database van beheerders als de Internet Cooperation for Assigned Names and Numbers (ICANN). Bij cybercrime is een correcte vermelding van een IP-adres in deze database echter geen vanzelfsprekendheid. Criminelen maken gebruik van diverse technieken om de feitelijke locatie van de gegevens of de identiteit en de locatie van het geautomatiseerd werk en zijn beheerder te verhullen. Soms kan technisch onderzoek uitkomst bieden, bijvoorbeeld door het benutten van zwakheden in de verhullingstechniek of het deconstrueren van de virtualisatieschakels bij dynamische IP-adressen. Aldus kan een virtueel dwaalspoor worden ontrafeld. Daarnaast kan het internetgebruik van een geautomatiseerd werk worden gevolgd en gekoppeld worden aan online-activiteiten van de gebruikers. Dit is echter tijdrovend en belastend voor de persoonlijke levenssfeer van de gebruikers.

Nadat een geautomatiseerd werk is binnengedrongen ontstaan meer mogelijkheden om de locatie ervan te bepalen. Voorbeelden zijn het deconstrueren van de gebruikte verhullingstechniek vanaf het geautomatiseerde werk, het verkrijgen van inzicht in het internetgebruik vanuit of via het werk, of het ontplooien van activiteiten die erop zijn gericht om het geautomatiseerde werk zichzelf te laten identificeren of lokaliseren. Deze mogelijkheden zijn afhankelijk van de aard van het geautomatiseerde werk en het risico van ontdekking door de gebruiker.

Op basis van de vooraf in kaart gebrachte situatie vindt, voorafgaand aan de daadwerkelijke inzet van de bevoegdheid, een uitgebreide afweging plaats van de te bereiken doelen, de beschikbare technieken en middelen (capaciteit en kennis), de mogelijke alternatieve middelen en de risico's die aan de inzet zijn verbonden. Wat betreft de risico's moet worden gedacht aan elementen als: de mate van inbreuk op de persoonlijke levenssfeer van de verdachte(n), de eventuele gevolgen voor de kwetsbaarheid van het systeem waarin de bevoegdheid zou moeten worden toegepast, de kans op ontdekking van de inzet van de software door de betrokkene, de kosten van de inzet en de kans op nadeel of schade bij derden.

Op basis van de informatie van de politie maakt de officier van justitie de afweging voor de afgifte van een bevel tot onderzoek in het geautomatiseerde werk. Het onderzoek kan uitsluitend zijn gericht op het verrichten van onderzoekshandelingen: het toepassen van de maatregel van de ontoegankelijkmaking of het inzetten van bepaalde bijzondere opsporingsbevoegdheden met betrekking tot het geautomatiseerde werk. De officier

van justitie weegt daarbij de invloed van de bevoegdheid op de persoonlijke levenssfeer van de verdachte of derden en de risico's voor het geautomatiseerde zorgvuldig af. De verdere procedure rond het bevel, zoals het voorleggen van het voornemen om het bevel af te geven aan de Centrale Toetsingscommissie en het verkrijgen van een schriftelijke machtiging van de rechter-commissaris, komt in paragraaf 2.6. aan de orde.

II Het onderzoek in een geautomatiseerd werk
Wanneer tijdens de voorfase is bepaald ten aanzien van welk geautomatiseerd werk en welke gegevens of categorieën van gegevens de bevoegdheid van onderzoek in een geautomatiseerd werk moet worden toegepast dan kan, indien aan de juridische voorwaarden daarvoor is voldaan en de risico's zorgvuldig zijn afgewogen, de officier van justitie bepalen dat ter uitvoering van het bevel daadwerkelijk wordt binnengedrongen in het geautomatiseerde werk.

Er zijn verschillende technieken beschikbaar die het mogelijk maken in een geautomatiseerd werk binnen te dringen, en daarbij eventuele beveiligingen te omzeilen. Het aantal verschillende technieken is niet limitatief, en de mate van beveiliging van de verschillende soorten van geautomatiseerde werken vertoont grote verschillen. In de eerste plaats kan worden binnengedrongen met behulp van inloggegevens die door middel van «social engineering» of het gebruik van kunstmatige intelligentie zijn verkregen. In de tweede plaats kunnen inloggegevens van een persoon worden verkregen door diegene te verleiden te reageren op een e-mailbericht of een ander verzoek om contact. Met behulp van deze technieken kan malware worden geplaatst, waardoor de toegang tot een geautomatiseerd werk open wordt gezet en een «bug» of «keylogger kan worden geplaatst. In de derde plaats kunnen kwetsbaarheden in een computer worden geëxploiteerd, zoals het gebruik van fouten of lekken in de software. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd. Zodra een dergelijke kwetsbaarheid wordt opgemerkt kan deze via het internet worden verspreid. Voordat deze informatie wordt verspreid wordt gesproken van een «zero day exploit». De softwarefabrikanten passen voortdurend de software aan om dergelijke kwetsbaarheden op te lossen. Indien de gebruiker de wijzigingen (zogenaamde patches) niet bijhoudt kan gebruik worden gemaakt van een lek in de gebruikte versie van de software.

De Afdeling advisering heeft geadviseerd om in de toelichting nader in te gaan op het risico van systeemzwakte, veroorzaakt door de gebruikte software bij het binnendringen van een geautomatiseerd werk, de mogelijkheden van oneigenlijk gebruik van die software door derden, waaronder de leveranciers. Daarbij zou tevens moeten worden ingegaan op de mogelijkheden om dit oneigenlijke gebruik te voorkomen en de wijze waarop de politie voorafgaand aan de inzet van een technisch hulpmiddel de daaraan verbonden risico's kan beheersen. Voorts is in diverse adviezen, waaronder dat van BoF, gewezen op de risico's van het gebruik van spyware.

Als de politie gebruik maakt van bestaande zwakheden in het systeem is het in theorie mogelijk dat derden deze kwetsbaarheden eveneens gebruiken om binnen te dringen. Niet is uit te sluiten dat derden van diezelfde kwetsbaarheid gebruik maken. Wanneer de politie gebruik maakt van een zwakheid, zal de politie waar mogelijk proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Het open laten van de mogelijkheid tot binnendringen in het systeem door derden tijdens de uitoefening van de bevoegdheid is niet in het belang van het onderzoek, omdat dit afbreuk kan doen aan de betrouwbaarheid van het bewijs. De

politie neemt voorts bij de inzet van de bevoegdheid technische maatregelen om de gegevensstroom onder controle te houden en de integriteit van de bewijsmiddelen te kunnen garanderen. Dit gebeurt door geautomatiseerde vastlegging van de gegevens ter uitvoering van het bevel (logging), waardoor misbruik door derden kan worden onderkend en maatregelen kunnen worden getroffen om dit misbruik te beëindigen. Indien gebruik gemaakt wordt van een technisch hulpmiddel moet het onder meer een functie bevatten die het functioneren van het technische hulpmiddel tijdens de inzet ervan technisch vastlegt.
Verschillende adviesorganen hebben erop gewezen dat de politie belang heeft bij het geheimhouden van lekken in de beveiliging van geautomatiseerde werken, om de mogelijkheid van binnendringen te vereenvoudigen. Ook in de internetconsultatie is hierop gewezen. Dit zou de overheid een perverse prikkel geven om informatie over kwetsbaarheden (zogenaamde «exploits») voor zichzelf te houden. In reactie hierop moet worden opgemerkt dat de politie streeft naar een veiliger Nederland en geen belang of baat heeft bij de instandhouding van onbeveiligde systemen, gelet op de maatschappelijke kosten die hiermee gepaard gaan De politie moedigt burgers en bedrijven juist aan hun systemen en gegevens goed te beveiligen door besturingssystemen en programma's actueel te houden, gebruik te maken van beveiligde verbindingen voor belangrijke zaken en zelfs door gegevens te versleutelen zodat zelfs wanneer een cybercrimineel weet binnen te komen, hij weinig of niets van waarde aantreft op het binnengedrongen systeem.
Overigens is het gebruik van kwetsbaarheden in de beveiliging van een computer door de politie in de praktijk lastig, omdat de beveiligingssoftware voortdurend wordt aangepast en up to date wordt gehouden. Het gebruik van exploits door de politie is niet alleen buitengewoon kostbaar maar ook riskant omdat de kwetsbaarheid zeer snel kan zijn opgelost.
Zodra in het geautomatiseerde werk is binnengedrongen kunnen bepaalde onderzoekshandelingen worden verricht. Deze onderzoekshandelingen kunnen handmatig dan wel met behulp van een technisch hulpmiddel worden verricht, in de vorm van een softwareapplicatie. Gezien de technische ontwikkelingen zal naar verwachting in de toekomst steeds meer gebruik worden gemaakt van software. De software die in deze fase wordt gebruikt kan verschillende functionaliteiten hebben waarmee de in het voorgestelde artikel 126nba, eerste lid, Sv omschreven doelen kunnen worden bereikt. Het bevel van de officier van justitie dient een aanduiding te bevatten van de functionaliteiten die zullen worden ingeschakeld, afhankelijk van het met het onderzoek te bereiken doel. Afhankelijk van het te bereiken doel zullen de in het bevel aangegeven functionaliteiten worden ingeschakeld. Daarvoor kan worden gedacht aan functionaliteiten als het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen of het doorzoeken van bepaalde bestandsmappen. Andere functionaliteiten worden niet ingeschakeld en geïnstalleerd in het geautomatiseerde werk waarin het onderzoek plaatsvindt. De Afdeling advisering heeft er op gewezen, met verwijzing naar een advies van BoF over het wetsvoorstel, dat de toelichting niet ingaat op ervaringen in Duitsland met de Finfisher software en dat zowel in Duitsland als in Frankrijk zou zijn afgezien van het gebruik van spyware, omdat oneigenlijk gebruik door derden en de politie niet viel uit te sluiten. In reactie hierop kan worden opgemerkt dat een voorafgaande keuring van het technische hulpmiddel is vereist, voordat dit wordt ingezet. Met de keuring kan worden voorkomen dat softwareapplicaties worden ingezet die niet voldoen aan de daaraan te stellen eisen. De ervaringen met bepaalde softwareapplicaties in andere landen onderstrepen het belang van een zorgvuldige keuring. De eisen rond de keuring zullen worden uitgewerkt in het Besluit technische hulpmiddelen strafvordering.

III De afsluiting van het onderzoek in een geautomatiseerd werk
Zodra het doel van het onderzoek in het geautomatiseerde werk is bereikt, of wanneer de geldigheidsduur van het bevel is verlopen, wordt het onderzoek beëindigd. Indien een technisch hulpmiddel is geplaatst dan wordt dit zoveel mogelijk verwijderd. Het verwijderen gebeurt door het technische team. De ambtenaren die betrokken zijn bij het tactische opsporingsonderzoek kunnen geen invloed uitoefenen op de verwijdering van het technische hulpmiddel. Sommige programma's bieden de functionaliteit van een zelfstandige vernietiging van de software na verloop van een bepaalde, vooraf ingestelde, periode. Nadat het technische hulpmiddel is verwijderd zal de server aan de zijde van de politie geen gegevens meer kunnen ontvangen. Er kunnen echter sporen van het middel in het geautomatiseerde werk achterblijven. Deze sporen kunnen het gevolg zijn van de invloed van het geïnstalleerde technische hulpmiddel op het geautomatiseerde werk, of van handelingen die door het technische team zijn uitgevoerd om het technische hulpmiddel te plaatsen of te verwijderen. In alle gevallen zal zoveel mogelijk worden geprobeerd het geautomatiseerde werk in de oorspronkelijke staat achter te laten, dat wil zeggen als ware de bevoegdheid nooit toegepast.
In sommige gevallen kan worden afgezien van de verwijdering van geïnstalleerde software of het ongedaan maken van de in het geautomatiseerde werk aangebrachte wijzigingen. Hierbij moet worden gedacht aan zwaarwegende belangen die zich verzetten tegen het verwijderen, zoals de situatie dat het verwijderen aanzienlijke risico's met zich mee brengt voor het systeem waarin het technische hulpmiddel is geïnstalleerd. Deze risico's worden in de hiervoor beschreven voorfase zoveel mogelijk in kaart gebracht en de officier van justitie wordt hierover door het technische team geïnformeerd. Wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk.
Van de handelingen die door het technische team in het kader van het onderzoek in het geautomatiseerde werk worden verricht en hun bevindingen, wordt overeenkomstig de algemene verplichting die is neergelegd in artikel 152 Sv proces-verbaal opgemaakt. Hierdoor is de inzet van de voorgestelde bevoegdheid controleerbaar.

De Afdeling advisering heeft geadviseerd in te gaan op de waarborgen van stopzetting van het dataverkeer door de politie en het risico dat derden van de niet verwijderde software gebruik kunnen maken. Tevens heeft de Afdeling geadviseerd een verplichting op te nemen tot het verstrekken van technische gegevens aan de hand waarvan het voor de beheerder van het geautomatiseerde werk mogelijk wordt om de in het kader van het onderzoek geïnstalleerde software te verwijderen.
In reactie hierop kan worden opgemerkt dat de politie het geautomatiseerde werk na beëindiging van de bevoegdheid zoveel mogelijk dient achter te laten in een staat als ware de bevoegdheid niet uitgeoefend. De politie heeft geen belang bij het achterblijven van gegevens omdat de gebruiker hierdoor vroegtijdig op de hoogte zou kunnen raken van het feit dat derden op afstand heimelijk zijn binnengedrongen en de nodige inspanningen zal verrichten om de software volledig te verwijderen. Tevens zou achtergelaten software of sporen daarvan de basis kunnen vormen voor onderzoek naar de werking van middelen van de politie, waar de politie belang heeft van de voorgezette afscherming daarvan. De politie zal daarom de nodige inspanning verrichten om zowel de software als sporen daarvan volledig te verwijderen.
Indien het niet mogelijk is om (sporen van) de software te verwijderen, bijvoorbeeld omdat het geautomatiseerde werk niet meer is verbonden met het internet, en het achterblijven van (de sporen van) die software een risico oplevert voor het functioneren van het geautomatiseerde werk

stelt de officier van justitie de beheerder van het geautomatiseerde werk daarvan in kennis en stelt de nodige informatie ter beschikking ten behoeve van de volledige verwijdering van de (sporen van de) software. Het feit dat (sporen van) software aanwezig blijft op een geautomatiseerd werk betekent niet dat derden daarvan gebruik kunnen maken. Bij algemene maatregel van bestuur worden eisen gesteld aan een technisch hulpmiddel met het oog op voorkoming van misbruik door derden, waarbij onder meer kan worden gedacht aan het beveiligen van het gebruik van de software.
Niet uit te sluiten is dat tijdens het onderzoek door het gebruik van de software veranderingen in het geautomatiseerde werk optreden. Doordat alle technische handelingen die door de opsporingsambtenaren van het technische team worden verricht, worden gelogd en deze handelingen bovendien hun weerslag vinden een proces-verbaal, is achteraf altijd controle mogelijk op de integriteit van de werking van het technische hulpmiddel en van de informatie die met behulp daarvan is vergaard, zonder dat gevoelige informatie over de methode zelf wordt prijs gegeven. Op deze manier is het mogelijk om de ter terechtzitting gevoerde verweren over de integriteit van het verzamelde bewijsmateriaal te toetsen.

Vanwege het vereiste van de keuring van de software is het niet waarschijnlijk dat in het geautomatiseerde werk, waarin op afstand heimelijk is binnengedrongen, schade zal ontstaan. Als er onverhoopt schade zou ontstaan ten gevolge van het onderzoek in een geautomatiseerd werk, dan kan de benadeelde de schade verhalen op de Staat der Nederlanden op grond van onrechtmatige daad (artikel 6:162 Burgerlijk Wetboek). Ook kan men terecht bij het arrondissementsparket of het Parket-Generaal, die verzoeken om schadevergoeding afhandelen op basis van de civielrechtelijke jurisprudentie of uit coulance, en daarmee in de praktijk als «voorportaal» van de burgerlijke rechter fungeren.
Overigens ben ik voornemens een eenvormige algemene regeling voor schadevergoeding in het wetboek op te nemen. Met het oog hierop wordt thans een impactanalyse uitgevoerd die beoogt de gevolgen van verschillende scenario's in kaart te brengen. Hiervoor kan worden verwezen naar de nota met een schets van de hoofdlijnen van het gemoderniseerde wetboek («Contourennota Modernisering Wetboek van Strafvordering»), die inmiddels aan de Kamer is aangeboden (Kamerstukken I 2015/16, 33 750 VI, AF).

2.6. De toetsing van de inzet van de voorgestelde bevoegdheid

De voorgenomen inzet van de bevoegdheid tot onderzoek in een geautomatiseerd werk zal door de officier van justitie aan de Centrale Toetsingscommissie (CTC) worden voorgelegd. De CTC is samengesteld uit leden van het OM en de politie en is een intern adviesorgaan van het OM. De CTC adviseert het College van procureurs-generaal (hierna ook te noemen: het College) over de voorgenomen inzet van een aantal bijzondere opsporingsbevoegdheden en methodieken. Op deze wijze wordt voor een aantal ingrijpende opsporingsbevoegdheden daadwerkelijk invulling gegeven aan de beginselen van proportionaliteit en subsidiariteit en een landelijk beleid ontwikkeld. De officier van justitie heeft de toestemming nodig van het College voordat bepaalde opsporingsbevoegdheden worden toegepast. Dit betreft bevoegdheden als de infiltratie, de burgerpseudokoop- of dienstverlening, het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel in een woning en toezeggingen aan getuigen in strafzaken.
De inzet van de bevoegdheid wordt getoetst aan de wet- en regelgeving, de jurisprudentie, de proportionaliteit en subsidiariteit en de afbreukrisico's. Voorts worden de effectiviteit van de bevoegdheid en het afbreuk-

risico afgewogen tegen het belang van de hantering van een bevoegdheid in het concrete geval. Deze afwegingen kunnen voor een aantal opsporingsbevoegdheden beter centraal dan op regionaal niveau worden gemaakt. De CTC legt haar advies voor aan het College van procureurs-generaal. Het College brengt periodiek verslag aan mij uit over het aantal ter toetsing en registratie aangeboden (bijzondere) opsporingsbevoegdheden.
De centrale toetsing van het onderzoek in een geautomatiseerd werk vergt geen wetswijziging. De toetsing berust op de interne gezagsverhoudingen binnen het OM en kan door het College worden voorgeschreven. In de Aanwijzing opsporingsbevoegdheden van het College van procureurs-generaal van 1 juni 2012 (registratienummer 2012A012) zijn de gevallen vermeld waarin een verplichte toetsing door de CTC dient plaats te vinden. Het College zal worden verzocht om de voorgestelde bevoegdheid, zodra deze kracht van wet heeft gekregen, op te nemen in de lijst van bevoegdheden waarvoor geldt dat deze aan de CTC voorgelegd moeten worden. De Aanwijzing opsporingsbevoegdheden zal worden aangepast zodat ook de voorgenomen inzet van het onderzoek in een geautomatiseerd werk aan de CTC zal moeten worden voorgelegd.

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

voor de toepassing van de bevoegdheid nodig is dat op afstand heimelijk wordt binnengedrongen in het geautomatiseerde werk.

Ten behoeve van de controleerbaarheid van de onderzoekshandelingen zal aan een aantal eisen moeten worden voldaan, zodat de authenticiteit en integriteit van de gegevens is gewaarborgd. Dit is mogelijk door de logging van de gegevens ter uitvoering van het bevel op een bepaalde wijze vorm te geven. Dit wordt geregeld in het Besluit technische hulpmiddelen strafvordering. Met behulp van de op deze wijze verzamelde gegevens kan de uitvoering van de bevoegdheid in voorkomende gevallen worden gecontroleerd.

De opsporingsambtenaar maakt van door hem verrichte handelingen ten spoedigste proces-verbaal op (artikel 152 Sv.)

Voor een adequate toetsing van de inzet van deze bevoegdheden is het van belang dat de politie, het OM en de rechterlijke macht over voldoende kennis beschikken op het gebied van de informatie- en communicatietechnologie en de opsporing, vervolging en afdoening van computercriminaliteit. Bij de politie is voor degenen die worden belast met de daadwerkelijke uitvoering van het onderzoek in een geautomatiseerd een hoog niveau van expertise en vaardigheden een vereiste om te kunnen worden aangewezen als opsporingsambtenaar die wordt belast met het onderzoek in een geautomatiseerd werk. Ook het Besluit technische hulpmiddelen strafvordering bevat verschillende regelingen die die inhoud van de expertise en de benodigde vaardigheden nader bepalen. Voor de tactische rechercheurs, zeker als zij bij het Team High Tech Crime van de landelijke recherche werken, wordt de kennis en kunde op het gebied van de toepassing van deze bevoegdheden in het specifieke opleidingstraject van het team opgenomen. Ook voor de rechercheurs die werken in het vakgebied van de digitale expertise zullen de nieuwe bevoegdheden in de bestaande opleidingen worden opgenomen.

Het OM organiseert voor de officieren van justitie en voor parketsecretarissen gericht bijscholingscursussen. Een actualiteitencursus voor computercriminaliteit is één van die cursussen. De cursussen zullen worden bijgesteld naar aanleiding van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk. Daarnaast heeft het OM expertise over de strafrechtelijke inzet tegen computercriminaliteit centraal ondergebracht bij het landelijk parket. De officieren van justitie en medewerkers van het landelijk parket fungeren als expertisecentrum voor het OM. Bij ieder regioparket is verder een zogenaamde cybercrime officier van justitie benoemd die, in nauw contact met collega's en het landelijk parket, een spil is in de aanpak van computercriminaliteit.

Voor de zittende magistratuur is bij het Gerechtshof te 's-Gravenhage een kenniscentrum voor computercriminaliteit opgericht. In samenwerking met de SSR heeft het Kenniscentrum Cybercrime een cursus speciaal voor de zittende magistratuur ontwikkeld. In deze cursus wordt speciale aandacht besteed aan de nieuwste ontwikkelingen op het gebied van computercriminaliteit, digitale opsporing en digitaal bewijs. Daarbij zullen de actualiteiten van het afgelopen jaar een belangrijke rol spelen. Ook kunnen een aantal rechters (en officieren van justitie) deelnemen aan door de ERA (Europaïsche Rechts Akademie), gevestigd in het Duitse Trier, georganiseerde seminars over «Basic training in the legal and technical aspects of cybercrime for judges and prosecutors».

Op grond van de algemene regels van Titel VD van het Wetboek van Strafvordering met betrekking tot de toepassing van bijzondere opsporingsbevoegdheden geldt een verplichting tot kennisgeving van de

uitoefening van de bevoegdheid van het onderzoek in een geautomatiseerd werk aan de betrokkene, zodra het belang van het onderzoek dat toelaat. Dit betreft de zogenaamde notificatieplicht (artikel 126bb Sv). Op grond van deze verplichting dient de betrokkene in kennis te worden gesteld van het feit dat op afstand heimelijk is binnengedrongen in een geautomatiseerd werk en van de daarbij toegepaste bevoegdheid waarvoor op grond van artikel 126bb Sv reeds een notificatieplicht geldt. Hierdoor kan de betrokkene op de hoogte komen van de toepassing van de bevoegdheid als onderzoek in het geautomatiseerde werk leidt tot de vastlegging of ontoegankelijkmaking van gegevens of tot het opnemen van gegevens. De betrokkene is doorgaans de verdachte.
De mededelingsplicht bestaat ten opzichte van de burger op wiens rechten inbreuk wordt gemaakt. Niet uitgesloten is dat een geautomatiseerd werk bij meerdere personen in gebruik is. Als de vastlegging van gegevens betrekking heeft op gegevens van een ander dan dient ook de verantwoordelijke voor die gegevens te worden genotificeerd. De mededeling moet schriftelijk geschieden. De mededeling behoeft geen uitputtende opgave van alle vastgelegde of ontoegankelijk gemaakte gegevens te bevatten. Volstaan kan worden met een aanduiding van de aard van de betrokken gegevens, dat wil zeggen met een globale aanduiding, die de betrokken persoon in staat stelt te beoordelen of zijn rechten (naar zijn oordeel) zijn geschonden (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 52).
Het onderzoek in een geautomatiseerd werk wordt heimelijk verricht. Het belang van het onderzoek kan ertoe nopen dat de mededeling wordt uitgesteld. Deze mogelijkheid zal ook gelden voor onderzoek in een geautomatiseerd werk. Uitstel van de mededeling kan aan de orde zijn bij een onderzoek in een andere strafzaak of bij een onderzoek tegen meerdere verdachten dat deels afgerond is.
Conform de werkwijze bij het aftappen van communicatie zal jaarlijks aan de Kamer worden gerapporteerd over de inzet van de bevoegdheid (Kamerstukken II 2007/08, 30 517, nrs. 5 en 6). Dit betreft het aantal malen dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid.

2.7. De wettelijke regelingen in buurlanden (België, Duitsland en Frankrijk).

In België is met de Wet inzake informatiecriminaliteit (Wet van 28 november 2000, Belgisch Staatsblad, 3 februari 2001, nr. 2909) de zoeking in informatiesystemen geregeld. De wet introduceerde in het Belgische Wetboek van Strafvordering (BSv) bepalingen met betrekking tot het onderzoek in informaticasystemen die een sterke verwantschap hebben met de inbeslagneming van voorwerpen. Zo is niet alleen het door de overheid kopiëren van gegevens die in een informaticasysteem zijn opgeslagen geregeld, maar ook het waarborgen van de integriteit van de gekopieerde gegevens en het ontoegankelijk maken van gegevens die een relatie hebben met strafbare feiten (artikel 39bis BSv). In artikel 88ter BSv is bepaald dat de onderzoeksrechter in bepaalde gevallen kan bepalen dat de zoeking in een informaticasysteem of in een deel ervan wordt uitgebreid naar een informaticasysteem of een deel daarvan dat zich op een andere plaats bevindt. In de eerste plaats moet het gaan om de noodzakelijkheid om de waarheid aan het licht te brengen ten aanzien van het misdrijf dat het voorwerp uitmaakt van de zoeking. In de tweede plaats kan uitbreiding van de zoeking alleen plaatsvinden indien andere maatregelen disproportioneel zouden zijn, of indien er een risico bestaat dat zonder deze uitbreiding bewijselementen verloren gaan. Deze twee eisen zijn cumulatief. Voorts stelt artikel 88ter BSv de eis dat de uitbreiding van de zoeking in een informaticasysteem zich niet verder mag

uitstrekken dan tot de informaticasystemen of de delen daarvan waartoe de personen die gerechtigd zijn het onderzochte informaticasysteem te gebruiken, in het bijzonder toegang hebben. Deze eis komt overeen met de Nederlandse bevoegdheid tot de netwerkzoeking, neergelegd in artikel 125j Sv. Wanneer het nuttig is om bij een dergelijke zoeking gegevens te kopiëren, zijn de regels van artikel 39bis BSv van toepassing.

Uit de beperking van de hiervoor beschreven reikwijdte van de zoeking in informaticasystemen waarmee het informaticasysteem van waaruit de zoeking is begonnen in verbinding staat, volgt dat de Belgische wetgever het op afstand heimelijk binnendringen van een geautomatiseerd werk door de overheid uitdrukkelijk uitsluit. Het is overheidsdiensten dan ook verboden om via de eigen informatiesystemen binnen te dringen in andere systemen die niet openstaan voor het publiek en die ervan worden verdacht te worden aangewend voor criminele doeleinden (T. Incalza, «Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming», uit: Jura Falconis Jg. 47, 2010/11, nummer 2, blz. 348). Daarentegen stellen Belgische wetenschappers «dat deze beperking niet noodzakelijk de onmogelijkheid inhoudt voor overheidsdiensten om hun primaire netwerkzoeking verder te zetten op eigen informaticasystemen, bijvoorbeeld wanneer zij beschikken over de gebruikersnaam en het wachtwoord van een Hotmailaccount, mits het tegendeel het onderzoek nodeloos zou bemoeilijken zonder dat sprake is van een verregaande inbreuk op het privéleven van de betrokkene» (T. Incalza, «Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming», Jura Falconis Jg. 47, 2010/11, nummer 2, blz. 353). Dit betekent dat wanneer opsporingsambtenaren via technieken als «social engineering» (het ontfutselen van informatie) een wachtwoord bemachtigen, hiermee onder een valse hoedanigheid of met behulp van een valse sleutel toegang kan worden verkregen tot een geautomatiseerd werk. Ook is denkbaar dat een wachtwoord vrijwillig door een systeembeheerder van een geautomatiseerd werk aan opsporingsambtenaren wordt gegeven, in welk geval sprake is van toestemming om de bevoegdheid tot het onderzoeken van een geautomatiseerd werk toe te passen. Het binnendringen van een geautomatiseerd werk door middel van een technische ingreep of het doorbreken van een beveiliging, bijvoorbeeld door de firewall uit te schakelen, lijkt daarmee uitgesloten.

In de Duitse nationale wetgeving is een bevoegdheid opgenomen die de Duitse Bondsrecherchedienst («Bundeskriminalamt») de mogelijkheid geeft om zich ter bestrijding van terrorisme onder bepaalde voorwaarden heimelijk met behulp van technische middelen toegang te verschaffen tot informatiseringsystemen en daaruit gegevens te verkrijgen (§ 20k BKAG). Dit betreft de zogenaamde «Verdeckter Eingriff in informationstechnische Systeme». Deze nationale regeling is tot stand gekomen naar aanleiding van een uitspraak van het Duitse Bundesverfassungsgericht (BVerfG) van 27 februari 2008 (1 BVR 370/07 en 1 BvR 595/07), waarin het BVerfG heeft geoordeeld dat een in de Duitse deelstaat Nordrhein-Westfalen aangenomen wet, die de opsporingsautoriteiten de bevoegdheid gaf voor het heimelijk op afstand doorzoeken van computers van verdachten, ongrondwettig is. Het BVerfG oordeelde dat een heimelijke infiltratie van een computersysteem alleen is toegestaan als er aanwijzingen zijn voor een concreet gevaar voor een belangrijk rechtsgoed, zoals gevaar voor leven of de vrijheid van een persoon of het staatsbelang. Ook is volgens het BVerfG een rechterlijke machtiging vereist.

Op grond van de Duitse regeling gelden strikte eisen voor de toepassing. De regeling mag alleen worden toegepast als sprake is van 1) lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen of 2) van gemeen gevaar voor goederen, dat een bedreiging oplevert voor het

voortbestaan van de staat of de mensheid. Voorts mag de opsporingsbevoegdheid alleen worden toegepast als wordt voldaan aan de in de wet neergelegde procedurele eisen. Zo mogen in het geautomatiseerde werk slechts de handelingen worden verricht die noodzakelijk zijn voor het vastleggen van gegevens en moeten de veranderingen die daardoor in het geautomatiseerde werk teweeg zijn gebracht na afloop van het toepassen van de bevoegdheid weer ongedaan worden gemaakt. Voorts moeten de vastgelegde gegevens (technisch) beveiligd worden tegen onbevoegd gebruik alsmede tegen onbevoegde toegang, verwijdering en kennisname van de gegevens. Aan iedere inzet van technische hulpmiddelen worden eisen gesteld. Zo moeten onder meer het tijdstip van de inzet van het technische hulpmiddel en de kenmerken van het geautomatiseerde werk waaraan onderzoek wordt verricht worden geregistreerd. De bevoegdheid mag slechts op verzoek van de voorzitter van de Duitse Bondsrecherchedienst en na toestemming van de rechtbank worden ingezet. Aan het bevel van de officier van justitie worden enkele formele eisen gesteld. Het bevel is maximaal drie maanden geldig en kan telkens voor drie maanden worden verlengd. Het is niet toegestaan om de bevoegdheid in te zetten als door de vastlegging van gegevens kennis wordt genomen van de levensovertuiging van de betrokkene. Worden dergelijke gegevens tijdens de inzet van de bevoegdheid wel vastgelegd, dan mogen zij niet worden gebruikt en moeten zij worden vernietigd.

Ook Frankrijk kent een wettelijke regeling die toestaat dat, wanneer de behoefte aan informatie met betrekking tot een ernstig misdrijf dit vereist, heimelijk een technisch hulpmiddel wordt geïnstalleerd met het doel toegang te verkrijgen tot elektronische gegevens, deze op te slaan, te bewaren en over te dragen «zoals zij op het scherm te zien zijn voor de gebruiker van een geautomatiseerd systeem voor het verwerken van gegevens of zoals hij ze daarin invoert door het invoeren van tekens». Aan deze regeling zijn bepaalde voorwaarden verbonden. Zo is een gemotiveerde beslissing van de rechter-commissaris vereist en dient – op straffe van nietigheid – een nauwkeurige omschrijving te worden gegeven van het strafbare feit dat het inzetten van de maatregel rechtvaardigt, van de exacte locatie of van de gedetailleerde omschrijving van de geautomatiseerde systemen voor het verwerken van gegevens alsmede van de duur van de maatregel. Het op elektronische wijze aanbrengen en verwijderen van het technische middel gebeurt op gezag en onder toezicht van de rechter-commissaris. De door de rechter-commissaris aangewezen opsporingsambtenaar maakt een proces-verbaal op van elke plaatsing van een technisch hulpmiddel en van alle afgetapte elektronische gegevens. In dit proces-verbaal staan de datum en het tijdstip vermeld waarop de technische actie is aangevangen en beëindigd. In het proces-verbaal wordt voorts een beschrijving gegeven van de gegevens die van nut zijn voor de waarheidsvinding. Geen enkele passage met betrekking tot het privéleven die niets te maken heeft met de strafbare feiten als omschreven in de machtiging voor de maatregel mag in het onderzoeksdossier worden bewaard.

2.8. Onderzoek in een geautomatiseerd werk en rechtsmacht

2.8.1. Inleiding
Met behulp van het internet kunnen gegevens eenvoudig over grote afstanden worden verzonden. Vanwege de afwezigheid van grenzen in cyberspace en op het op anonimiteit, en daarmee op het niet achterhalen van een geografische plaats, gerichte internetgedrag van bepaalde personen komt het zeer geregeld voor dat politie en justitie niet kunnen vaststellen op welke fysieke locaties gegevens zijn opgeslagen, worden verwerkt of overgedragen terwijl de gegevens als zodanig wel kenbaar en benaderbaar zijn. Dit wetsvoorstel voorziet in de bevoegdheid tot

onderzoek in een geautomatiseerd werk. Niet uitgesloten is dat de gegevens, waartoe toegang kan worden verkregen, opgeslagen zijn op een server die zich in een ander land bevindt. Bij onderzoek in een geautomatiseerd werk is het vraagstuk van de extraterritoriale rechtsmacht dan ook aan de orde. Dit geldt overigens ook voor de bestaande bevoegdheden van de doorzoeking ter vastlegging van gegevens en de netwerkzoeking. Met de ontwikkeling van Cloudcomputingdiensten is het belang van dit vraagstuk toegenomen. Het begrip rechtsmacht omvat twee componenten: de toepasselijkheid van de Nederlandse wet (wetgevende rechtsmacht) en het verrichten van handelingen door Nederlandse rechtshandhavingsautoriteiten met het oog op opsporing en vervolging in Nederland (uitvoerende rechtsmacht). Deze begrippen hangen met elkaar samen: uitvoerende rechtsmacht veronderstelt wetgevende rechtsmacht.

Centrale grondslag voor wetgevende rechtsmacht is het territorialiteitsbeginsel, op grond waarvan de Nederlandse strafwet toepasselijk is op een ieder die zich in Nederland aan enig strafbaar feit schuldig maakt (artikel 2 Sr). Daarnaast is er het personaliteitsbeginsel, dat rechtsmacht verbindt aan de nationaliteit van de pleger (actief personaliteitsbeginsel) of het slachtoffer (passief nationaliteitsbeginsel). De Nederlandse strafwet is eveneens toepasselijk op de Nederlander die zich buiten Nederland schuldig maakt aan bepaalde strafbare feiten (artikelen 6 en 7 Sr). Verder is er sprake van het universaliteitsbeginsel dat voorziet in de meest ruime grondslag voor het uitoefenen van rechtsmacht, namelijk ongeacht waar en door wie een strafbaar feit is gepleegd.

Een gemeenschappelijk kenmerk van de verschillende vormen van computercriminaliteit, door middel waarvan Nederlandse rechtsbelangen worden geraakt, is dat het zich vaak gedeeltelijk in Nederland voordoet. Op grond van de jurisprudentie wordt aangenomen dat een feit op het Nederlandse grondgebied is gepleegd als er een aanknopingspunt is met Nederland. De Hoge Raad heeft recent geoordeeld dat op grond van artikel 2 Sr vervolging van de ook ten aanzien van dat feit deel uitmakende gedragingen die buiten Nederland hebben plaatsgevonden mogelijk is, indien naast in ook buiten Nederland gelegen plaatsen kunnen gelden als plaats waar een strafbaar feit is gepleegd (HR 02 februari 2010, NJ 2010, 89 en Rb Breda 16-10-2007, BB5936). Juist bij het plegen van computercriminaliteit is het betrekkelijk eenvoudig om delicten te plegen waarbij andere jurisdicties betrokken zijn. Dit kan betrekking hebben op zowel de daders (phishing door Nigeriaanse bendes) als de slachtoffers (het verspreiden van kinderpornografie). In de gevallen waarin kan worden aangenomen dat Nederland op grond van de artikelen 2 tot en met 8 Sr over wetgevende rechtsmacht beschikt, voorziet artikel 539a Sv in een wettelijke basis om opsporingshandelingen te verrichten buiten Nederland, voor zover het volkenrecht en interregionale recht dit toelaten. Er is dan ook uitvoerende rechtsmacht.

Bij het toepassen van dwangmaatregelen jegens personen (zoals arrestatie voor verhoor, inverzekeringstelling of huiszoeking) ligt zelfstandig optreden door een handhavende staat minder voor de hand omdat de betreffende persoon niet op het grondgebied van die staat aanwezig is. Het optreden van de handhavende staat is dan niet mogelijk zonder hulp van de staat waar de dader zich bevindt of waar uitvoeringshandelingen hebben plaatsgevonden. In een dergelijk geval is een verzoek om rechtshulp aangewezen. Dit betekent dat de aangezochte staat door de verzoekende staat wordt verzocht om bepaalde opsporingshandelingen te verrichten ten behoeve van het opsporingsonderzoek of de strafvervolging in de verzoekende staat of dat de aangezochte staat ermee instemt dat de verzoekende staat opsporingshandelingen verricht op zijn

grondgebied. Een rechtshulpverzoek heeft betrekking op het respecteren van de soevereiniteit en de territoriale integriteit van de andere staat en de toepasselijkheid van de eigen wetgeving op dat grondgebied, evenals de bevoegdheid van de andere staat om zelf op te treden tegen inbreuken op de rechtsorde die op het eigen grondgebied worden beraamd of gepleegd. Uitgangspunt is dat rechtshulp wordt gevraagd als bekend is dat de gegevens zich op het grondgebied van een andere staat bevinden, bijvoorbeeld als de gegevens zijn opgeslagen op een server op het territorium van die andere staat. Een verzoek om rechtshulp kan, afhankelijk van de rechtshulprelatie met het desbetreffende land, mondeling of schriftelijk worden gedaan.

Vanwege de dikwijls ruime regelingen van wetgevende rechtsmacht in andere landen is het bepaald niet uitgesloten dat meerdere staten rechtsmacht hebben bij de opsporing en vervolging van vormen van computercriminaliteit waar meerdere staten bij zijn betrokken. Als staten dat van elkaar weten, ligt het in de rede dat zij onderling overleggen over de meest geschikte manier en jurisdictie om het concrete geval aan te pakken. De praktijk wijst dat ook uit. De botnets vormen een goed voorbeeld van situaties waarin meerdere staten rechtsmacht kunnen hebben en die ook zouden willen uitoefenen, omdat de schadelijke gevolgen van het gebruik van dergelijke botnets zich in een groot aantal staten kunnen manifesteren.

2.8.2. Ontwikkelingen in het internationale recht
Het Cybercrime Verdrag van de Raad van Europa bevat een specifieke regeling voor de grensoverschrijdende toegang tot computergegevens. Ook in dit verdrag wordt ervan uitgegaan dat de verdragspartijen nader overleg voeren in het geval van overlappende rechtsmacht (Article 22(5): When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution). In een tweetal situaties is de grensoverschrijdende toegang tot gegevens mogelijk. Dit betreft in de eerste plaats de toegang tot openbare gegevens (uit open bronnen) die zijn opgeslagen, ongeacht de locatie van de gegevens (artikel 32, onderdeel a, van het Cybercrime Verdrag). Dit betreft in de tweede plaats de toegang, door middel van een netwerkzoeking, tot opgeslagen gegevens in een andere verdragspartij, met de rechtmatige en vrijwillige instemming van de persoon die gerechtigd is de gegevens via het computersysteem aan de partij te verstrekken (artikel 32, onderdeel b, van het Cybercrime Verdrag). Degene die gerechtigd is in te stemmen is niet uitsluitend de verdachte of een andere individuele persoon, het kan ook de aanbieder zijn van een dienst. Bij de onderhandelingen konden de verdragspartijen aan het eind van de vorige eeuw niet tot overeenstemming komen over voorwaarden waaronder in andere situaties grensoverschrijdende toegang tot gegevens mogelijk is. In het Cybercrime Verdrag ligt het accent dan ook op de wederzijdse bijstand. Hoewel het meer principiële punt van de bescherming van de soevereiniteit ook toen reeds aan de orde was, werd de mate waarin dit in de praktijk voor de opsporing tot problemen zou leiden, destijds niet voorzien. De enorme groei van het gebruik van steeds kleinere en krachtiger computers, zoals smartphones en tablets, de opkomst van de zogenaamde webbased applicaties en Cloud computing en het gebruik van anonimisering- en versleutelingstechnieken hebben inmiddels een grote vlucht genomen.
Vanwege de beperkingen van de regeling van het Cybercrime Verdrag wordt in de Raad van Europa verder gesproken over de verhouding tussen het grensoverschrijdend vastleggen van gegevens en de uitvoerende rechtsmacht. Inmiddels is door een werkgroep van de Raad van Europa, de zogenaamde Transborder Group, een rapport uitgebracht over

jurisdictie en grensoverschrijdende toegang tot gegevens (Trans border access and jurisdiction: What are the options?, Report of the Trans border Group, Adopted by the T-CY on 6 December 2012, Straatsburg 6 December 2012, www.coe.int/TCY). In het rapport wordt bevestigd dat er vanwege de technologische ontwikkelingen, de toenemende complexiteit en het internationale karakter van computercriminaliteit een toenemende behoefte is aan versterking van de bevoegdheden tot grensoverschrijdende toegang tot gegevens. Geconstateerd wordt dat opsporingsdiensten van veel staten zich in de praktijk toegang verschaffen tot gegevens die zijn opgeslagen in geautomatiseerde werken die zich op het grondgebied van andere staten bevinden, ten behoeve van het veiligstellen van elektronisch bewijs. Dit vloeit meestal voort uit het feit dat de opsporende staat niet zeker weet op welk grondgebied de gegevens zich bevinden. Deze praktijk kan volgens de Transborder Group geen grondslag vinden in artikel 32, onder b, van het Cybercrime Verdrag. Desondanks ziet de Transborder Group geen aanleiding om artikel 32 van het verdrag in zijn huidige vorm aan te passen. Volgens de Transborder Group is de effectiviteit van artikel 32 van het verdrag juist gebaat bij een meer eenduidige uitleg van de in die bepaling neergelegde begrippen als «rechtmatige en vrijwillige instemming». Het Comité van verdragspartijen bij het Cybercrime Verdrag heeft inmiddels een Begeleidende Notitie («Guidance Note») over artikel 32 van het Cybercrime Verdrag opgesteld. Hiermee wordt meer duidelijkheid geboden over de ruimte van bestaande bevoegdheden die op grond van het Cybercrime Verdrag kunnen worden uitgeoefend.

Voorts wordt geconcludeerd dat, zoals blijkens het «explanatory report» reeds ten tijde van het opstellen van het verdrag werd voorzien, het territorialiteitsbeginsel in «cyberspace» onder druk staat en dat het beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. Dit is een gevolg van de toenemende vluchtigheid van gegevens en versnipperde opslag van gegevens op verschillend grondgebied. Op basis van meer recent in de praktijk opgedane ervaringen zou, met een Aanvullend Protocol («Additional Protocol») bij het Cybercrime Verdrag, kunnen worden voorzien in aanvullende regelgeving voor situaties waarin gegevens in verschillende jurisdicties zijn opgeslagen of waarin de fysieke locatie van de gegevens niet bekend is. In het rapport van de Transborder Group van december 2014 is geconcludeerd dat het proces voor rechtshulpverzoeken inefficiënt is, in het bijzonder voor het verkrijgen van elektronisch bewijs. Dat leidt tot het niet kunnen voltooien van onderzoeken. Een werkgroep onderzoekt de mogelijkheden voor het verbeteren van het vergaren van digitaal bewijs in de Cloud en voor het versterken van de procedures voor rechtshulp bij digitale onderzoeken. Nederland zet zich in voor internationale consensus hierover. Op korte termijn is dit echter niet te verwachten.

In opdracht van het WODC hebben prof. dr. E.J. Koops en dr. M.E.A. Goodwin, verbonden aan TILT – Tilburg Institute for Law, Technology, and Society – van de Universiteit van Tilburg, onderzoek verricht naar de rechtmatigheid van grensoverschrijdende toegang tot gegevens. Dit vooral vanuit de kernbeginselen van territoriale integriteit en het verbod op inmenging in binnenlandse aangelegenheden en niet zozeer vanuit de mensenrechtelijke aspecten van cyberopsporing. In het rapport (Cyberspace, de cloud, en grensoverschrijdende opsporing: de grenzen en mogelijkheden van internationaal recht, 2014) wordt vastgesteld dat het grondgebied het kernelement blijft waarop internationaal recht is gebaseerd. De opvatting van cyberspace als «plaats» in de zin van territorium blijkt echter twijfelachtig. In het rapport wordt vastgesteld dat in de strikte – en dominante – klassieke interpretatie van het internationale recht iedere unilaterale bewijs verkrijgende activiteit in een buitenlandse staat als inbreuk op de soevereiniteit wordt beschouwd, behoudens de toestemming van de betrokken staat. Er zijn volgens de onderzoekers

echter plausibele argumenten te hanteren die een alternatieve omgang tussen staten met betrekking tot de Cloud en cyberspace kunnen rechtvaardigen. Staten kunnen onderling een alternatief internationaal juridische regime ontwikkelen dat de klassieke soevereiniteitsargumenten terzijde schuift. Gewezen wordt op eenzelfde ontwikkeling met betrekking tot andere ruimten waar het karakter van de ruimte het moeilijk maakt om die ruimte als «plaats» te behandelen, zoals Antarctica en de kosmische ruimte. Een andere optie is dat een of enkele landen gezamenlijk het voortouw nemen met een alternatieve uitleg van de huidige juridische kaders voor hun onderlinge betrekkingen, als voorlopers van een opkomende praktijk die op langere termijn door de bredere internationale gemeenschap kan worden geaccepteerd. Een belangrijk aspect wordt gevormd door de inspanning om de locatie van data te achterhalen. Ook kunnen waarborgen worden gezocht op het gebied van de beperking van de te verrichten handelingen, de universeel erkende ernst van het strafbare feit of de notificatie van de betrokken staat. De onderzoekers bevelen aan te bevorderen dat op internationaal niveau deze vraagstukken door regeringen worden onderkend en aangepakt. Volgens hen is van belang dat experts op het gebied van opsporing en cybercrime en op het gebied van het internationale recht zich meer in elkaars problematiek verdiepen en elkaars «taal» leren begrijpen. Op de korte termijn kunnen staten zich richten op het verhogen van de legitimiteit van nauw afgebakende, transparant uitgevoerde, en met sterke waarborgen omklede unilaterale acties, die daarbij een aannemelijk alternatief vormen voor de strikte interpretatie van het internationaal recht in cyberspace. Bij deze minder strikte interpretatie van het internationaal recht wordt een handeling van staten als meer of minder toelaatbaar beschouwd afhankelijk van de argumenten die de staat voor die handeling aandraagt. Tegelijkertijd kan er op de langere termijn worden gestreefd naar het creëren van een internationaal bindend instrument.

2.8.3. Uitvoerende rechtsmacht en de bestrijding van computercriminaliteit

De verdere ontwikkeling van een internationaalrechtelijk kader, dat is toegesneden op de toepassing van uitvoerende rechtsmacht bij de bestrijding van computercriminaliteit, verdient de voorkeur. De Nederlandse regering hecht veel waarde aan een gemeenschappelijk optreden van staten bij de bestrijding van de grensoverschrijdende criminaliteit en zal zich inzetten voor de verdere ontwikkeling van de internationale samenwerking tussen landen op het gebied van de wederzijdse rechtshulp, zodat beter tegemoet kan worden gekomen aan de specifieke behoeften met betrekking tot de bestrijding van cybercrime. De ontwikkeling van een dergelijk internationaalrechtelijk kader betreft echter een ideaal dat slechts op langere termijn kan worden gerealiseerd. In afwachting daarvan zal moeten worden gekozen tussen twee minder ideale situaties. Het afzien van het verrichten van opsporingshandelingen met betrekking tot gegevens wanneer niet bekend is waar deze zich bevinden of het zelfstandig op een zorgvuldige wijze uitoefenen van rechtsmacht bij de bestrijding van computercriminaliteit, waarbij zoveel mogelijk rekening wordt gehouden met de verschillende belangen. De eerste optie betekent in feite dat het internet een vrijplaats is voor criminaliteit, zolang de daders ervoor zorg dragen dat hun handelingen betrekking hebben op gegevens waarvan niet bekend is waar deze zich bevinden. Dat is niet aanvaardbaar. Hieruit vloeit voort dat, in afwachting van de ontwikkeling van een internationaalrechtelijk kader, wordt gekozen voor een zorgvuldige toepassing van rechtsmacht. Daarom wordt de volgende handelwijze voorgesteld:

Het uitgangspunt is dat er rechtshulp wordt gevraagd als de te verrichten opsporingshandelingen betrekking hebben op gegevens die zich in op het territorium van een andere staat bevinden. Een staat dient zijn bevoegd-

heden met de grootste zorgvuldigheid uit te oefenen, gezien het belang van het respecteren van de soevereiniteit van andere staten. Zoals in paragraaf 2.5. aan de orde is gekomen, wordt een zekere inspanning verricht om de feitelijke locatie van gegevens te achterhalen. Als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden dan is een verzoek om rechtshulp aangewezen, waarbij aan de bevoegde buitenlandse autoriteiten verantwoording wordt afgelegd over de handelingen die zijn verricht en de afwegingen die daarbij zijn gemaakt. Bij de uitoefening van opsporingshandelingen met betrekking tot gegevens die zich op het territorium van een andere staat blijken te vinden is het van belang dat op de kortst mogelijke termijn alsnog toestemming wordt gevraagd van het desbetreffende land.

Diverse landen hebben ten behoeve van de snelle afhandeling van rechtshulp in cybercrimezaken een 24/7 contactpunt ingericht. Uit het EU evaluatierapport over de aanpak van cybercrime in Nederland dat op 13 augustus 2015 (Kamerstukken II, 2014/15, 28 684, nr. 446) aan uw Kamer is gestuurd, blijkt dat Nederland inzake cybercriminaliteit internationaal zeer goed samenwerkt binnen Europol/EC3 en Eurojust, en met Interpol en andere derden. Met het oog op een spoedige en effectieve samenwerking met derde landen is het 24/7-contactpunt voor dringende verzoeken is ondergebracht bij het Team High Tech Crime (THTC), dat korte lijnen heeft met het Landelijk Parket voor high-tech crime. Het evaluatierapport stelt vast dat gemiddeld binnen 24 uur een eerste antwoord wordt gegeven. Dat kan een aanwijzing zijn van de daadwerkelijk benodigde tijd voor de gevraagde hulp. Ook wordt gewezen op de statistieken van 2012 en 2013 die een stijgende trend vertonen in het aantal inkomende en uitgaande rechtshulpverzoeken in verband met cybercrime. Als de toestemming door een andere staat wordt geweigerd dan is het aan de strafrechter om te oordelen over de consequenties daarvan voor de strafzaak. De Hoge Raad heeft inmiddels geoordeeld dat «de vraag of door de Nederlandse opsporingsambtenaren het volkenrecht is nageleefd, in beginsel in het kader van de strafzaak tegen de verdachte niet relevant is, omdat de belangen die het volkenrecht in zoverre beoogt te beschermen, geen belangen zijn van de verdachte, maar van de staat op het grondgebied waarvan buitenlandse opsporingsambtenaren optreden» (HR 05-10-2010 en 17-04-2012, ECLI: NL: HR: 2010: BL5629 en BV9070).

In sommige gevallen is de feitelijke locatie van gegevens redelijkerwijs niet te achterhalen. Dit komt voor wanneer vrijwel alle gegevens op de Cloud worden opgeslagen of bewaard. Dit kan ook verband houden met het op anonimiteit – en daarmee op het niet kunnen achterhalen van een geografische plaats – gerichte internetgedrag van bepaalde personen, zoals bij gegevens die via het Tor-netwerk worden gerouteerd of die door middel van NAT (network address translation; het veranderen van IP-adressen in de IP-header) worden verzonden (waarbij een groot aantal computers gebruik maakt van eenzelfde IP-adres). In deze gevallen is een gegeven niet altijd terug te voeren op een IP-adres en bestaat er niet altijd wetenschap van de locatie van de gegevens, en ook niet van de staat die betrokken is bij de opslag of verwerking van de gegevens. Dit kan betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk waarvan niet bekend is waar zich dit bevindt, bijvoorbeeld een server, met het oog op het verrichten van bepaalde onderzoekshandelingen. Voorstelbaar is dat een DDOS-aanval wordt gedaan op een overheidsdienst of een financiële instelling in Nederland waardoor de online dienstverlening gedurende langere tijd wordt onderbroken. Als geen duidelijkheid bestaat over het land dat rechtsmacht heeft over het beëindigen van die DDOS-aanval en de aanhouding van de daders, dan kan de ernst van de gevolgen van een dergelijke aanval voor het maatschappelijk verkeer rechtvaardigen dat onverwijld wordt

opgetreden om de verstoring van de dienstverlening te beëindigen en gegevens te verzamelen ten behoeve van het opsporingsonderzoek en de vervolging van de daders. Indien echter duidelijkheid ontstaat over de feitelijke locatie van de gegevens dan wordt zo snel mogelijk alsnog een rechtshulpverzoek gedaan en aan de bevoegde buitenlandse autoriteiten verantwoording afgelegd over het handelen en de daaraan ten grondslag liggende afwegingen.

Een dergelijk zelfstandig optreden dient zeer zorgvuldig te worden ingekaderd, op basis van een zoveel mogelijk stapsgewijze aanpak. In het algemeen zal worden gestart met een beperkte eerste vordering, het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker. 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. Aan de hand van criteria zal het optreden in het concrete gevallen worden afgewogen. Deze criteria 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. Deze criteria zullen worden uitgewerkt en vastgelegd in een OM-Aanwijzing dan wel bij algemene maatregel van bestuur. Tenslotte zal, als bekend is dat de gegevens niet in Nederland zijn opgeslagen, dit in het bevel moeten worden vermeld zodat de rechter-commissaris hierover controle kan uitoefenen.

De Afdeling advisering onderkent dat het eenvoudig is om de locatie van een geautomatiseerd werk of opgeslagen gegevens te verhullen. Het beperken van de inzet van de bevoegdheid tot gevallen waarin het zeker is dat het informatiesysteem zich in Nederland bevindt is niet goed mogelijk, ook in die gevallen moet optreden mogelijk zijn. Tegelijkertijd wordt hiermee het aanmerkelijke risico genomen dat opsporingshandelingen buiten het territorium van Nederland worden verricht, zonder volkenrechtelijke grondslag. In de regelgeving zou tot uitdrukking moeten komen dat hiermee voorzichtig wordt omgegaan. Nu niet vereist is dat in het bevel of de machtiging wordt vermeld waar het informatiesysteem zich bevindt, noch hoeveel moeite mag worden verwacht om de locatie van een systeem te achterhalen staat het niet vast dat de rechter-commissaris en de officier van justitie een expliciete afweging zullen maken over de internationale toepassing van de bevoegdheid. De regeling is niet beperkt tot gevallen waarin onverwijld grensoverschrijdend opgetreden moet worden. Tenslotte ontbreekt aandacht voor de situatie dat de locatie van het systeem na het binnendringen duidelijk wordt. Dan moet de toepassing worden beëindigd of toestemming worden gevraagd van het betreffende land. In het voorstel moet geregeld zijn wat met de verkregen informatie dient te geschieden. De Afdeling advisering adviseert in toelichting nader in te gaan op de toepassing van de bevoegdheid wanneer niet vaststaat dat het informatiesysteem zich in Nederland bevindt en het voorstel zonodig aan te passen.

Naar aanleiding van het advies van de Afdeling advisering is het wetsvoorstel aangepast en de toelichting verhelderd. In het bevel dient de officier van justitie, indien daarover wetenschap bestaat, te vermelden dat de gegevens niet in Nederland zijn opgeslagen. Dit geldt ook voor het geval dat niet bekend is waar de gegevens zijn opgeslagen. Hiermee is een expliciete afweging door de officier van justitie en de rechter-commissaris ten aanzien van de mogelijk internationale toepassing van de

opsporingsbevoegdheid verzekerd. Het is in beginsel aan de officier van justitie om de rechtmatigheid van het opsporingsonderzoek te bewaken. De vermelding in het bevel dat de gegevens niet in Nederland zijn opgeslagen vormt een extra waarborg voor een zorgvuldige voorbereiding van de inzet van de bevoegdheid door de officier van justitie, waarover rekenschap moet kunnen worden afgelegd bij de rechter-commissaris. Als de rechter-commissaris een machtiging afgeeft voor het op afstand heimelijk binnendringen van een geautomatiseerd werk, dan mag hij erop vertrouwen dat het bevel rechtmatig wordt uitgevoerd. In paragraaf 2.5. is nader ingegaan op de inspanning die wordt verricht op de locatie van de gegevens te achterhalen, de noodzaak van een zorgvuldige toepassing van de bevoegdheid en op de situatie dat na het binnendringen duidelijk wordt dat het geautomatiseerd werk zich niet Nederland bevindt. Verschillende adviesorganen menen dat het de voorkeur verdient om nadere internationale afspraken over dit onderwerp te maken. Daarbij wordt door enkele adviesorganen, zoals de NOvA en het Nederlands Juristen Comité voor de Mensenrechten (NCJM), gewezen op het element van de reciprociteit, namelijk dat eigenmachtig optreden van Nederlandse opsporingsautoriteiten ertoe zal kunnen leiden dat andere landen dit voorbeeld zullen overnemen en de soevereiniteit van Nederland zullen schenden als dat nodig is met het oog op de opsporing van strafbare feiten. BoF wijst er op dat uitoefening van de bevoegdheid een schending van de soevereiniteit van een ander land vormt en ertoe kan leiden dat andere landen inbreken op computers in Nederland. In zijn advies merkt het College van procureurs-generaal daarentegen op dat als de locatie van een systeem niet kan worden vastgesteld, dan ook niet kan worden vastgesteld dat de computer in het buitenland staat. In deze situatie geldt volgens het College de zogenaamde ubiquiteitsleer, die met zich meebrengt dat meerdere plaatsen als locus delicti kunnen worden aangemerkt en Nederland rechtsmacht heeft.

In reactie op deze adviezen merk ik op dat de rechtsmacht van een staat niet is beperkt tot het eigen grondgebied, de regels over de rechtsmacht in het Nederlandse Wetboek van Strafrecht zijn immers niet beperkt tot het beginsel van territorialiteit. Juist bij computercriminaliteit is het betrekkelijk eenvoudig om strafbare feiten te plegen waarbij vanuit meerdere landen wordt geopereerd. Hierbij is de vraag aan de orde in hoeverre opsporingshandelingen kunnen worden verricht met betrekking tot gegevens die zich in een andere jurisdictie bevinden, terwijl de staat die wenst te handhaven wel over extraterritoriale rechtsmacht beschikt. Op grond van het arrest van het Permanent Hof van Internationale Justitie, de voorloper van het Internationale Gerechtshof, in de zogenaamde Lotus-zaak kan worden aangenomen dat een staat slechts executieve rechtsmacht mag uitoefenen op het grondgebied van een andere staat met toestemming van die staat (Series A Nr 10 Leyden 1927). In casu betrof dit het optreden van opsporingsambtenaren in persoon op het grondgebied van een andere staat. De ontwikkeling van de informatie- en communicatietechnologie maakt het betrekkelijk eenvoudig om strafbare feiten te plegen waarbij de schadelijke gevolgen zich in andere landen manifesteren. Op grond van de wet (artikel 539a Sv) en de jurisprudentie bestaat er voor politie en justitie ruimte om, binnen de kaders van het volkenrecht en het interregionale recht, buiten de grenzen van het Nederlandse grondgebied op te treden. De omstandigheden waarin, en voorwaarden waaronder, zelfstandig optreden geïndiceerd kan zijn, zijn hierboven reeds aan de orde gekomen.
Uit het vorenstaande mag uitdrukkelijk niet worden afgeleid, zoals de NOvA stelt, dat de territorialiteit van andere staten maar moet wijken voor het Nederlandse opsporingsbelang. Het internationaalrechtelijke kader en de bilaterale relaties met andere staten op het gebied van de rechtshulp staan hieraan in de weg, en Nederland hecht juist zeer veel waarde aan

een gemeenschappelijk optreden van staten bij de bestrijding van de grensoverschrijdende criminaliteit. Het zelfstandig optreden van de rechtshandhavingsautoriteiten mag geen afbreuk doen aan bestaande afspraken en regels op het gebied van de rechtshulp. Als de locatie van de gegevens bekend is, dienen deze afspraken en regels te worden nageleefd. Daarbij kan nog worden opgemerkt dat er op grond van de wet strikte kaders gelden voor het optreden van de politie. Voor zowel de bestaande bevoegdheid van de doorzoeking ter vastlegging van gegevens alsook de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk geldt het vereiste van een rechterlijke machtiging. De voorafgaande rechterlijke toetsing heeft eveneens betrekking op de locatie van de gegevens. Het vereiste van de notificatie van de inzet van een bijzondere opsporingsbevoegdheid geldt eveneens als de bevoegdheid wordt ingezet met betrekking tot gegevens ten aanzien waarvan de locatie niet bekend is.

2.8.4. Conclusie

Voor de opsporing van grensoverschrijdende ernstige strafbare feiten, waarbij gebruik wordt gemaakt van geautomatiseerde werken voor de verwerking en de opslag van gegevens, is het van essentieel belang dat gebruik kan worden gemaakt van onderzoeksbevoegdheden, ook wanneer dat betekent dat daarmee toegang wordt verkregen tot geautomatiseerde werken die zich buiten Nederland bevinden. De huidige wetgeving op het gebied van extraterritoriale strafvordering biedt daartoe reeds mogelijkheden binnen de grenzen van het volkenrecht. Daarbij dienen de afspraken en regels over de internationale rechtshulp in acht te worden genomen. Vanwege het grensoverschrijdende karakter van deze vormen van criminaliteit is het niet uitgesloten dat meerdere staten over rechtsmacht beschikken. Als staten dat van elkaar weten dan ligt onderling overleg over de meest geëigende aanpak in de rede. Als bekend is dat gegevens zich in een bepaalde andere rechtsmacht bevinden dan is rechtshulpaangewezen.
In internationaal verband is vastgesteld dat het territorialiteitsbeginsel in «cyberspace» onder druk staat en dat het beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. In het kader van het overleg in de Raad van Europa worden de mogelijkheden onderzocht voor het verbeteren van het vergaren van digitaal bewijs in de Cloud en voor het versterken van de procedures voor rechtshulp bij digitale onderzoeken.

In cyberspace is de feitelijke locatie van gegevens echter niet altijd te achterhalen.
In afwachting van de verdere ontwikkeling van het internationaalrechtelijke kader voor de uitoefening van rechtsmacht bij de bestrijding van computercriminaliteit zal zelfstandig opgetreden moeten kunnen worden, om te voorkomen dat internet een vrijplaats wordt voor criminaliteit. Dit kan met zich meebrengen dat opsporingshandelingen worden verricht met betrekking tot gegevens die niet in Nederland zijn opgeslagen. Er zullen toetsingscriteria worden opgesteld voor dit optreden, deze criteria zullen worden vastgelegd in een OM-Aanwijzing of bij algemene maatregel van bestuur. Indien dat bekend is dient in het bevel te worden vermeld dat de gegevens niet in Nederland zijn opgeslagen, zodat hierover rekenschap kan worden afgelegd bij de rechter-commissaris.

2.9. De bescherming van grondrechten

De voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk is weliswaar in het belang van de opsporing maar raakt aan de grondrechten van burgers. Daar waar de overheid zich inlaat met het privéleven van burgers kunnen verschillende grondrechten in het geding zijn.

Daarvoor kan worden gedacht aan de eerbiediging van de persoonlijke levenssfeer (artikel 10 van de Grondwet), de onschendbaarheid van de woning (artikel 12 van de Grondwet) en de onschendbaarheid van het brief-, telefoon- en telegraafgeheim (artikel 13 van de Grondwet). Aantasting van of inmenging in die grondrechten door de overheid is uitsluitend mogelijk in de gevallen bij wet voorzien. In het Wetboek van Strafvordering of in bijzondere wetten is geregeld in welke gevallen en onder welke voorwaarden gekomen kan worden tot aantasting van grondrechten ten behoeve van het publieke belang van de opsporing en vervolging van strafbare feiten. Van oudsher vormde de onschendbaarheid van het briefgeheim een belangrijke waarborg voor de bescherming van de briefwisseling tussen burgers. Later verkreeg de communicatie door middel van de telefoon en telegraaf een belangrijke plaats in het maatschappelijk verkeer. Dit leidde in 1983 tot constitutionele bescherming van het telefoon- en telegraafgeheim. De onschendbaarheid van het brief-, telefoon-, en telegraafgeheim betekent echter niet dat er sprake is van een absoluut recht jegens de overheid, die zich heeft te onthouden van iedere aantasting van of inmenging in dat recht. Het publieke belang van de rechtshandhaving kan strekken tot beperking van de grondrechten van burgers. Er is dan sprake van een zodanig zwaarwegend algemeen belang dat dit een dergelijke beperking rechtvaardigt. Vanwege dit belang is in het Wetboek van Strafvordering een wettelijke regeling opgenomen voor het aftappen van communicatie. Gedurende de afgelopen jaren heeft de telefoontap zich ontwikkeld tot een onmisbaar instrument voor politie en justitie om zicht te verkrijgen op de betrokkenheid van personen bij het beramen of plegen van strafbare feiten. In de gevallen waarin de communicatie tussen burgers via andere kanalen verloopt staan andere bijzondere opsporingsbevoegdheden ter beschikking. Met de Wet bijzondere opsporingsbevoegdheden, van 1 februari 2000, is in het Wetboek van Strafvordering de bevoegdheid opgenomen van het direct afluisteren. Dit betreft gesprekken tussen personen, zonder dat daarbij gebruik wordt gemaakt van een communicatiedienst. Met de Wet bevoegdheden vorderen gegevens, van 1 juni 2004, is de bevoegdheid geïntroduceerd van het vorderen van gegevens die zijn opgeslagen in het geautomatiseerde werk van een aanbieder. Dit kan gegevens betreffen die betrekking hebben op communicatie tussen burgers, zoals e-mail- of sms-berichten die bij de aanbieder zijn opgeslagen.

In paragraaf 2.1. is reeds aan de orde gekomen dat de ontwikkelingen op het gebied van de informatie- en communicatietechnologie nieuwe eisen stellen aan opsporing van strafbare feiten. De opsporing wordt ernstig belemmerd door de versleuteling van gegevens en het gebruik van Cloudcomputingdiensten. Het op afstand heimelijk binnendringen in een geautomatiseerd werk door de politie vormt een ernstige aantasting van het privéleven van de burger, doordat de overheid inzage krijgt in gegevens die in het geautomatiseerde werk worden verwerkt of opgeslagen. Dit betreft een ingrijpende bevoegdheid. Daar staat tegenover dat ook thans, bij het gebruik van bestaande opsporingsbevoegdheden, inzage kan worden verkregen in de gegevens die door burgers worden verwerkt met behulp van een geautomatiseerd werk. Een computer of smartphone kan inbeslaggenomen worden, waardoor de overheid tevens de beschikking verkrijgt over alle gegevens van het geautomatiseerde werk. Ook kan een bug worden geplaatst op een geautomatiseerd werk waarmee toetsaanslagen kunnen worden afgevangen, of kunnen e-mailberichten worden gevorderd bij de aanbieder. Dit wetsvoorstel beoogt de opsporingsbevoegdheden in evenwicht te brengen met de stand van de technologie. Daarbij moet een zorgvuldig evenwicht worden bewaard tussen de rechten van burgers en de belangen van een behoorlijke rechtshandhaving. De bescherming van

de burger tegen aantasting van zijn grondrechten kan niet willekeurig plaatsvinden, daaraan dienen strikte voorwaarden te worden verbonden die waarborgen dat het evenwicht tussen de rechten van de burger en de bevoegdheden van de overheid in stand blijft. De grondrechten vormen een essentiële waarborg voor de burger dat de overheid zich onthoudt van maatregelen die een ongerechtvaardigde aantasting van die rechten vormen. Anderzijds dienen de overheid afdoende maatregelen of middelen ter beschikking te staan om op te kunnen treden tegen strafbaar handelen van burgers waarbij welbewust maatregelen zijn getroffen om ontdekking en opsporing te voorkomen. Dit is in het belang van de veiligheid en het welbevinden van de samenleving. Die maatregelen of middelen zullen soms openlijk kunnen worden toegepast, in andere gevallen is die toepassing alleen effectief als deze heimelijk plaatsvindt. Hieronder wordt nader ingegaan op de grondrechten die bij de bevoegdheid van onderzoek in een geautomatiseerd werk in het geding zijn en de afwegingen ter zake.

2.9.1. Het recht op eerbiediging van de persoonlijke levenssfeer
De bevoegdheid tot onderzoek in een geautomatiseerd werk moet worden beoordeeld 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 Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM). Het recht op bescherming van de persoonlijke levenssfeer houdt in dat de overheid de persoonlijke levenssfeer van burgers dient te respecteren. Onderdeel van het recht op bescherming van de persoonlijke levenssfeer is dat de burger het recht heeft met rust gelaten te worden en onbevangen zichzelf te zijn. Een beperking van dit recht is slechts mogelijk als dat in de wet is geregeld. Het EVRM stelt daarnaast als eis dat de beperking noodzakelijk is in een democratische samenleving in het belang van onder andere de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten. In de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) komt naar voren dat deze noodzaak mede wordt bepaald aan de hand van de beginselen van proportionaliteit en subsidiariteit. Artikel 8 van het EVRM en de daarop gebaseerde jurisprudentie stellen ook eisen aan de kwaliteit van de wettelijke regeling. Deze moet voor de burger voldoende toegankelijk en kenbaar zijn. Dit betekent dat de regeling voldoende precies moet zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden bevoegdheden mogen worden toegepast. De regeling moet bovendien waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. Deze eis weegt zwaarder naarmate een bevoegdheid meer ingrijpend is en heimelijk kan worden toegepast.

Met de toepassing van de bevoegdheid tot onderzoek in een geautomatiseerd werk wordt een inbreuk gemaakt op de rechten en vrijheden van de betrokkene. De burger mag erop vertrouwen dat de integriteit van zijn computersysteem gewaarborgd is en dat derden niet zonder toestemming kennis kunnen nemen van vertrouwelijke documenten en kunnen meeluisteren bij vertrouwelijke communicatie via computers. De inbreuk van het onderzoek in een geautomatiseerd werk is vergelijkbaar met de toepassing van andere bevoegdheden waarbij een computer wordt doorzocht, zoals bij de doorzoeking ter vastlegging van gegevens, de netwerkzoeking en bij het direct afluisteren en het aftappen van communicatie. Het aftappen van communicatie en het direct afluisteren worden door het EHRM onder omstandigheden als een schending van artikel 8 van het EVRM gezien. Het op afstand heimelijk toegang verkrijgen tot een geautomatiseerd werk ten behoeve van de opsporing van ernstige strafbare feiten kan daarom worden beschouwd als een inbreuk op de

persoonlijke levenssfeer, zoals beschermd in het EVRM (J.J. Oerlemans, Hacken als opsporingsbevoegdheid, DD 2011, afl. 8/62, blz. 898).

Uit de bescherming van het recht op eerbiediging van de persoonlijke levenssfeer, als neergelegd in artikel 10 van de Grondwet en artikel 8 van het EVRM, vloeit voort dat de bevoegdheid tot het op afstand heimelijk binnendringen, onderzoeken en eventueel opnemen of vastleggen van gegevens noodzakelijk moet zijn in een democratische samenleving, in het belang van de openbare veiligheid en de voorkoming en vervolging van strafbare feiten. Zoals in paragraaf 2.1 aan de orde kwam, vult de voorgestelde bevoegdheid een leemte in de bestaande opsporingsbevoegdheden. Deze leemte wordt veroorzaakt door de eerder in de inleiding omschreven technologische ontwikkelingen op het gebied van informatie- en communicatietechnologie, zoals het toenemend gebruik van versleuteling van gegevens, het gebruik van netwerken en Cloudcomputingdiensten. Deze ontwikkelingen brengen met zich mee dat met de bestaande wettelijke bevoegdheden het doel, namelijk het vergaren of vorderen van gegevens die mogelijk als bewijs kunnen dienen, niet kan worden bereikt. De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een dringende behoefte van de opsporing om ernstige vormen van criminaliteit te kunnen bestrijden door onderzoek te kunnen verrichten in een geautomatiseerd werk met het oog op de in het voorgestelde artikel 125nba, eerste lid, Sv omschreven doelen. Op grond van de bestaande bevoegdheden kan niet worden tegemoetgekomen aan de gesignaleerde problemen rond de ontwikkelingen op het gebied van de informatie- en communicatietechnologie.
De beginselen van proportionaliteit en subsidiariteit worden als volgt ingevuld. Het beginsel van proportionaliteit houdt in dat het belang dat wordt gediend met de bevoegdheid, in verhouding moet staan tot de omvang van de beperking van de persoonlijke levenssfeer. Voor de beoordeling van de omvang van deze beperking is ten eerste van belang dat de voorgestelde bevoegdheid een aanvulling vormt op de bestaande wettelijke bevoegdheden. De bevoegdheid tot onderzoek in een geautomatiseerd werk kan slechts worden toegepast als uit het opsporingsonderzoek blijkt dat met de bestaande wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt. Er dient sprake te zijn van een dringend opsporingsbelang. De bevoegdheid is beperkt tot een geautomatiseerd werk dat bij de verdachte in gebruik is. De reden waarom niet met een andere wettelijke opsporingsbevoegdheid kan worden volstaan, dient in het bevel te worden vermeld.
In de tweede plaats is de inzet van de bevoegdheid beperkt tot de in het voorgestelde artikel 126nba, eerste lid, Sv omschreven doelen. Deze doelen zijn limitatief omschreven. Dit betreft het verrichten van bepaalde onderzoekshandelingen, waarvoor het nodig is dat op afstand heimelijk wordt binnengedrongen in het geautomatiseerde werk. De limitatieve opsomming van de doelen vereenvoudigt een zorgvuldige afweging door de officier van justitie inzake de noodzaak van de inzet van de afzonderlijke bevoegdheden in een concreet geval. Dit is ook in het belang van een zorgvuldige rechterlijke toetsing.
In de derde plaats is voorzien in een voorafgaande rechterlijke toetsing van de voorgenomen inzet van onderzoek in een geautomatiseerd werk. Het vereiste van de rechterlijke toetsing geldt voor zowel het binnendringen in het geautomatiseerde werk, als voor de nadere onderzoekshandelingen, die limitatief omschreven zijn.
In de vierde plaats houdt de bevoegdheid in dat deze wordt toegepast in een zo beperkt mogelijk deel van een geautomatiseerd werk. Deze beperking dient in het bevel te worden omschreven en waarborgt dat de overheid geen onbegrensde toegang heeft tot gegevens die zijn opgeslagen in een geautomatiseerd werk. Wanneer tijdens de toepassing van de bevoegdheid blijkt dat de bevoegdheid in een ander deel van het

geautomatiseerde werk moet worden toegepast, dan is daarvoor een aangepast bevel en uitdrukkelijke toestemming van de rechter-commissaris nodig.
In de vijfde plaats is de toepassing van de bevoegdheid beperkt in tijd. Het bevel vermeldt het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven. De bevoegdheid mag slechts voor de duur van hoogstens vier weken worden toegepast en kan telkens voor een periode van ten hoogste vier weken worden verlengd. Gelet op het voorgaande voldoet de voorgestelde bevoegdheid aan het vereiste van proportionaliteit.

Het beginsel van subsidiariteit houdt in dat het beoogde doel niet kan worden bereikt met een andere maatregel die minder ingrijpend is voor de persoonlijke levenssfeer. Hierover kan worden opgemerkt dat er geen andere opsporingsbevoegdheid is waarmee toegang kan worden gekregen tot gegevens die een vaste opslaglocatie ontberen, of waarmee het hoofd kan worden geboden aan de knelpunten in de opsporing die samenhangen met de toenemende mobiele toepassingen van internetgebruik en de versleuteling van gegevens. Daarvoor kan worden verwezen naar paragraaf 2.1. De bevoegdheid draagt daarmee bij aan het vergaren van digitaal bewijs en het opsporen van strafbare feiten. Zoals hiervoor al is beschreven dient in het bevel de reden te worden opgenomen waarom niet met een andere wettelijke bevoegdheid kan worden volstaan. Daarmee wordt de rechter-commissaris in staat gesteld om deze voorwaarde te toetsen. De voorgestelde bevoegdheid voldoet daarmee aan het subsidiariteitvereiste.

Een andere eis waaraan de regeling ingevolge artikel 8 van het EVRM moet voldoen, betreft de kwaliteit van de wettelijke regeling. De wettelijke regeling moet voor de burger voldoende toegankelijk en kenbaar zijn. Met de voorgestelde regeling van artikel 126nba Sv wordt aan deze eis voldaan. Artikel 126nba, eerste lid, Sv vormt de grondslag voor het verrichten van onderzoek in een geautomatiseerd werk; de doelen waarvoor de bevoegdheid kan worden toegepast zijn in dat artikel limitatief omschreven.

De wettelijke regeling moet ook waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. In het voorgestelde artikel 126nba Sv zijn deze waarborgen nader uitgewerkt.
De bevoegdheid kan slechts worden toegepast als sprake is van een verdenking van ernstige strafbare feiten die een ernstige inbreuk op de rechtsorde opleveren. Daarnaast moet sprake zijn van een dringend onderzoeksbelang. Voorts kan bij de inzet van de bevoegdheid slechts gebruik worden gemaakt van een technisch hulpmiddel dat voldoet aan bepaalde eisen, die zijn neergelegd in het Besluit technische hulpmiddelen strafvordering. Met deze voorwaarden wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik alsmede voor het verzekeren van de authenticiteit en integriteit van door middel van het technische hulpmiddel vastgelegde gegevens. Daarbij is voorzien in functiescheiding tussen opsporingsambtenaren die betrokken zijn bij het onderzoek in een geautomatiseerd werk (het technische team) en de opsporingsambtenaren die betrokken zijn bij het operationele opsporingsonderzoek (het tactische team). Ook is voorzien in logging van de gegevens over de handelingen die in het kader van de inzet van het technische hulpmiddel worden verricht.
Ten slotte dient het bevel nauwkeurig te worden onderbouwd met de in het tweede lid omschreven informatie, zodat de rechter-commissaris in staat wordt gesteld om een gedegen afweging te maken alvorens hij een machtiging geeft aan de officier van justitie.

2.9.2. Het recht op bescherming van het brief-, telefoon- en telegraafgeheim

Het recht op bescherming van het brief-, telefoon- en telegraafgeheim, dat is vastgelegd in artikel 13 van de Grondwet, beschermt de vertrouwelijkheid van communicatie die plaatsvindt per brief, telefoon of telegraaf en die is toevertrouwd aan een instelling die is belast met het transport of de verzending van de communicatie. Dit grondrecht beschermt tegen onbevoegde kennisneming van communicatie door derden, inclusief de overheid, tijdens het transport of de verzending. Schending van het briefgeheim vereist een last van de rechter, schending van het telefoon- of telegraafgeheim vereist een machtiging van hen die daartoe bij de wet zijn aangewezen (artikel 13 van de Grondwet). De algemene eis is dat de formele wetgever bepaalt in welke gevallen beperkingen zijn toegestaan. Het recht op bescherming van het brief-, telefoon- en telegraafgeheim wordt eveneens beschermd door het eerdergenoemde artikel 8 van het EVRM en door artikel 17 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR) van de Verenigde Naties.

Vanwege de beperkte reikwijdte van het brief-, telefoon- en telegraafgeheim zal de bescherming van artikel 13 van de Grondwet bij het binnendringen van een geautomatiseerd werk slechts in bijzondere gevallen aan de orde kunnen zijn. In de eerste plaats geldt dat elektronische vormen van communicatie, zoals e-mail, niet onder de reikwijdte van het brief-, telefoon- of telegraafgeheim vallen. Daar komt bij dat het brief-, telefoon- en telegraafgeheim betrekking heeft op de bescherming van communicatie die aan een derde is toevertrouwd.

De uitoefening van de in dit wetsvoorstel voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk kan met zich meebrengen dat inzage wordt verkregen in communicatie die in elektronische vorm is opgeslagen of vastgelegd. Dit kan aan de orde zijn bij het vaststellen van de aanwezigheid van gegevens, het vastleggen van gegevens die in het geautomatiseerde werk zijn opgeslagen of vastgelegd of de ontoegankelijkmaking van gegevens. Daarbij is het echter van minder belang in hoeverre dit gegevens betreft die onder de reikwijdte van artikel 13 van de Grondwet vallen. De bescherming tegen onbevoegde kennisneming van de gegevens is namelijk gelijk aan die van communicatie die met behulp een brief of telefoon wordt overgebracht. De kennisneming van de gegevens is bij wet voorzien, en met het vereiste van een rechterlijke machtiging is voorzien in rechterlijke tussenkomst voordat de bevoegdheid wordt toegepast. In dit opzicht worden met dit wetsvoorstel gelijke waarborgen geboden ter bescherming van elektronische communicatie als voor de communicatie die met behulp van brief of telefoon wordt overgebracht.

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

Voor de toetsing aan de vereisten die uit artikel 8 van het EVRM voortvloeien kan worden verwezen naar de vorige paragraaf. Aanvullend kan worden opgemerkt dat uit de jurisprudentie van het Europese Hof voor de Rechten van de Mens kan worden afgeleid dat rechterlijke toetsing voorafgaand aan inzage in de inhoud van de brief- en telecommunicatie, in beginsel wenselijk is omdat de inzage heimelijk plaatsvindt buiten medeweten van de betrokkene (Klass tegen Duitsland, EHRM 6 september 1978, series A28, par. 55–56). Wat betreft artikel 17 IVBPR kan worden opgemerkt dat met dit wetsvoorstel wordt voorzien in adequate waarborgen tegen willekeurige of onwettige inmenging van de overheid in het privéleven of de briefwisseling van de burger.

3. De ontoegankelijkmaking van gegevens

3.1. Algemeen

In paragraaf 2.3 is de bevoegdheid aan de orde gekomen om gegevens ontoegankelijk te maken die in het kader van doorzoeking of onderzoek in een geautomatiseerd werk ter vastlegging van gegevens, als bedoeld in de artikelen 125i, 125j en het voorgestelde 126nba Sv, worden aangetroffen. Dit is geregeld in artikel 126cc, vijfde en zesde lid, Sv. Zoals eerder is opgemerkt kunnen onder het begrip «ontoegankelijkmaking» verschillende maatregelen worden verstaan die nodig zijn om te voorkomen dat onbevoegden van de gegevens kunnen kennisnemen of daarvan gebruik kunnen maken. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is, rekening houdend met de eisen van proportionaliteit en subsidiariteit (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 21). Het enkele «verstoren» van het kennisnemen van gegevens behoort tot de mogelijkheden. Dit is onder meer van belang voor de bestrijding van botnets.

Daarnaast voorziet het Wetboek van Strafrecht in de mogelijkheid tot het ontoegankelijk maken van gegevens door een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn (artikel 54a Sr). Voorgesteld wordt de bevoegdheid tot het vorderen dat gegevens ontoegankelijk worden gemaakt als afzonderlijke en zelfstandige bevoegdheid op te nemen in het Wetboek van Strafvordering. Het is uit wetssystematisch oogpunt gewenst dat de bevoegdheid om de ontoegankelijkmaking van gegevens te vorderen in het Wetboek van Strafvordering wordt opgenomen in plaats van – zoals thans het geval is – het Wetboek van Strafrecht. Artikel 54a Sr bevat, naast een bevoegdheid om ontoegankelijkmaking van gegevens te bevelen, ook een – onder nadere voorwaarden toepasselijke – vervolgingsuitsluitingsgrond voor aanbieders van een communicatiedienst. Deze vervolgingsuitsluitingsgrond is in het Wetboek van Strafrecht opgenomen ter uitvoering van de Richtlijn inzake elektronische handel (Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt), die er onder andere toe strekt de aansprakelijkheid van intermediaire dienstverleners van de informatiemaatschappij te beperken. Uit de rechtspraak met betrekking tot artikel 54a Sr kan worden afgeleid dat onder andere de in dat artikel vervatte combinatie van een vervolgingsuitsluitingsgrond en een bevelsbevoegdheid vragen oproept en de toepassing van de regeling in de praktijk compliceert (zie Rechtbank Assen 22 juli 2008, LJN BD8451, Hof Leeuwarden 20 april 2009, LJN BI1645 en Rechtbank Assen 24 november 2009, LJN BK4226). Opneming van de bevoegdheid tot het vorderen van de ontoegankelijkmaking van gegevens in het Wetboek van Strafvordering is daarmee niet alleen uit wetssystematisch oogpunt, maar ook uit een oogpunt van

overzichtelijkheid en duidelijkheid voor de praktijk van belang. Met de voorgestelde bevelsbevoegdheid – op basis van het onderzoeksrapport «Wat niet weg is, is gezien» van M.H.M. Schellekens, B.J. Koops en W.G. Teepe – kan worden gekomen tot een betere toepassing van de bestaande regeling waardoor de samenleving beter kan worden beschermd tegen dergelijke gedragingen. Van de gelegenheid is gebruik gemaakt om de in artikel 54a Sr resterende vervolgingsuitsluitingsgrond op enkele punten te verhelderen.

Reeds eerder is een conceptwetsvoorstel tot aanpassing van de regeling van de ontoegankelijkmaking van gegevens in consultatie gegeven. Naar aanleiding van de adviezen is het eerdere voorstel herzien en in dit wetsvoorstel opgenomen. In het eerdere conceptwetsvoorstel was voorzien in een zelfstandige bevelsbevoegdheid voor de officier van justitie. Mede naar aanleiding van de adviezen is ervoor gekozen het vereiste van een voorafgaande machtiging van de rechter-commissaris te handhaven, conform de huidige regeling van artikel 54a Sr. De in het eerdere conceptwetsvoorstel voorziene mogelijkheid van een dwangsom voor het niet of niet tijdig voldoen aan het bevel, is in dit wetsvoorstel niet overgenomen.

3.2. De noodzaak tot aanpassing van de huidige wettelijke regeling

Inmiddels is door een groot aantal internetproviders op basis van vrijwilligheid een gedragscode opgesteld en ondertekend (Kamerstukken II 2008/09, 28 684, nr. 232). Dit betreft de gedragscode «Notice and Take Down» (hierna ook te noemen: NTD-gedragscode). De NTD-gedragscode richt zich op tussenpersonen die in Nederland een openbare telecommunicatiedienst op het internet leveren en bevat een procedure voor het omgaan met meldingen van onrechtmatige en strafbare informatie op het internet. Indien er naar het oordeel van de tussenpersoon sprake is van onmiskenbaar onrechtmatige of strafbare inhoud, zorgt de tussenpersoon ervoor dat de desbetreffende inhoud onverwijld wordt verwijderd. Indien niet tot een eenduidig oordeel wordt gekomen of er al dan niet van onrechtmatige of strafbare inhoud sprake is, kan de melder overgaan tot het doen van aangifte of de rechter betrekken. Deze procedure wordt eveneens toegepast bij verzoeken van de politie als het gaat om het verwijderen van kinderpornografie van het internet die in Nederland wordt «gehost». De voorgestelde regeling is, evenals de bestaande regeling van artikel 54a Sr, bedoeld voor de gevallen waarin de zelfregulering binnen de bedrijfstak tekort schiet. In die gevallen waarin de NTD-gedragscode niet afdoende is voor de verwijdering van de gegevens, kan de officier van justitie gebruik maken van de bevoegdheid van het voorgestelde artikel 125p Sv. De bevoegdheid is van belang in die gevallen waarin de aanbieder van een communicatiedienst niet bereid is op basis van de NTD-gedragscode de gegevens ontoegankelijk te maken. Dat zal bij de internetproviders die deze code hebben ondertekend wellicht alleen aan de orde zijn in (uitzonderlijke) gevallen waarin de officier van justitie en de provider van mening zouden (blijven) verschillen over de vraag of bij de ontoegankelijkmaking de vrijheid van meningsuiting in het geding is. Belangrijker is echter dat het bevel ook kan worden gericht tot aanbieders van een communicatiedienst die de NTD-gedragscode niet hebben ondertekend, waarbij te denken valt aan hosting providers en beheerders van een website. Handhaving van de bevoegdheid te bevelen dat gegevens ontoegankelijk worden gemaakt is dus gewenst om strafbare feiten te kunnen beëindigen of om nieuwe strafbare feiten te voorkomen.

Gelet op de belangen die bij een bevel tot ontoegankelijkmaking in het geding zijn, ligt het in de rede om een voorafgaande rechterlijke

machtiging te vereisen. Een rechter-commissaris moet bij uitstek in staat worden geacht om een onpartijdige en zorgvuldige afweging tussen de verschillende belangen te maken. In die gevallen waarin de NTD-gedragscode niet afdoende is kan het gaan om gevallen waarin verschil van inzicht bestaat over de strafbaarheid van de gegevens. Daarbij kan de vrijheid van meningsuiting in het geding zijn. Met het vereiste van een rechterlijke machtiging is een zorgvuldige afweging van de belangen gewaarborgd. Vanuit het oogpunt van de bescherming van de maatschappij is het niet aanvaardbaar als de daadwerkelijke verwijdering afhankelijk zou zijn van een beslissing van de rechter naar aanleiding van de ingestelde strafvervolging, wegens het niet voldoen aan een ambtelijk bevel of het plegen van of deelnemen aan een strafbaar feit in verband met het verspreiden van de desbetreffende gegevens. Het zou dan enkele maanden of langer duren voordat er een definitieve uitspraak van de rechter is, die de grondslag kan vormen voor het ontoegankelijk maken van de gegevens. De officier van justitie is gehouden om aan de rechter-commissaris voldoende gegevens voor te leggen op grond waarvan deze de vordering van de officier van justitie kan beoordelen en tot een verantwoorde beslissing over de afgifte van een machtiging kan komen. De rechter-commissaris geeft de machtiging niet dan nadat de aanbieder in de gelegenheid is gesteld te worden gehoord.
In het arrest van het EHRM van 14 september 2010 in de zaak Sanoma tegen Nederland (application no. 38224/03) werd – kort gezegd – geoordeeld dat bij een vordering tot uitlevering van een voorwerp waarbij het recht op bescherming van een journalistieke bron in het geding kan zijn, een wettelijke plicht moet zijn voorzien van voorafgaande toetsing door een rechter. Met de tussenkomst van de rechter-commissaris wordt hieraan voldaan.

In zijn advies over het conceptwetsvoorstel heeft het College van procureurs-generaal opgemerkt dat de officier van justitie, op grond van het voorgestelde artikel 125p Sv, een bevel tot ontoegankelijkmaking van gegevens tot de aanbieder kan richten in geval van verdenking van ieder strafbaar feit. Omdat deze bevoegdheid zal worden ingezet in gevallen waarin de vrijheid van meningsuiting vaak een rol speelt dreigt het risico dat het OM in de rol van een censurerende internetpolitie wordt gedrongen. Het College adviseert derhalve de bevoegdheid tot het geven van een dergelijk bevel te beperken tot een verdenking van een strafbaar feit, als bedoeld in artikel 67 Sv. Dit past ook beter bij het voorstel dat het bevel slechts kan worden gegeven na een machtiging van de rechter-commissaris. Met het College ben ik van oordeel dat het, gelet op de systematiek van de wet, in de rede ligt het bevel tot ontoegankelijkmaking van gegevens te beperken tot ernstige misdrijven, waarvoor voorlopige hechtenis mogelijk is. Naar aanleiding van dit advies is het voorgestelde artikel 125p Sv in deze zin aangepast. De NOvA heeft een soortgelijk bezwaar tegen de voorgestelde regeling ingebracht, en opgemerkt dat de bevelsbevoegdheid door de officier van justitie kan worden gebruikt in een bagatelgeval, bijvoorbeeld een particuliere site waar een of slechts enkele auteursrecht schendende bestanden of hyperlinks zijn geplaatst. De NOvA adviseert de bevelsbevoegdheid uitdrukkelijk aan serieuze situaties te verbinden, door deze te beperken tot een strafbaar feit dat ernstige inbreuk op de rechtsorde met zich meebrengt. In reactie op dit advies kan worden opgemerkt dat de beperking tot een strafbaar feit waarvoor voorlopige hechtenis mogelijk is, in combinatie met het vereiste van de machtiging van de rechter-commissaris, in de weg staat aan toepassing van de voorgestelde bevoegdheid in bagatelzaken. Het criterium van de ernstige inbreuk op de rechtsorde acht ik echter te zwaar om de verspreiding van strafbare uitingen op het internet adequaat tegen te kunnen gaan. In vergelijking het huidige artikel 54a Sr, op grond

waarvan een bevel tot ontoegankelijkmaking van gegevens mogelijk is voor ieder strafbaar feit, zou dit een stap terug betekenen.

3.3. De uitvoering van een bevel tot ontoegankelijkmaking van gegevens

Van de aanbieder wordt verlangd dat hij alle maatregelen neemt «die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken». De officier van justitie kan, indien de gegevens niet ontoegankelijk worden gemaakt en hij gegronde redenen heeft om aan te nemen dat degene tot wie het bevel is gericht zich onvoldoende heeft ingespannen om de gegevens ontoegankelijk te maken, deze zo nodig vervolgen voor het niet voldoen aan een bevoegd gegeven ambtelijk bevel (artikel 184 Sr) dan wel voor het plegen van of deelnemen aan het strafbare feit waarop de gegevens, waarvan de ontoegankelijkmaking is bevolen, betrekking hebben. Een argument om een aanbieder van een communicatiedienst in voorkomende gevallen uitsluitend te vervolgen voor het niet voldoen aan een ambtelijk bevel kan zijn dat daarin veelal de kern van het aan de aanbieder te maken verwijt zal liggen. Een dergelijke vervolging bij uitingsdelicten kan in het algemeen bewijstechnisch eenvoudiger zijn dan vervolging voor medeplichtigheid aan het met gebruikmaking van de communicatiedienst begane uitingsdelict, omdat voor het voor een veroordeling ter zake van schending van artikel 184 Sr in combinatie met het voorgestelde artikel 125p Sv voldoende is dat een verdenking van een uitingsdelict bestond. Bij vervolging voor alleen artikel 184 Sr wordt door de rechter niet buiten redelijke twijfel vastgesteld dat het met gebruikmaking van de communicatiedienst begane delict strafbaar is. Dit is kenmerkend voor artikel 184 Sr: de kern van het verwijt bij dit misdrijf tegen het openbaar gezag is – kort gezegd – dat de verdachte, hoewel hij daartoe verplicht is, niet desgevraagd meewerkt met de overheid. Een dergelijke verplichting kan door uitoefening van tal van bevoegdheden ontstaan, terwijl voor die uitoefening veelal alleen een bepaalde verdenking is vereist.

De ontoegankelijkmaking van gegevens betreft een voorlopige maatregel. De definitieve beslissing over de vernietiging van de gegevens is voorbehouden aan de rechter. Als de door de officier van justitie ingestelde strafvervolging leidt tot een einduitspraak neemt de rechter, als het bevel niet is opgeheven, tevens een beslissing over het bevel (artikel 354 Sv). Net als bij de onttrekking aan het verkeer van voorwerpen is voorzien in de mogelijkheid van vernietiging bij afzonderlijke rechterlijke beschikking. Bij een dergelijke beslissing kan worden gelast dat de ontoegankelijk gemaakte gegevens worden vernietigd indien het gegevens betreft met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan, voor zover de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten (artikel 552fa Sv).

Als de rechter-commissaris de vordering afwijst staat voor de officier van justitie de mogelijkheid van hoger beroep open (artikel 446 Sv). De raadkamer kan, indien zij meent dat aan de voorwaarden van artikel 125p Sv is voldaan, alsnog bevelen dat de gegevens ontoegankelijk worden gemaakt.

Vanwege de mogelijk verstrekkende consequenties van een bevel tot ontoegankelijkmaking van gegevens staat voor de belanghebbende, waaronder degene tot wie het bevel is gericht, de mogelijkheid open van beklag bij de raadkamer van de rechtbank. Belanghebbenden kunnen zich schriftelijk beklagen over het bevel tot ontoegankelijkmaking van gegevens op grond van de bestaande beklagregeling voor inbeslaggenomen voorwerpen (artikel 552a Sv). Vanwege het spoedeisende karakter van de beslissing beslist de rechtbank zo spoedig mogelijk. Tegen de

beschikking op het beklag staat voor zowel de klager als de officier van justitie beroep in cassatie open.

De bevoegdheid tot ontoegankelijkmaking van gegevens laat de mogelijkheid onverlet dat de officier van justitie besluit de strafbare feiten te beëindigen door middel van een doorzoeking ter vastlegging van gegevens of een onderzoek in een geautomatiseerd werk. In dit wetsvoorstel wordt tevens de bevoegdheid voorgesteld van onderzoek in een geautomatiseerd werk. Indien bij de doorzoeking ter vastlegging van gegevens of het onderzoek in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is begaan, kan de officier van justitie op grond van het voorgestelde artikel 126cc, vijfde en zesde lid, Sv bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

Denkbaar is dat het OM beleidsregels opstelt over de toepassing van de in dit wetsvoorstel voorziene bevoegdheid van de officier van justitie om, met een machtiging van de rechter-commissaris, de ontoegankelijkmaking van gegevens te bevelen. Daarbij is – in verband met de omstandigheid dat de inzet van het strafrecht ultimum remedium is – van betekenis dat benadeelden in bepaalde gevallen ook andere wegen kunnen bewandelen om gegevens van het internet te weren. Zo biedt het Wetboek van Burgerlijke Rechtsvordering een regeling om inbreuken op intellectueel eigendom aan te pakken (artikel 1019 e.v. Rv). Deze regeling maakt het mogelijk dat de rechtbank, in sommige gevallen zelfs binnen een uur nadat een verzoek daartoe is ingekomen, de gedaagde partij beveelt om de onrechtmatige activiteiten te beëindigen. Tevens kan worden gewezen op de speciale procedures in de Auteurswet (artikel 26d) en de Wet op de naburige rechten (artikel 15e), waarbij de rechter kan worden verzocht om een internetprovider te bevelen om de inbreuk makende activiteiten van derden te staken.

3.4. De bescherming van grondrechten

Het recht op vrijheid van meningsuiting wordt beschermd door artikel 10 van het EVRM en artikel 7 van de Grondwet. Het EVRM bepaalt dat aan de uitoefening van dit recht bepaalde formaliteiten, voorwaarden, beperkingen of sancties kunnen worden verbonden, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen. Zoals ook in paragraaf 2.9.1. ten aanzien van artikel 8 van het EVRM is uiteengezet, wordt de noodzaak tot de inzet van een bevoegdheid waarmee dit recht kan worden beperkt mede bepaald aan de hand van de beginselen van proportionaliteit en subsidiariteit. Ook moet de regeling voldoende precies zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden bevoegdheden mogen worden toegepast. De regeling moet bovendien waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid.

De in dit wetsvoorstel opgenomen bevoegdheid van het voorgestelde artikel 125p Sv voldoet aan deze eisen. Zoals in paragraaf 3.1. is beschreven gaat het om een bestaande bevoegdheid die in dit wetsvoorstel vanuit wetssystematisch oogpunt van het Wetboek van

Strafrecht (artikel 54a Sr) wordt overgeheveld naar het Wetboek van Strafvordering. Het doel van de bevoegdheid is om in die gevallen waarin de aanbieder van een communicatiedienst niet bereid is om op basis van de NTD-gedragscode de gegevens ontoegankelijk te maken, een het bevel kan worden opgelegd tot het ontoegankelijk maken van gegevens met het oog op de beëindiging van het strafbare feit of de voorkoming van nieuwe strafbare feiten. De bevoegdheid vormt daarmee een waardevolle wettelijke aanvulling op het instrument van zelfregulering.

Voorts zijn in de regeling de omstandigheden opgenomen waaronder de bevoegdheid kan worden toegepast. Zo moet er sprake zijn van een verdenking van een ernstig strafbaar feit en moet de bevoegdheid dienen tot beëindiging van een strafbaar feit of het voorkomen van nieuwe strafbare feiten.

Ten slotte biedt de regeling waarborgen tegen een willekeurige inmenging van de overheid in het persoonlijke leven van de burger en tegen misbruik van de bevoegdheid. Het bevel kan uitsluitend aan de aanbieder van een communicatiedienst worden gericht op grond van een voorafgaande machtiging van de rechter-commissaris. Daardoor is in rechterlijke tussenkomst voorzien. Het bevel van de officier van justitie moet aan bepaalde inhoudelijke eisen voldoen. Dit betekent dat het strafbare feit in verband waarmee de bevoegdheid moet worden toegepast in het bevel moet worden vermeld. Voorts moeten de feiten en omstandigheden in het bevel worden vermeld waaruit blijkt dat ontoegankelijkmaking van de gegevens noodzakelijk is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen. Verder dient het bevel een beschrijving van de gegevens te bevatten die ontoegankelijk moeten worden gemaakt. De regeling voorziet erin dat de rechter-commissaris degene tot wie de vordering is gericht, in de gelegenheid stelt om te worden gehoord.

4. Het wederrechtelijk overnemen en «helen» van gegevens

4.1. Algemeen

Het wetsvoorstel beoogt de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen verder te verbeteren. Daartoe bevat het wetsvoorstel twee elementen:

- Het wordt strafbaar om niet-openbare gegevens die door middel van een geautomatiseerd werk zijn opgeslagen wederrechtelijk met een technisch hulpmiddel over te nemen (artikel 138c Sr);
- Het wordt strafbaar om niet-openbare gegevens die door misdrijf zijn verkregen voorhanden te hebben of bekend te maken (artikel 139g Sr).

Met de eerstgenoemde strafbaarstelling – betreffende het wederrechtelijk overnemen van gegevens – wordt een betere bescherming geboden tegen het overnemen van gegevens uit een geautomatiseerd werk in de gevallen waarin de gegevens gekopieerd zijn en de rechthebbende dus de beschikking houdt over de gegevens. De rechthebbende heeft echter geen invloed op het gebruik dat vervolgens van de overgenomen gegevens kan worden gemaakt, waardoor hij benadeeld kan worden.

Met de als tweede genoemde strafbaarstelling wordt strafrechtelijke aansprakelijkheid gecreëerd van degene die dergelijke gegevens voorhanden heeft of bekend maakt. Langs deze weg wordt het «helen» van de desbetreffende gegevens strafbaar gesteld. Hiermee wordt uitvoering gegeven aan een toezegging aan de Tweede Kamer om heling van gegevens strafbaar te stellen (Kamerstukken II 2008/09, 28 684, nr. 232, blz. 4). Strafbaarstelling van «heling» van gegevens is van belang in situaties waarin niet aangetoond kan worden dat de persoon die deze gegevens bekend maakt degene is die deze gegevens zelf heeft overge-

nomen, al dan niet na in een geautomatiseerd werk te zijn binnengedrongen (de computervredebreuk, strafbaar gesteld in artikel 138ab Sr).

De beide voorgestelde strafbaarstellingen waren opgenomen in een conceptwetsvoorstel dat reeds eerder in consultatie is gegeven. Zij zullen in dit hoofdstuk in hun onderlinge samenhang worden besproken.

4.2. De voorgestelde strafbaarstellingen

Met het voortschrijden van de informatie- en communicatietechnologie wordt het steeds eenvoudiger om gegevens uit een computer over te nemen en vervolgens op het internet te zetten. Daardoor kan het gebeuren dat vertrouwelijke gegevens snel worden verspreid en voor grote groepen mensen toegankelijk worden. Het is bovendien niet eenvoudig om via het internet verspreide gegevens daarvan volledig verwijderd te krijgen. De technologische ontwikkelingen nopen tot een verdere strafrechtelijke bescherming van gegevens. Het uit een computer overnemen van gegevens over personen, en die gegevens vervolgens op het internet zetten, zijn verwerpelijke gedragingen waartegen adequaat strafrechtelijk moet kunnen worden opgetreden, vooral met het oog op bescherming van de persoonlijke levenssfeer van degene wiens gegevens het betreft. De personen die zich aan dergelijke handelingen schuldig maken, kunnen weten dat het hier om verwerpelijke gedragingen gaat. Dit is niet alleen van belang voor de bescherming van de persoonlijke levenssfeer. De strafbaarstelling van het voorhanden hebben van door misdrijf verkregen gegevens is ook van belang voor gevallen waarin een verdachte waardevolle gegevens voorhanden heeft, zoals bankrekeningnummers of wachtwoorden, die eerder door misdrijf zijn verkregen. In veel gevallen is computercriminaliteit gericht op het wederrechtelijk vergaren van gegevens en het vervolgens gebruiken van deze gegevens bij het plegen van andere misdrijven. Het inbreken in computers van bedrijven om gegevens over creditcards te achterhalen of het door middel van het zogenaamde phishen (het opzetten van een valse website) ontfutselen van bancaire gegevens en pincodes zijn hier inmiddels bekende voorbeelden van. Phishing (of: identity theft) is strafbaar als een vorm van oplichting (artikel 326 Sr). Vereist is dat een persoon door middel van – kort gezegd – misleiding wordt gebracht tot de afgifte van een goed of van gegevens. Het is niet (meer) vereist dat deze gegevens een geldswaarde in het handelsverkeer hebben.

Gebleken is dat het thans niet mogelijk is een persoon te vervolgen voor «heling» van gegevens die door dergelijke misdrijven zijn verkregen. Het College van procureurs-generaal heeft – bij gelegenheid van de consultatie over het ontwerp van het aan de Wet van 12 juni 2009, Stb. 245 ten grondslag liggende wetsvoorstel – aandacht gevraagd voor de onmogelijkheid iemand te vervolgen voor het «helen» van gegevens (Kamerstukken II 2007/08, 31 386, nr. 3, blz. 2). Bij verschillende gelegenheden is gebleken dat behoefte bestaat aan een dergelijke mogelijkheid. Dit betrof volgens het College onder meer een geval waarbij gegevens door computervredebreuk uit een e-mailbox waren gekopieerd, en vervolgens aan een derde doorgegeven. Deze derde heeft de gegevens, ondanks dat vrijwel vaststond dat hij moest weten dat zij door misdrijf waren verkregen, in ontvangst genomen en door middel van het internet gepubliceerd. Omdat het in deze zaak om (gekopieerde) gegevens ging, en niet om een goed, kon deze derde niet strafrechtelijk aansprakelijk worden gesteld voor heling van een goed. De hacker kon worden vervolgd wegens computervredebreuk (artikel 138ab Sr). Inmiddels hebben ook andere gevallen in de media de nodige aandacht gekregen, zoals de publicatie op het internet van door computervredebreuk verkregen digitale naaktfoto's van een bekende presentatrice. Naar

aanleiding van dit geval zijn Kamervragen gesteld over de noodzaak om «heling» van gegevens strafbaar te stellen. Bij de beantwoording van die vragen is aangegeven dat strafbaarstelling van heling van gegevens bij het onderzoek van de knelpunten in het juridisch instrumentarium zal worden betrokken en dat de mogelijkheden voor een juridische vormgeving van een dergelijke strafbepaling zullen worden onderzocht (Handelingen II 2007/08, nr. 888).
In zijn advies maakt de korpschef van de politie melding van het aantreffen van grote hoeveelheden gegevens op plaatsen waarvoor geen redelijke verklaring is, zoals de creditcardgegevens van honderden of duizenden personen bij iemand die geen webwinkel heeft. Met de voorgestelde strafbaarstelling kunnen professionele tussenhandelaren, die op grote schaal via botnets verzamelde gegevens verder verhandelen aan organisaties met de mogelijkheid deze gegevens te gelde te maken, strafrechtelijk worden aangepakt.

Burgers, bedrijven en de overheid zijn zich in toenemende mate bewust van de gevaren die aan het misbruik van gegevens verbonden zijn en investeren het nodige om hun gegevens tegen onrechtmatige toegang en gebruik te beschermen. Gelet op de maatschappelijke belangen die op het spel staan bij het onrechtmatige bezit of gebruik van gegevens is het van belang dat de strafrechtelijke bescherming tegen misbruik van gegevens verder wordt verstrekt. Voor een vermindering van de prikkel om systemen goed te beveiligen behoeft naar mijn oordeel niet te worden gevreesd, omdat burgers en bedrijven zich voldoende bewust zijn van het belang van een adequate gegevensbeveiliging. Bovendien is het ook voor het misdrijf van computervredebreuk – met de inwerkingtreding van de Wet computercriminaliteit II – niet langer vereist dat een beveiliging wordt doorbroken. De strafbepalingen van diefstal en verduistering van goederen – uit een woning of gebouw – zijn evenmin gebonden aan een dergelijk vereiste.

Met de Wet computercriminaliteit is er destijds voor gekozen om gegevens begripsmatig afzonderlijk te behandelen en niet gelijk te stellen aan een «goed» (Kamerstukken II 1989/90, 21 551, nr. 3, blz. 3). Ook in de jurisprudentie van de Hoge Raad is de gelijkstelling van gegevens aan een goed afgewezen (HR 3 december 1996, NJ 1997, 574). Doorslaggevend argument is dat een «goed» individualiseerbaar is en dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft. Gegevens kunnen echter worden overgenomen zonder dat de rechthebbende de beschikkingsmacht over de gegevens verliest. De rechthebbende kan echter geen invloed uitoefenen op het gebruik dat vervolgens van de overgenomen gegevens wordt gemaakt, waardoor hij benadeeld kan worden als de gegevens worden geopenbaard of anderszins worden aangewend op een wijze waardoor zijn belangen worden geschaad. Daar waar de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht is strafvervolging op grond van diefstal volgens enkele uitspraken van feitenrechters niet uitgesloten. Een voorbeeld hiervan betreft de diefstal van een virtueel amulet en een virtueel masker uit een online computerspel (HR 31 januari 2012, LJN BQ9251, NJ 2012, 536).

Het onderscheid dat met de Wet computercriminaliteit is gemaakt tussen het begrip goed en het begrip gegevens heeft ertoe geleid dat in het Wetboek van Strafrecht en het Wetboek van Strafvordering specifieke bepalingen zijn opgenomen met betrekking tot gegevens. Zo kent het Wetboek van Strafrecht afzonderlijke strafbaarstellingen van computervredebreuk (artikel 138ab Sr), het wederrechtelijk aftappen of opnemen van gegevens (artikel 139c Sr), het beschikken over of bekend maken van gegevens die zijn afgetapt, opgenomen of afgeluisterd (artikel 139e Sr),

het «vernielen» van gegevens (artikelen 350a en 350b Sr), het bekend maken of uit winstbejag gebruiken van gegevens over een onderneming (artikel 273 Sr) alsmede strafbaarstelling van de persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of -dienst en die wederrechtelijk niet voor hem bestemde gegevens overneemt (artikel 273d Sr).

In lijn met de keuze die destijds bij de Wet computercriminaliteit en de Wet computercriminaliteit II is gemaakt, is ervoor gekozen de benodigde verbeteringen in de strafrechtelijke bescherming van gegevens door te voeren in de strafbepalingen die in de Vijfde Titel van het Tweede Boek van het Wetboek van Strafrecht zijn opgenomen. Het – in het algemeen – strafbaar stellen van het wederrechtelijk overnemen van gegevens die zijn opgeslagen door middel van een geautomatiseerd werk sluit aan bij de in die titel opgenomen strafbaarstelling van het wederrechtelijk aftappen of opnemen van dergelijke gegevens (artikel 139c Sr). Bovendien is het overnemen van gegevens uit een geautomatiseerd werk door iemand die daarin wederrechtelijk is binnengedrongen ook reeds in die titel strafbaar gesteld (artikel 138ab, tweede lid, Sr). Het wederrechtelijk overnemen van gegevens is voorts, zoals hierboven werd aangestipt, strafbaar gesteld voor zover dit gebeurt door een persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of -dienst (artikel 273d Sr). De door het voortschrijden van de informatie- en communicatietechnologie wenselijke versterking van de strafrechtelijke bescherming van gegevens brengt mee dat het wederrechtelijk overnemen van gegevens in het algemeen strafbaar wordt gesteld.

Voor strafbaarheid van het wederrechtelijk overnemen van gegevens is niet – zoals in artikel 138ab, tweede lid, Sr – vereist dat het geautomatiseerde werk waaruit de gegevens worden overgenomen, is binnengedrongen. Met andere woorden: de gegevens behoeven niet door computervredebreuk te zijn verkregen. De voorgestelde strafbepaling is, in aanvulling op de strafbaarstelling van computervredebreuk, vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot niet-openbare gegevens van een computer, en deze gegevens wederrechtelijk overneemt. Daarbij kan worden gedacht aan de werknemer die gegevens waartoe hij uit hoofde van zijn functie toegang heeft, kopieert met de bedoeling deze voor zichzelf of voor een ander te gebruiken. Om deze reden wordt artikel 139c Sr in dit wetsvoorstel zo gewijzigd dat niet alleen het opnemen van gegevensoverdracht (stromende gegevens) maar ook het wederrechtelijk overnemen van opgeslagen gegevens – in het algemeen – strafbaar wordt. Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen. Er is dan als het ware sprake van «verduistering» van gegevens, met dien verstande dat de rechthebbende de beschikkingsmacht over de gegevens behoudt, in welk geval strafvervolging op grond van artikel 321 Sr niet mogelijk is omdat in een dergelijk geval van een goed geen sprake is. Met het gebruik van de term «overnemen» wordt tot uitdrukking gebracht dat niet is vereist dat de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht. Het opzettelijk en wederrechtelijk overnemen van de gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, vormt daarmee een zelfstandige strafbare gedraging.

Verder acht ik het wenselijk de gedraging strafbaar te stellen die kan worden omschreven als het «helen» van de hier besproken gegevens. Met het voorgestelde artikel 139g Sr, dat voortbouwt op het huidige artikel 139e Sr, wordt degene strafbaar die niet-openbare gegevens, die

door misdrijf zijn verkregen, verwerft, voorhanden heeft, aan een ander ter beschikking stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt. Hiermee wordt een voorziening getroffen voor de gevallen waarin iemand gegevens voorhanden heeft die zijn verkregen uit een misdrijf dat door een ander is begaan of waarin niet kan worden bewezen dat degene die de gegevens voorhanden heeft deze zelf door misdrijf heeft verkregen, bijvoorbeeld door het wederrechtelijk overnemen van de gegevens, al dan niet door middel van computervredebreuk. Zo worden personen strafbaar die gegevens, die uit de computer van anderen zijn ontvreemd, bekend maken aan een ander, verkopen of op internet plaatsen. Hiermee zal ook degene die zich erop beroept deze gegevens niet zelf te hebben ontvreemd maar van een derde te hebben verkregen, strafbaar zijn. Het is daarbij niet per sé noodzakelijk dat de dader weet dat de gegevens door misdrijf zijn verkregen; voldoende is dat hij redelijkerwijs moet vermoeden dat dit het geval is.

De strafbaarstelling van zowel het wederrechtelijk overnemen van gegevens als van het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens heeft uitsluitend betrekking op niet-openbare gegevens. Hiermee worden gegevens bedoeld die niet voor het publiek beschikbaar zijn. Gegevens die op het internet zijn geplaatst, zijn openbaar mits het publiek toegang heeft tot de internetpagina waar de teksten zijn weergegeven (vgl. Hof Amsterdam 23 november 2009, NJFS 2010,29). Het downloaden van openbare gegevens van internet is dus niet strafbaar op grond van deze strafbepalingen. Hiervoor kan worden verwezen naar de artikelsgewijze toelichting op artikel 139g Sr (Artikel I, onderdeel E). De voorgestelde strafbaarstelling laat de mogelijkheid van civielrechtelijk optreden door het slachtoffer, op grond van onrechtmatige daad, onverlet.

Samenvattend: met de voorgestelde artikelen 138c en 139g Sr wordt de rechthebbende van gegevens een betere bescherming geboden tegen personen die de gegevens waar zij rechtmatig toegang toe hebben overnemen, zonder dat er sprake is van computervredebreuk. Tevens wordt voorzien in een strafbaarstelling van een gedraging die zou kunnen worden aangemerkt als «heling» van dergelijke gegevens.

Overwogen is het wederrechtelijk overnemen van niet-openbare gegevens, alsmede het voorhanden hebben of bekend maken van door misdrijf verkregen gegevens, strafbaar te stellen als diefstal, verduistering en heling (artikelen 310, 321, 416 en 417bis Sr). Nadeel daarvan zou zijn dat zou worden afgeweken van de keuze uit de Wet computercriminaliteit en de Wet computercriminaliteit II om gegevens niet aan een goed gelijk te stellen. Het strafbaar stellen van diefstal of verduistering van gegevens is een minder geschikte oplossing als de gegevens zijn gekopieerd en de rechthebbende de beschikkingsmacht daarover dus niet heeft verloren. Als de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, is volgens de hierboven bedoelde uitspraken van enkele feitenrechters sprake van diefstal van een goed en valt dit gedrag onder artikel 310 Sr in zijn huidige vorm. Voorts zou een gelijkstelling van gegevens met goederen in de artikelen betreffende diefstal, verduistering en heling leiden tot een aanzienlijke overlap met de verschillende andere (al bestaande) artikelen betreffende gegevens (namelijk de artikelen 139c, 139e, 273 en 273d Sr). Hiermee is tevens ingegaan op de vraag van de NVvR, waarom ter zake van deze strafbepaling geen aansluiting is gezocht bij de strafbepaling van artikel 310 Sr. Zoals hierboven reeds aan de orde is gekomen, is die aansluiting vanuit oogpunt van de wetssystematiek gecompliceerd en minder goed verenigbaar met het onderscheid tussen het begrip «goed» en het begrip «gegevens» in het Wetboek van Strafvordering.

4.3. De wederrechtelijkheid

Het overnemen van gegevens is in het voorgestelde artikel 138c Sr alleen strafbaar voor zover dit wederrechtelijk is. Uit de consultatie over het concept van het eerdere wetsvoorstel bleek de wens om een nadere toelichting op de wederrechtelijkheid. Allereerst ontbreekt de wederrechtelijkheid in het geval dat aangenomen mag worden dat de gegevens met toestemming van de rechthebbende zijn overgenomen. Als een medewerker in het kader van het thuiswerken gegevens uit een computer van het werk mee naar huis neemt op een usb-stick, is dit niet wederrechtelijk en daarmee niet op grond van het voorgestelde artikel 138c Sr strafbaar als dit gebeurt met toestemming van de werkgever en/of voldoet aan door de werkgever gestelde regels. Daarnaast ontbreekt de wederrechtelijkheid wanneer op rechtmatige wijze uitvoering wordt gegeven aan wettelijke bevoegdheden tot het overnemen van gegevens. Te denken valt aan de in artikel 125i Sv omschreven bevoegdheid tot een doorzoeking ter vastlegging van gegevens. Naar aanleiding van het advies van het College van procureurs-generaal kan nog worden verwezen naar een uitspraak van de rechtbank Oost-Brabant in een strafzaak rond computervredebreuk, strafbaar gesteld in artikel 138ab Sr (ECLI:NL:RBOBR:2013:BZ1157). In het vonnis stelt de rechtbank voorop dat elke inbreuk op een geautomatiseerd werk zonder toestemming van de rechthebbende strafbaar is, tenzij er onder zeer bijzondere omstandigheden hogere belangen zijn die een dergelijke inbreuk in volle omvang kunnen rechtvaardigen. Bij de beoordeling of in deze zaak sprake is van dergelijke bijzondere omstandigheden die het wederrechtelijk karakter aan het handelen van verdachte doen ontvallen, zijn naar het oordeel van de rechtbank, mede gelet op het bepaalde in artikel 10 van het EVRM, drie factoren van belang. Ten eerste moet worden beoordeeld of verdachte heeft gehandeld in het kader van een wezenlijk maatschappelijk belang. Bij bevestigende beantwoording van deze vraag moet vervolgens worden bezien of het handelen van verdachte proportioneel was (ging verdachte niet verder dan noodzakelijk was om zijn doel te bereiken) en of er geen andere, minder vergaande, manier(en) was/waren om het door verdachte beoogde doel te kunnen bereiken (subsidiariteit). In casu oordeelde de rechtbank dat het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens een wezenlijk maatschappelijk belang kan dienen en achtte de rechtbank het inloggen op een website en het vervolgens raadplegen van enkele dossiers niet wederrechtelijk. Wel achtte de rechtbank het verdere handelen van de verdachte, het meerdere malen inloggen en uitprinten van gegevens en het inschakelen van de media, in strijd met de proportionaliteit en subsidiariteit.

Tijdens de over het concept van het eerdere wetsvoorstel gehouden consultatie is van verschillende zijden gewezen op de mogelijkheid dat wanneer journalisten of klokkenluiders door misdrijf verkregen gegevens via de krant of het internet bekend maken, dit gerechtvaardigd kan zijn. Voorop gesteld kan worden dat van strafbaarheid van journalisten en klokkenluiders geen sprake behoort te zijn wanneer bekendmaking van de gegevens in het algemeen belang noodzakelijk is. Indien bekendmaking in het algemeen belang noodzakelijk is, zijn ook personen die betrokken zijn bij websites die informatie door middel van het internet openbaar maken, en de aanbieders die toegang bieden tot deze websites, van strafbaarheid uitgesloten. Het wetsvoorstel beoogt niet te voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders, of van degenen die hen daarbij faciliteren. In dit verband kan worden gewezen op het recht op vrije nieuwsgaring dat voortvloeit uit onder andere de artikelen 7 van de Grondwet en 10 van het EVRM. Het is wenselijk om met het oog daarop een zelfstandige waarborg in de wet op te nemen voor degene die te goeder trouw heeft kunnen aannemen dat

het algemeen belang bekendmaking van de door misdrijf verkregen gegevens vereiste (zie het tweede lid van het voorgestelde artikel 139g Sr). Een vergelijkbare waarborg is opgenomen in artikel 273 Sr dat betrekking heeft op bekendmaking van door misdrijf verkregen bedrijfsgegevens. Langs deze weg wordt bereikt dat bij de beslissing of vervolging moet worden ingesteld en bij de beslissing van de rechter of van strafbaarheid sprake is, op basis van een expliciete bepaling rekening kan worden gehouden met conflicterende belangen: aan de ene kant het recht op een vrije nieuwsgaring en aan de andere kant het recht op bescherming van gegevens. In dit verband kan ook worden gewezen op de jurisprudentie waarbij voor de beantwoording van de vraag of door strafvervolging en veroordeling wegens een in het kader van een journalistiek onderzoek gepleegd strafbaar feit een noodzakelijke inbreuk wordt gemaakt op de journalistieke vrijheid van meningsuiting, de plichten en verantwoordelijkheid van degene die met een beroep op zijn vrijheid van meningsuiting dat feit pleegde moeten worden meegewogen. Journalisten kunnen in beginsel niet op basis van de hun door artikel 10 van het EVRM gegeven bescherming worden ontslagen van hun verplichting de door de strafwet getrokken grenzen in acht te nemen. Het door artikel 10 van het EVRM gewaarborgde recht op vrijheid van meningsuiting kan echter dwingen tot het maken van een uitzondering op dit uitgangspunt (HR 26 maart 2013, LJN BY3752).

Opmerking verdient dat de zelfstandige waarborg alleen behoeft te worden ingeroepen als de gegevens door misdrijf zijn verkregen. Daarvan is geen sprake als de gegevens eerder met instemming van de rechthebbende zijn overgenomen.

De in het voorgestelde tweede lid opgenomen uitzondering van de strafbaarheid strekt zich uit tot de in het voorgestelde eerste lid strafbaar gestelde handelingen. In het conceptwetsvoorstel dat in consultatie is gegeven was deze uitzondering beperkt tot de bekendmaking van de gegevens. Tijdens over het thans voorliggende wetsvoorstel gehouden consultatie is er door de NOvA en BoF op gewezen dat daardoor klokkenluiders die bepaalde gegevens hebben overgenomen strafbaar zouden zijn, ook als de journalist die de gegevens publiceert niet strafbaar is op grond van deze uitzondering. Ook een werknemer die belastend materiaal overneemt om dit aan de politie te overhandigen zou strafbaar zijn, vanwege het voorhanden hebben van de gegevens. Naar aanleiding van deze adviezen is de tekst van het voorgestelde tweede lid verruimd, zodat degene niet strafbaar is die te goeder trouw heeft kunnen aannemen dat het algemeen belang een in het voorgestelde eerste lid strafbaar gestelde handeling vereiste.

5. De verruiming van de strafbaarheid van grooming en van verleiding van minderjarigen tot ontucht

Dit onderdeel is ingevoegd na de consultatie over het oorspronkelijke conceptwetsvoorstel, omdat het belang van een adequate bestrijding van het seksueel benaderen van kinderen door volwassenen via internet noopt tot een onverwijlde aanpassing van de strafbaarstelling van verleiding van minderjarigen en grooming. Vanuit inhoudelijk oogpunt is er sprake van een nauwe relatie met dit wetsvoorstel omdat de strafbare gedragingen met behulp van het internet worden gepleegd.

De ontwikkeling van de informatietechnologie, zoals internet en de mobiele telefonie, biedt volwassenen nieuwe mogelijkheden om kinderen te benaderen voor seksuele doeleinden. Hierbij wordt door volwassenen gedrag vertoond waarmee kinderen worden aangemoedigd om naakt poseren te poseren voor een webcam of andere ontuchtige handelingen

voor een webcam te verrichten. Ook komt het voor dat volwassenen kinderen proberen te verleiden tot een ontmoeting, met als doel het plegen van seksueel misbruik, of dat kinderen met het beeldmateriaal worden gechanteerd tot het verrichten van verdergaande seksuele handelingen. Het gaat hier om vanuit maatschappelijk oogpunt bezien zeer schadelijke verschijnselen.

Het op 25 oktober 2007 te Lanzarote tot stand gekomen Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (Trb. 2008, 58) verplicht in artikel 23 van tot strafbaarstelling van «grooming». Hieronder wordt verstaan het benaderen en verleiden van een kind met als uiteindelijk doel het plegen van seksueel misbruik met dat kind. Bepaalde vormen van grooming kunnen onder de delictsomschrijving van artikel 248a Sr worden gebracht. Daarbij gaat het om situaties waarin een minderjarige via internet met gebruik van middelen (giften, beloften of misbruik van uit feitelijke verhoudingen voortvloeiend overwicht) wordt aangezet tot het aannemen van seksueel getinte houdingen of het plegen van seksuele handelingen met zichzelf of met een derde en dit voor de verdachte te zien is op een webcam. Gedragingen die niet resulteren in het plegen van een feitelijke seksuele handeling of een begin van uitvoering daartoe, vallen evenwel buiten de reikwijdte van artikel 248a Sr (zie ook: Kamerstukken II 2008/09, 31 810, nr. 3). Voor die gedragingen is ter uitvoering van het Verdrag een strafbaarstelling in artikel 248e Sr inzake grooming geïntroduceerd. Ingevolge artikel 248e Sr is niet vereist dat het contact op het internet daadwerkelijk leidt tot fysiek contact tussen kind en dader. De nadruk ligt meer op de fase waarin het kind via internet of andere communicatiemiddelen, bijvoorbeeld door middel van chat- of e-mailverkeer door de dader wordt bewerkt en verleid. De strafbaarstelling vereist dat het gedrag van de dader zich concretiseert tot een voorstel tot een ontmoeting met het kind, gevolgd door een handeling gericht op het verwezenlijken van die ontmoeting.

Om het benaderen van kinderen voor seksuele doeleinden via internet of andere communicatiemiddelen te bestrijden zou in theorie denkbaar zijn dat gebruik wordt gemaakt van een minderjarige die passief optreedt en als lokvogel fungeert. Het behoeft echter nauwelijks betoog dat dit volstrekt ongewenst is, omdat de minderjarige alsdan wordt geconfronteerd met de gedragingen waartegen hij of zij juist beschermd zou moeten worden. Om grooming te bestrijden en groomers op te sporen maakte de politie tot voor kort gebruik van een zogenaamde «lokpuber». Dit betreft een politiefunctionaris die zich als een kind onder de zestien jaar voordoet. In het geval de verdachte, in de veronderstelling verkerend met een kind onder de zestien jaren contact te hebben, een ontmoeting voorstelde met het oogmerk ontuchtige handelingen te verrichten of een afbeelding van een seksuele gedraging te vervaardigen waarbij degene aan wie de ontmoeting is voorgesteld is betrokken, mogelijkerwijs gevolgd door een handeling gericht op het verwezenlijken van die ontmoeting, kwam de politie in actie en ging het OM over tot vervolging.

Inmiddels is in de rechtspraak geoordeeld dat de verdachte van grooming niet strafbaar is als degene die in de tekst van het huidige artikel 248e Sr wordt aangeduid als de persoon die de leeftijd van zestien jaren nog niet heeft bereikt, in werkelijkheid zestien jaar of ouder is en dat het daarbij niet uitmaakt of de verdachte met betrekking tot die leeftijd in een andere veronderstelling verkeerde of mocht verkeren (Rechtbank 's-Gravenhage 14 september 2012, ECLI:NL:RBSGR:2012:BX8188, bevestigd door Gerechtshof Den Haag, 25 juni 2013, ECLI:NL:GHDHA:2013:2302). Het Hof oordeelde, met verwijzing naar de parlementaire geschiedenis bij de totstandkoming van artikel 248e Sr, dat voor een strafbaar handelen in de

zin van dit artikel rechtens als voorwaarde heeft te gelden dat het beoogde slachtoffer van dat feit de leeftijd van zestien jaren nog niet heeft bereikt. De intenties aangaande de leeftijd zijn in dit verband niet doorslaggevend, aldus het Hof. Het voorgaande bracht het Hof tot de conclusie dat niet tot een bewezenverklaring kon worden gekomen. Met deze jurisprudentie wordt de bestaande lijn gevolgd dat, bij het gebruik van de constructie «weet of redelijkerwijs moet vermoeden», de omstandigheid waarop die subjectieve bestanddelen betrekking hebben in casu, de leeftijd van zestien jaren, eerst objectief dient vast te staan.

Het feit dat de inzet van de «lokpuber» niet kan bijdragen aan het bewijs van het plegen van grooming levert serieuze problemen op voor de opsporing van dit delict. Inmiddels is de inzet van lokpubers stilgelegd. Deze situatie doet ernstig afbreuk aan de bescherming van kinderen tegen grooming. In verband hiermee is er aanleiding om de delictsomschrijving alsnog te bezien, zoals toegezegd in de memorie van toelichting bij de wet van 26 november 2009 (Kamerstukken II 2008/09, 31 810, nr. 3, blz. 10).

Hiervoor kwam al aan de orde dat bepaalde vormen van «grooming» onder de delictsomschrijving van artikel 248a Sr (verleiding van een minderjarige tot ontucht) vallen. In verband met het gebruik van dezelfde constructie ten aanzien van de leeftijd van der minderjarige als in de delictsomschrijving van grooming, is de inzet van de lokpuber momenteel evenmin mogelijk bij de opsporing van het delict verleiding van een minderjarige tot ontucht.

Uit een advies van het College van procureurs-generaal komt naar voren dat in de opsporingspraktijk eveneens behoefte is aan de inzet van de lokpuber bij de opsporing van het delict verleiding van een minderjarige tot ontucht (248a Sr). Het College van procureurs-generaals wijst erop dat internet en sociale media tegenwoordig een grote rol spelen bij het ronselen van slachtoffers voor seksueel misbruik. Groomers, waaronder zogenaamde «loverboys», proberen meisjes te verleiden om zich voor de webcam uit te kleden en seksuele handelingen te verrichten. Het beeldmateriaal wordt vervolgens gebruikt om het slachtoffer onder druk te zetten om steeds opnieuw voor de camera te komen of verdergaande seksuele handelingen te verrichten.

Om de politie in staat te stellen om in een vroegtijdig stadium dergelijke praktijken aan te pakken, beveelt het College van procureurs-generaal aan om artikel 248a Sr, gelijk artikel 248e, Sr te wijzigen, zodat de inzet van de lokpuber ook ten behoeve van de opsporing van seksuele verleiding van een minderjarige mogelijk wordt.

In het licht van bovenstaand advies wordt voorgesteld om de artikelen 248a en 248e Sr zodanig te wijzigen dat dat kinderen beter beschermd worden tegen benadering via internet of andere communicatiemiddelen voor seksuele doeleinden. De beschermingsomvang wordt zodanig uitgebreid dat de strafbaarstelling ook ziet op het benaderen voor seksuele doeleinden van iemand die zich voordoet als iemand die de leeftijd van zestien jaren (grooming) of achttien jaren (verleiding van een minderjarige tot ontucht) nog niet heeft bereikt.
De daadwerkelijke betrokkenheid van een minderjarige (bij grooming: beneden de leeftijd van zestien jaren) behoeft niet te worden bewezen. Ook als de persoon die betrokken is ouder is kan sprake zijn van een strafbare gedraging, als bewezen kan worden dat deze zich voordeed als een minderjarige. Met de verruiming van de strafbaarstellingen wordt de inzet van de zogenaamde «lokpuber» mogelijk. Ook kan, anders dan thans het geval is, tot een bewezenverklaring worden gekomen als degene die zich voordoet als de minderjarige een ouder of een oudere broer of zus is

die, bijvoorbeeld op verzoek van het onraad ruikende kind, de chat heeft overgenomen.
Anders dan de Afdeling advisering uit een eerdere versie van de toelichting afleidde, wordt bij de inzet van lokpubers geen gebruik gemaakt van virtuele personen. Voor het leggen van contact via chatsites of via communicatiemiddelen, zoals whatsapp, wordt een profiel of een chatnaam aangemaakt, waaraan een profielfoto gekoppeld kan zijn. Deze profielfoto kan een willekeurige foto of afbeelding zijn. De communicatie vindt plaats met een natuurlijke persoon, een opsporingsambtenaar, die achter het profiel schuil gaat.

De adviezen van het College van procureurs-generaal, de Rvdr, de NVvR en de NOvA hebben, naast het hierboven reeds toegelichte voorstel tot wijziging van artikel 248a Sr, geleid tot het schrappen van de voorgestelde wijziging van artikel 248d Sr. Uit een advies van het College van procureurs-generaal kwam naar voren dat de handeling die onder het voorgestelde artikel 248d Sr zouden moeten vallen, het verrichten van seksuele handelingen voor de webcam door de verdachte zelf, nu al vervolgbaar is op grond van artikel 239 Sr (schennis) of 240a (Sr) (bescherming van jeugdigen onder zestien jaar). Het College van procureurs-generaal heeft er tevens op gewezen dat dit in de praktijk niet een feit is waarvoor een lokpuber wordt ingezet.

Voorts zijn naar aanleiding van een advies van het College enkele wijzigingen in het voorgestelde artikel 248e Sr doorgevoerd. Hiermee wordt tegemoet gekomen aan de kritiek van het College van procureurs-generaal dat het bij wet voorschrijven in artikel 248e Sr dat de chatpartner en de ontmoetingspartner dezelfde persoon moeten zijn in de praktijk tot problemen leidt als gebruik wordt gemaakt van een lokpuber, omdat in het geval van de lokpuber de ontmoeting niet aan een kind beneden de zestien jaren wordt voorgesteld. Ingevolge de voorgestelde delictsomschrijving dient het oogmerk van de verdachte gericht te zijn op het plegen van ontuchtige handelingen waar een persoon bij is betrokken die de leeftijd van zestien jaren nog niet bereikt heeft. De chatpartner en de beoogde ontmoetingspartner hoeven dus niet dezelfde persoon te zijn. Voor het bewijs van het oogmerk is voldoende dat de verdachte aantoonbaar zijn zinnen heeft gezet op willekeurig welke zestienminner. Met de toegevoegde wijziging worden de mogelijke problemen met betrekking tot de bewijsbaarheid, waar het College, de NVvR en de Rvdr naar vragen, ondervangen. Zoals hierboven uiteengezet is het voldoende dat bewezen wordt dat de persoon die wordt benaderd door een verdachte zich voordeed als iemand beneden de leeftijd van zestien en de verdachte het oogmerk had om ontuchtige handelingen te plegen met een persoon die de leeftijd van zestien jaren nog niet heeft bereikt dan wel een afbeelding te vervaardigen van een seksuele gedraging waarbij een persoon die de leeftijd van zestien jaren nog niet heeft bereikt is betrokken.

De NVvR wijst er in haar advies op dat de uitbreiding van de strafbaarstelling van grooming in artikel 248e Sr aan een principieel punt raakt. Volgens de NVvR is toe nu toe steeds het uitgangspunt geweest in de zedenwetgeving dat minderjarigen tegen opdringerige volwassenen beschermd worden. Daarbij is de werkelijke leeftijd van de minderjarige steeds bepalend geweest. Het strafbaar stellen van louter een intentie om een minderjarige te misbruiken is niet in lijn met de huidige uitgangspunten van de zedenwetgeving, aldus de NVvR.
In reactie hierop kan worden opgemerkt dat het uitgangspunt dat aan de strafbaarstelling van kinderporno (artikel 240b Sr) ten grondslag ligt, eveneens verder gaat dan alleen de bescherming van een concreet kind tegen misbruik. De toevoegingen «kennelijk jonger dan achttien jaar» en

«schijnbaar betrokken» in de delictsomschrijving leiden ertoe dat ook als de persoon die te zien is op een afbeelding ouder is dan achttien jaren of er sprake is van een virtueel kind sprake kan zijn van een strafbare gedraging. Het uitgangspunt dat aan de uitbreiding van deze strafbaarstelling ten grondslag lag was dat niet alleen bescherming nodig is tegen misbruik van een concreet kind maar ook tegen gedrag dat kan worden gebruikt om kinderen aan te aanmoedigen of te verleiden om deel te nemen aan seksueel gedrag of gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert (Kamerstukken II 2001/02, 27 745, nr 6). De uitbreiding van de strafbaarstelling van grooming sluit hierbij aan. In de huidige delictsomschrijving van grooming ligt de nadruk op de contactfase en het vooropgezet doel om ontuchtige handelingen te plegen met een kind beneden de zestien. In zoverre is al sprake van een (specifieke) strafbaarstelling van voorbereidingshandelingen. Het wetsvoorstel brengt hierin geen wijziging. Het is nog steeds een vereiste dat de contacten uitmonden in een voorstel tot ontmoeting, zij het dat het voorstel tot ontmoeting nu ook kan worden gedaan aan iemand die zich voordoet als een kind beneden de leeftijd van zestien.
Dat dit, zoals de NVvR opwerpt, de deur zou kunnen openzetten voor burgerinitiatieven om pedofielen op te sporen valt niet geheel uit te sluiten. Bij afweging van alle betrokken belangen, dient het belang van de bescherming van kinderen tegen gedrag op het internet of via communicatiemiddelen dat gebruikt wordt om kinderen te verleiden tot seksuele gedragingen dient mijns inziens het zwaarste te wegen. Het OM zal een prudent vervolgingsbeleid hanteren.

De Rvdr vraagt in zijn advies naar de implicaties van het arrest van het EHRM in de zaak Khudobin (EHRM 26 oktober 2006, EHRC 2007.6) en vraagt waar de grens met uitlokking ligt. Voorts vraagt de Raad of beoogd wordt nadere uitvoeringsregelgeving tot stand te brengen over de gevallen waarin inzet van de lokpuber geoorloofd is. De NOvA heeft principieel bezwaar tegen de systematiek waarmee de inzet van een lokpuber mogelijk wordt gemaakt. Het gaat hier volgens de NOvA in wezen om het mogelijk maken van een opsporingsmethode. Dit behoort volgens de NOvA plaats te vinden via een aanpassing van het Wetboek van Strafvordering.

In de zaak Khubodin tegen Rusland, van 26 oktober 2006, was het geval aan de orde van een onder dekmantel («under cover») opererende agent van politie die aan de klager kenbaar had gemaakt geïnteresseerd te zijn in een dosis heroïne en aan de klager geld had gegeven om die heroïne voor haar te kopen. In de zaak bij het EHRM voerde klager aan dat artikel 6 EVRM was geschonden, omdat hij was uitgelokt door de politie. Het EHRM achtte de klacht gegrond, onder meer omdat naar het oordeel van het Hof sprake was geweest van uitlokking. In Nederland hanteert de Hoge Raad, om te voorkomen dat sprake is van uitlokking, voor de inzet van lokmiddelen onder meer de voorwaarde dat de verdachte door het optreden van de opsporingsambtenaar niet is gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht, het zogenaamde Tallon-criterium (HR 4 december 1979, NJ 1989, 356; zie HR 28 oktober 2008, NJ 2009, 224 voor de inzet van een lokfiets). Op grond van dit criterium dient de verdachte bij de inzet van een «lokpuber» door het optreden van de opsporingsambtenaar niet te worden gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht.

Vooropgesteld kan worden dat opsporingsambtenaren volgens bestendige rechtspraak van de Hoge Raad op basis van algemene taakstellende bepalingen – het betreft de artikel 3 Politiewet 2012 en 141 Sv – onder voorwaarden bevoegd zijn tot het inzetten van «lokmiddelen».

Eén van de voorwaarden is dat de verdachte door het optreden van de opsporingsambtenaar niet wordt gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht (het hiervoor genoemde Tallon-criterium). In de praktijk betekent dit – wat betreft de inzet van de lokpuber – dat een opsporingsambtenaar in beginsel zelf de communicatie niet start, maar afwacht totdat iemand contact met hem legt voor seksuele doeleinden. Voor zover in de opsporingspraktijk gebruik gemaakt gaat worden van bewegende animaties waarachter een opsporingsambtenaar schuilgaat – uit het advies van het College van procureurs-generaal blijkt dat hier momenteel (nog) geen sprake van is – zal het Tallon-criterium in acht genomen dienen te worden.
Bij de huidige stand van de jurisprudentie zie ik geen aanleiding voor een nadere regeling over het de inzet van de lokpuber. Die inzet vindt een toereikende grondslag in de algemene taakstellende bepalingen van opsporingsambtenaren, zoals die in de rechtspraak is genormeerd. Wel zal in het kader van de voorgenomenaanstaande modernisering van het Wetboek van Strafvordering worden bezien of het Tallon-criterium als algemene bepaling van het voorbereidend onderzoek in het wetboek kan worden neergelegd.

De Rvdr wijst op de strafverzwaringsgrond van artikel 248, derde lid, Sr, dat de in de artikelen 248a tot en met 248f Sr bepaalde gevangenisstraffen met een derde kunnen worden verhoogd indien het feit wordt begaan tegen een persoon bij wie misbruik van een kwetsbare positie wordt gemaakt, en acht het wenselijk dat in de toelichting aandacht wordt besteed aan de vraag in hoeverre deze bepaling van toepassing is als de opsporingsambtenaar uitlatingen doet betreffende de kwetsbaarheid van de gepretendeerde minderjarige aangaande seksuele wensen van derden. De inzet van een lokpuber staat in de weg aan toepassing van artikel 248, derde lid, Sr, omdat de lokpuber niet in een kwetsbare positie verkeert. In het geval dat de verdachte de minderjarige benadert op grond van eerdere uitlatingen van de lokpuber namens de minderjarige, bijvoorbeeld als de lokpuber gebruik heeft gemaakt van een account van die minderjarige, kan deze bepaling wel worden toegepast maar dit betreft een tamelijk hypothetische situatie, al was het maar omdat de lokpuber zich van dergelijke uitlatingen zal onthouden. Overigens vormen de normstelling en samenhang van de zedentitel momenteel voorwerp van wetenschappelijk onderzoek. In het de loop van 2015 is een WODC-onderzoek naar de algemene herziening van titel XIV van het Wetboek van Strafrecht opgeleverd. Het onderzoek zal, voorzien van een beleidsreactie, aan de Kamer worden aangeboden. Het door de Rvdr aangekaarte vraagstuk inzake de strafverzwaring, dat verband houdt met de samenhang binnen de zedentitel, maakt hier onderdeel van uit. In die reactie zal hierover een standpunt worden ingenomen.

6. De online handelsfraude

Dit onderdeel is eveneens ingevoegd na de consultatie over het oorspronkelijke conceptwetsvoorstel, omdat de strafbare handelingen worden gepleegd op het internet en het dringend gewenst is dat hiertegen strafrechtelijk kan worden opgetreden. Op grond van de jurisprudentie is dit thans beperkt mogelijk. In antwoord op vragen van de leden Recourt en Van der Steur heb ik aangegeven om in overleg met het OM te bezien of, en zo ja op welke wijze, nieuwe strafrechtelijke mogelijkheden moeten worden gecreëerd (Kamerstukken II 2012/13, Aanhangsel, 2013Z10763 en 2013Z11407).

De handel in goederen en diensten via het internet vindt steeds meer ingang. Zowel bedrijven als particulieren gebruiken het internet als een platform om goederen en diensten te koop aan te bieden. Dit betreft

nieuwe en tweedehands goederen. De koop en verkoop van goederen en het aanbieden en afnemen van diensten via het internet zijn in belangrijke mate gebaseerd op het vertrouwen dat beide partijen de overeengekomen transactie naleven. Als er problemen ontstaan kan de beheerder van de website, via welke de transactie is gesloten, maatregelen treffen tegen de koper of verkoper.

Gedurende de afgelopen jaren vormt de zogenaamde online handelsfraude (of: internetoplichting) in toenemende mate een maatschappelijk probleem. Uit CBS-cijfers over 2013 blijkt dat in 2013 3,1 procent van de Nederlanders van 15 jaar of ouder wel eens opgelicht is bij het verkopen via internet[3]. Bij het landelijk meldpunt internetoplichting (LMIO) van de politie werd in 2014 ruim 7,9 miljoen euro aan internetfraude gemeld bij de politie. In totaal werd bijna 44.000 keer aangifte gedaan.
Veel aangiften hebben betrekking op eenzelfde aanbieding. Het opsporingsonderzoek, dat naar aanleiding van aangiften van online handelsfraude wordt gestart, omvat gemiddeld 180 slachtoffers. Voor de bestrijding van internetoplichting is een goede preventie essentieel. In overleg met de politie nemen de grotere marktpartijen zelf maatregelen die zijn gericht op het weren van malafide aanbieders. Dit blijkt echter niet voldoende om dit verschijnsel adequaat het hoofd te bieden. Er wordt namelijk ook gewerkt met tijdelijke websites, die voor een weekend online gaan en na het weekend offline, waarbij de koper of afnemer wordt verleid tot gedeeltelijke of volledige betaling zonder dat er wordt geleverd. Zodra de kopers merken dat er niet wordt geleverd is de website al uit de lucht en de aanbieder van de goederen of diensten onvindbaar. Kenmerk van dergelijke vormen van handelsfraude is dat er een groot aantal slachtoffers is betrokken en dat de kopers of afnemers de verkoper of aanbieder niet kunnen aanspreken omdat deze voor hen niet of nauwelijks is te achterhalen. Dit impliceert dat het voor hen evenmin mogelijk is de verkoper of aanbieder tot nakoming te manen, dan wel schadevergoeding te vorderen. Voor de politie is de situatie anders, in die zin dat de politie aan de hand van de aangiften of meldingen inzicht verkrijgt in de omvang van de handelsfraude en over strafvorderlijke bevoegdheden beschikt, bijvoorbeeld het vorderen van gegevens bij een bank of een webhost (de aanbieder van de dienst die particulieren of bedrijven ruimte aanbiedt voor het opslaan van informatie, afbeeldingen, of andere inhoud die toegankelijk is via een website) ingeval van verdenking van een strafbaar feit waarvoor voorlopige hechtenis mogelijk is, teneinde de daders op te sporen.

De vervolging van deze vorm van handelsfraude, op grond van het strafbare feit van oplichting (artikel 326 Sr) blijkt tot nu toe beperkt succesvol. In de rechtspraak wordt geoordeeld dat het aanbieden van goederen of diensten via het internet, zonder de intentie tot leveren, niet zonder meer oplichting oplevert. De Rvdr heeft in zijn advies opgemerkt dat verschillende feitenrechters geoordeeld hebben dat dergelijke gedragingen strafbaar zijn op grond van artikel 326 Sr. De jurisprudentie is echter niet eenduidig. Voor oplichting is vereist het aannemen van een valse naam of van een valse hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels. Van een valse hoedanigheid kan sprake zijn als op bedrieglijke wijze gebruik wordt gemaakt van een in het maatschappelijk verkeer geldend gedragspatroon. Een voorbeeld betreft de gast van een restaurant die na afloop van de maaltijd geen geld blijkt te hebben (HR 10-02-1998, NJ 1998, 497). Diverse feitenrechters hebben, op basis van deze jurisprudentie, geoordeeld dat het enkele niet leveren van een goed beschouwd moet worden als het aannemen van een valse

[3] http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/artikelen/archief/2014/2014-4083-wm.htm.

hoedanigheid, omdat hiermee in strijd wordt gehandeld met het goed vertrouwen dat in het maatschappelijk verkeer gebruikelijk is (zie onder meer Hof Arnhem-Leeuwarden 21-06-2013, ECLI:NL:GHARL:2013:4498)[4]. De Hoge Raad heeft evenwel ook geoordeeld dat de enkele omstandigheid dat een persoon zich in strijd met de waarheid voordoet als bonafide huurder, niet oplevert het aannemen van een valse hoedanigheid of een listige kunstgreep (HR 13 november 2001, LJN AD4320 en HR 29 juni 2010, LJN BL8638). Op basis hiervan oordeelde de rechtbank Haarlem dat het te kwader trouw ontvangen van betalingen door kopers, zonder intentie tot levering, niet oplevert het bewegen tot afgifte van geld door het aannemen van een valse hoedanigheid of een valse naam (Rechtbank Noord-Holland ECLI:NL:RBNHO:2013: BZ9266). Ook het Gerechtshof 's-Gravenhage en het Gerechtshof Amsterdam hebben geoordeeld dat het zich voordoen als bonafide verkoper in combinatie met het vragen om vooruitbetaling, niet oplevert het aannemen van een valse hoedanigheid, noch listige kunstgrepen of een samenweefsel van verdichtsels (Gerechtshof 's-Gravenhage, 20-04-2012, ECLI:NL:GHSGR:2012:BW:5086 en 29-08-2013, ECLI:NL:GHDHA:2013:3425 en Gerechtshof Amsterdam, 21-01-02013, ECLI:NL:GHAMS:2013:BY9049).

In 2014 heeft de Hoge Raad (HR 11 november 2014, ECLI:NL:HR:2014:3144) geoordeeld dat het zich in strijd met de waarheid voordoen als bonafide verkoper in combinatie met het verstrekken van onbruikbare contactgegevens aan een wederpartij het aannemen van een valse hoedanigheid kan opleveren. De Hoge Raad bevestigt in deze uitspraak dat de enkele omstandigheid dat iemand zich in strijd met de waarheid voordoet als bonafide verkoper, die in staat is en voornemens is tot levering, niet oplevert het aannemen van een valse hoedanigheid in de zin van artikel 326 Sr. Indien de gedragingen echter meer omvatten en er naast het zich voordoen als betrouwbare verkoper telkens opzettelijk foute namen en e-mailadressen worden gehanteerd met het doel de mogelijkheden tot verhaal te bemoeilijken, dan kunnen deze gedragingen wel worden gekwalificeerd als oplichting in de zin van artikel 326 Sr. In een andere zaak heeft de Hoge Raad het oordeel van het Gerechtshof te Amsterdam (ECLI:NL:GHAMS:2012:982) dat de enkele omstandigheid dat de verdachte via een website goederen te koop aanbood en bestellingen en betalingen van kopers accepteerde in het besef dat hij niet (langer) aan zijn leverings- of restitutieverplichtingen kon voldoen niet kan worden aangemerkt als het aannemen van een valse hoedanigheid als bedoeld in artikel 326 Sr, geen blijkt geeft van een onjuiste rechtsopvatting (ECLI:NL:HR:2014:3546).

Van de deelnemers aan het handelsverkeer wordt gevergd dat zij zorgvuldigheid betrachten bij het aangaan van een overeenkomst en de daaraan verbonden risico's in beginsel zelf dienen te dragen. Bij de totstandkoming van het delict van oplichting kon echter niet worden voorzien dat het handelsverkeer in belangrijke mate via het internet zou verlopen en transacties in toenemende mate «op afstand» worden verricht. Er kan strafrechtelijk worden opgetreden tegen malafide kopers die zich bij herhaling schuldig maken aan het kopen zonder te betalen. Dit betreft de zogenaamde flessentrekkerij (artikel 326a Sr). Er kan echter beperkt strafrechtelijk worden opgetreden tegen malafide verkopers of

[4] Gelijkluidend oordeelden Rechtbank Breda van 1 april 2008 (ECLI:NL:RBBRE:2008:BC8213) en 25 maart 2011 (ECLI:NL:RBBRE:2011:BP9283), Rechtbank Noord-Holland van 2 december 2013 (ECLI:NL:RBNHO:2013:11557), Hof Arnhem-Leeuwarden van 7 juni 2013 (ECLI:NL:GHARL:2013, 4093), Hof Den Bosch van 11 juli 2013 (ECLI:NL:GHSHE:2013:3013), en Rechtbank Noord-Holland, locatie Haarlem, 29 april 2013, ECLI:NL:RBNHO:2013:BZ9266, NJFS2013/156). Voor een uitgebreid overzicht kan worden verwezen naar de conclusie van de procureur-generaal bij het arrest van de Hoge Raad van 9 december 2014 (ECLI:NL:HR:2014:3546).

aanbieders die zich bij herhaling schuldig maken aan het verkopen of aanbieden zonder te leveren. Tegen deze achtergrond meen ik dat er, gelet op de ontwikkeling van het internet, aanleiding bestaat om het OM in staat te stellen vervolging in te stellen bij vormen van grootschalige handelsfraude, waarbij gebruik wordt gemaakt van het internet. De slachtoffers zijn daarbij gebaat, ook omdat zij zich dan ter zake van hun vordering tot schadevergoeding als benadeelde partij in het strafproces kunnen voegen (artikel 51f, eerste lid, Sv). Hierbij moet worden aangetekend dat de strafrechtelijke handhaving van online handelsfraude plaats vindt binnen de algemene handhavingskaders voor financieel-economische criminaliteit, waarbij een geïntegreerde aanpak wordt gehanteerd (preventie, toezicht, bestuursrechtelijke en strafrechtelijke aanpak). De bestrijding van online handelsfraude is een gedeelde verantwoordelijkheid van zowel private- als publieke partijen. Zo hebben private partners er doorgaans beter zicht op waar en op welke wijze fraude het meest wordt voorkomt. Vervolgens wordt beoordeeld wat private partijen zelf kunnen doen om de fraude de te voorkomen en te bestrijden en waar het echt noodzakelijk is dat het OM strafrechtelijk optreedt. Vanwege de schaarse capaciteit voor opsporing en vervolging moeten het OM en de politie prioriteiten stellen en kan niet bij ieder geval van internetfraude worden overgaan tot opsporing en vervolging.

Voorgesteld wordt een gevangenisstraf van ten hoogste vier jaren of een geldboete van de vijfde categorie. Met de voorgestelde strafbedreiging wordt aangesloten bij de strafbedreiging voor oplichting (artikel 326 Sr) en flessentrekkerij (artikel 326a Sr).

7. Financiële paragraaf

Uitvoering van de bevoegdheden in dit wetsvoorstel hebben financiële gevolgen voor de politie die worden opgevangen binnen het totaal beschikbare budget. Ook voor het OM en de rechtspraak zal het wetsvoorstel leiden tot enige werklastgevolgen, met name voor de rechter-commissaris. Bij de politie gaat het niet alleen om de feitelijke ontwikkeling en inzet van onderzoek in een geautomatiseerd werk en het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid, maar ook om de inzet van menskracht. De omvang van dit financiële beslag is nog niet goed te voorzien. De inzet van het onderzoek in een geautomatiseerd werk is geheel nieuw. Vergelijkingen met de inzet van bijvoorbeeld een telefoontap gaan zeker niet op. Aan het onderzoek in een geautomatiseerd werk worden strikte voorwaarden gesteld. Dit brengt met zich mee dat dit onderzoek minder veelvuldig zal worden verricht. Daarnaast kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk mogelijk ook andere vormen van politie-inzet kan vervangen en daarmee middelen kunnen worden bespaard om de investeringen in automatisering binnen de begroting te dekken. Als gevolg van de invoering van dit nieuwe opsporingsinstrument voor de politie zal naar verwachting sprake kunnen zijn van verschuiving van de aanwending van de financiële middelen van de nationale politie binnen het totaal beschikbare budget. De mate waarin is afhankelijk van de verwachtingen van en ervaring met toepassing van het instrument. Dat zal niet alleen gelden voor de feitelijke ontwikkeling en inzet van onderzoek in een geautomatiseerd werk en het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid, maar ook voor de inzet van menskracht. Bij het OM en in de rechtspraak bestaan de gevolgen uit het doen dan wel beoordelen van met name vorderingen tot machtigingen als bedoeld in artikel 126nba Sv (op afstand heimelijk binnendringen in geautomatiseerd werk). De toetsing op rechtmatigheid, proportionaliteit en subsidiariteit zal vooral bij de rechtercommissaris een aanzienlijke inspanning vergen. Ook voor de

zittingsrechter kan het wetsvoorstel werklastgevolgen hebben. Voor het OM geldt net zoals voor de politie dat kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk ook andere bevoegdheden tot het doen van onderzoek door de politie kan vervangen. In het verlengde van nieuwe strafbepalingen zullen ook zittingsrechters met nieuwe zaken te maken krijgen en daarover hebben te beslissen. In welke mate van de ruimere bevoegdheden gebruik zal worden gemaakt, is volgens de Rvdr op voorhand niet te kwantificeren. Vooralsnog gaat de Raad uit van een relatief klein aantal (ten opzichte van het totaal aantal strafzaken) als gevolg waarvan de werklastgevolgen naar verwachting niet van substantiële aard zullen zijn. Uitgangspunt is dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk dekken binnen het reguliere budget.

De nieuwe strafbaarstelling inzake online handelsfraude (artikel 326 Sr) leidt naar verwachting van de Rvdr tot ongeveer vijfenzestig extra zaken op jaarbasis. Het betreft relatief complexe zaken, mede gelet op de vermoedelijk vele slachtoffers en/of benadeelde partijen. De Rvdr verwacht dat deze werklasttoename voor extra kosten zorgt van ongeveer € 500.000 per jaar.

8. De adviezen over het wetsvoorstel

Over het oorspronkelijke conceptwetsvoorstel is advies ontvangen van het College van procureurs-generaal, de korpschef van de politie, de Rvdr, de NVvR, de NOvA, het Cbp en BoF. Over de onderdelen inzake de verruiming van de strafbaarheid van grooming en verleiding van minderjarigen tot ontucht en de strafbaarstelling van de on line handelsfraude is advies ontvangen van het College van procureurs-generaal, de korpschef van de politie, de Rvdr, de NVvR, de NOvA en het Cbp. Daarnaast is het conceptwetsvoorstel op internet gepubliceerd en is een ieder in de gelegenheid gesteld hierop te reageren. Dit heeft ruim vijftig reacties opgeleverd.

Hieronder wordt de inhoud van de adviezen en de reacties naar aanleiding van de internetconsultatie op hooflijnen besproken. De voorstellen op deelterreinen komen elders in deze toelichting aan de orde.

8.1. Het onderzoek in een geautomatiseerd werk

Het College van procureurs-generaal onderstreept dat het van het grootste belang is dat het onderzoek in een geautomatiseerd werk wordt ingevoerd. De ontwikkelingen op het terrein van technologie, internet en communicatie gaan razendsnel en ook criminele maken van gebruik van nieuwe technologieën. In de toekomst zal het praktisch gesproken alleen nog mogelijk zijn om communicatie te onderscheppen op het moment dat deze wordt ingevoerd in de computer, telefoon, of tablet, dan wel op het moment dat de boodschap wordt ontvangen. De bevoegdheden van politie en het OM zijn onvoldoende toegesneden op deze nieuwe ontwikkelingen. Wil de opsporing in staat worden gesteld om gelijke tred te houden met de moderne ontwikkelingen op het gebied van computers en internet dan is deze bevoegdheid onmisbaar.

De Rvdr erkent de in de memorie van toelichting genoemde knelpunten en problemen voor de opsporingspraktijk en onderschrijft de memorie van toelichting voor wat betreft de voorgestelde reikwijdte van de bevoegdheid. De vraag naar mogelijkheden om direct toegang te krijgen tot een geautomatiseerd werk is begrijpelijk. Ook onderschrijft de Raad de expliciete uitsplitsing in het voorgestelde artikel 125nba Sv naar een aantal verschillende doelen waartoe kan worden binnengedrongen,

omdat hiermee wordt bewerkstelligd dat reeds bij het vragen van een machtiging van de rechter-commissaris concreet en helder wordt geformuleerd waarvoor deze ingrijpende bevoegdheid zal worden toegepast.

De NOvA acht de invoering van de voorgestelde bevoegdheid een zeer verstrekkende stap in de verruiming van mogelijkheden om burgers heimelijk te bespieden, terwijl de noodzaak daartoe niet uit de toelichting kan worden afgeleid. Zonder deugdelijke onderbouwing zou een dergelijk vergaand opsporingsmiddel niet moeten worden ingevoerd. Derhalve wijst de NOvA de introductie van het heimelijk binnendringen in zijn geheel af. Anders dan de NOvA zie ik in de ontwikkelingen op het gebied van de informatie- en communicatietechnologie, zoals de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en het gebruik van Cloudcomputing, aanleiding om de bevoegdheden van politie en justitie meer in evenwicht te brengen met de ontwikkelingen binnen de digitale wereld. In paragraaf 2.1. is op deze noodzaak uitgebreid ingegaan.

Het Cbp merkt op dat het bereik van de voorgestelde bevoegdheid zich uitstrekt tot een zeer grote hoeveelheid gegevens, inclusief historische gegevens die op randapparatuur zijn opgeslagen en gegevens die worden uitgewisseld via alle communicatiekanalen waarmee de randapparatuur is verbonden. De bevoegdheid kan ook betrekking hebben op toekomstige gegevens of gegevens die elders, zoals in de Cloud, zijn opgeslagen. De privacy inbreuk betreft daarmee in veel gevallen een grote groep burgers tot wie de verdenking zich niet richt. De bevoegdheid ziet bovendien op alle apparatuur die digitaal kan communiceren. De uitbreiding die de voorgestelde nieuwe bevoegdheid biedt is daarmee ongekend omvangrijk.
Voor wat betreft de noodzaak is in de toelichting onvoldoende geconcretiseerd noch aangetoond waaruit de dringende noodzaak voor de samenleving bestaat die tot het invoeren van deze inbreuk makende maatregel noopt. De dringende noodzaak, als bedoeld in artikel 8 van het EVRM, dient in objectieve bewoordingen onomstotelijk te worden vastgesteld en is in de toelichting onvoldoende onderbouwd. Het Cbp adviseert om de ontbrekende overwegingen alsnog op te nemen. Naar aanleiding van dit advies is de memorie van toelichting aangevuld. Daarbij is nader ingegaan op het onderscheid tussen het versleutelen van bestanden, het versleutelen van communicatiestromen in transit en het opslaan van gegevens in de Cloud. Daarbij kan er nog op worden gewezen dat op het internet een masterscriptie beschikbaar is, waarin wordt geconcludeerd dat het voorgestelde artikel 126nba Sv in beginsel de noodzakelijkheidstoets van artikel 8, tweede lid, van het EVRM kan doorstaan (Hacken als opsporingsbevoegdheid in het licht van artikel 8 lid 2 EVRM: de zoektocht naar een *«fair balance»* tussen opsporing en privacy, Y.J.G.H.L. Straus, blz. 63; http://njb.nl/Uploads/2014/2/Scriptie-Straf-proces-recht-Yannick-Straus-Radboud-Universiteit-Nijmegen---inzending-NJB.pdf). Wat betreft de proportionaliteit miskent het voorstel de omvang van de inbreuk die het gevolg zal zijn van invoering van deze bevoegdheid. De vereiste afweging of de ernst van de inbreuk die het middel tot gevolg heeft in verhouding staat tot het daarmee te dienen doel, ontbreekt in de toelichting. Na verkregen toegang tot het geautomatiseerde werk door middel van plaatsing van spyware, valt die toegang niet te beperken tot hetgeen slechts werd beoogd met het bevel. Dit is niet alleen disproportioneel te achten, maar leidt ook tot een bovenmatige verwerking van politiegegevens. Naar aanleiding van dit advies is de memorie van toelichting aangevuld. Te dien aanzien moet echter worden opgemerkt dat de officier van justitie gehouden is de te verrichten handelingen en de aard van de te onderzoeken gegevens te specificeren. De werking van de software zal gedifferentieerd moeten worden zodat deze binnen de

grenzen van het bevel kan worden toegepast. Als de in het bevel gestelde grenzen niet in acht zouden worden genomen, dan zal dit uit de logging kunnen blijken.
Het CBP stelt vast dat het voorstel in een aantal waarborgen voorziet maar acht daarnaast ook de volgende waarborgen wezenlijk. Een belangrijke waarborg dient te zijn gelegen in de controleerbaarheid van de toepassing gedurende het gehele proces van de aanvraag tot en met de uitvoering. Naast de «gewone» journaal en verbaliseringsverplichting is de logging van belang. Logging kan vooralsnog niet leiden tot het weergeven van alle relevante handelingen. Daarbij geldt dat voor zinvolle logging de exacte werking van de gebruikte software bekend moet zijn, waaronder begrepen kennis van de broncode. Naar aanleiding van dit advies kan worden opgemerkt dat de broncode van de gebruikte software inderdaad niet altijd bekend zal zijn, bijvoorbeeld bij het betrekken van software van een private onderneming. In een dergelijk geval is de goedkeuring door de keuringsdienst een voorwaarde voor inzet. Bij die keuring wordt onder meer bezien of alle relevante handelingen van de politie tijdens de inzet correct worden gelogd. De controle betreft de integriteit van de informatie die is verzameld, de werking van de software en daarmee ook de onderzoekshandelingen die zijn verricht.
Voorts wijst het Cbp erop dat de nieuwe bevoegdheid is geplaatst in titel IV, inzake enige bijzondere dwangmiddelen, en niet in titel IVA, inzake bijzondere bevoegdheden tot opsporing. Deze laatste titel bevat specifieke waarborgen die met de voorgestelde plaatsing in titel IV – ten minste ten dele – aan de onderhavige bevoegdheid worden onthouden. In reactie hierop kan worden opgemerkt dat inmiddels, naar aanleiding van het advies van de Afdeling advisering, is gekozen is voor opneming van de voorgestelde bevoegdheid in Titel IVA van het Wetboek van Strafvordering, dit is in het algemeen deel van de toelichting (paragraaf 2.2.) aan de orde gekomen. Daarbij is aangesloten bij de regels voor de doorzoeking ter vastlegging van gegevens, die zijn opgenomen in de zevende afdeling van titel IV. Dit betreft de regeling van het verschoningsrecht, de ontoegankelijkmaking van gegevens en de vernietiging van gegevens (artikel 126nba, eerste lid, en 126cc, vijfde en zesde lid, Sv).
Ten slotte merkt het Cbp op dat de notificatie aan de betrokkene een geringe waarborg vormt voor de verantwoording van de toepassing van de bevoegdheid. Het verdient aanbeveling te voorzien in een controle-instrument, waarmee direct en effectief toezicht wordt uitgeoefend op de wijze van uitvoering van de bevoegdheid, onder meer door middel van een verplichting tot het regelmatig beschikbaar stellen van statistieken en overzichten. Opname van een horizonbepaling is eveneens onontbeerlijk. Naar aanleiding van dit advies kan worden verwezen naar het algemeen deel van deze toelichting (paragraaf 2.6.) waar is aangegeven dat jaarlijks aan de Kamer zal worden gerapporteerd, naar het model van de jaarlijkse verstrekking van gegevens over het aftappen van telecommunicatie. Het opnemen van een horizonbepaling acht ik minder wenselijk omdat de in het wetsvoorstel opgenomen maatregelen niet zijn bedoeld van tijdelijke te aard zijn. Wel is voorzien in een evaluatiebepaling, zodat de doeltreffendheid en effecten van de wet in de praktijk getoetst zullen worden.

BoF is van oordeel dat de voorgestelde bevoegdheid grote bezwaren kent. In de eerste plaats betreft dit een onbegrensd opsporingsmiddel. Het middel is niet beperkt tot verdachten. Omdat criminelen bijna nooit vanaf hun eigen computer werken zullen vooral computers van onschuldige burgers of bedrijven worden getroffen. Verder kan het middel bij teveel misdrijven worden ingezet en kan een hele server worden binnengedrongen waardoor de politie toegang tot gegevens van andere onschuldige burgers verkrijgt, zijn na het inbreken ontelbare handelingen mogelijk en is de voorgestelde duur van de «virtuele plaatsopneming» te ruim. Ten slotte is het middel technisch onbeperkt omdat de software

eenvoudig buiten de grenzen van de bevoegdheid kan worden ingezet. In de tweede plaats is de bevoegdheid in strijd met fundamentele rechten. Het grondrecht op privacy wordt ernstig ingeperkt, omdat ook eerder uitgewisselde en/of opgeslagen data in het vizier van de opsporing komen. De noodzaak en proportionaliteit van de voorgestelde bevoegdheid worden onvoldoende onderbouwd. Het verdient aanbeveling de huidige bevoegdheden beter te benutten. In de derde plaats is de voorgestelde bevoegdheid in strijd met het volkenrecht omdat deze leidt tot schending van de soevereiniteit van andere landen en in strijd is met internationale verdragen, zoals het Cybercrime Verdrag. In de vierde plaats creëert de voorgestelde bevoegdheid onaanvaardbare risico's, omdat de politie belang heeft bij de kwetsbaarheid van de systemen. Ook is de software kwetsbaar voor aanvallen van derden en leren de ervaringen in Duitsland dat de functionaliteiten daarvan verder gaan dan toegestaan. BoF concludeert dat een hackbevoegdheid diverse veiligheidsrisico's creëert die door het wetsvoorstel onvoldoende worden erkend en ondervangen. Dit zal Nederland niet veiliger, maar juist onveiliger maken.

Naar aanleiding van het advies van BoF merk ik op dat de voorgenomen inzet van de voorgestelde bevoegdheid zodanig is ingekaderd dat het in de praktijk niet goed voorstelbaar is dat onschuldige internetgebruikers worden getroffen in plaats van de criminelen die van hun IP-adres gebruik maken. Het binnendringen in een geautomatiseerd werk wordt zeer zorgvuldig voorbereid, waarbij wordt nagegaan in welk geautomatiseerd werk moet worden binnengedrongen ten behoeve van de uitoefening van bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden. Anders dan Bof schetst is het niet zo dat criminelen vooral vanaf de computers van onschuldige burgers werken. Eerder maken zij gebruik van (draadloze) netwerken die ook voor derden toegankelijk zijn of van de vele mogelijkheden tot anonimisering (proxy, TOR, VPN). De kans dat bij het onderzoek in een geautomatiseerd werk wordt binnengedrongen in een geautomatiseerd werk dat slechts eenmalig in verband kan worden gebracht met de verdachte of het strafbare feit acht ik niet erg groot. In het geval dat gebruik is gemaakt van een IP-adres dat ook voor derden toegankelijk is, zoals het IP-adres van een internetcafé, zal reeds bij het opvragen van de identificerende gegevens bij de internetprovider blijken dat het IP-adres bij dit café in gebruik is. Aan het onderzoek in een geautomatiseerd werk gaat overigens een dermate gedegen en langdurige voorbereiding vooraf dat het door BoF geschetste scenario niet goed voorstelbaar is.

De keuze voor de categorie van misdrijven waarbij de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk kan worden toegepast, is ingegeven doordat de opsporing van dergelijke misdrijven in ernstige mate wordt gehinderd doordat het niet mogelijk is binnen te dringen in een geautomatiseerd werk. Dit is echter bepaald niet de enige voorwaarde voor het onderzoek in een geautomatiseerd werk. De juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid, zoals het vereiste van het dringende onderzoeksbelang en de voorafgaande machtiging van de rechter-commissaris, waarborgen een zorgvuldige afweging voordat de voorgestelde bevoegdheid wordt ingezet. Ook de voorafgaande toetsing door de CTC staat in de weg aan een brede toepassing, als door BoF voorzien. De voorgestelde bevoegdheid dient als een laatste redmiddel, als andere opsporingsbevoegdheden tekort schieten. Hierbij moet worden opgemerkt dat de inbreuk op de privacy, die het onderzoek van een geautomatiseerd werk met zich mee brengt, mede afhankelijk is van de te verrichten onderzoekshandeling of de inzet van de bijzondere opsporingsbevoegdheid. Het

vaststellen van de aanwezigheid van gegevens of het overnemen van gegevens impliceert dat kennis wordt genomen van gegevens die in een geautomatiseerd werk worden opgeslagen of verwerkt. Dit ligt anders bij het onderzoek in een geautomatiseerd werk met het oog op de toepassing van het aftappen van telecommunicatie, omdat er een dergelijk geval het binnendringen van het geautomatiseerde werk uitsluitend is gericht op het gebruik van dat werk ten behoeve van de inzet van een bestaande bevoegdheid. In dit geval wordt het geautomatiseerde werk uitsluitend gebruikt voor de toepassing van een bestaande bevoegdheid. De aantasting van de persoonlijke levenssfeer verschilt dan niet of nauwelijks van de situatie waarin een telefoon of computer op grond van de bestaande bevoegdheden wordt getapt.

Als een computer onderdeel vormt van een botnet, kan op grond van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk inderdaad iedere geïnfecteerde computer worden binnengedrongen. Anders dan Bof acht ik dit bij voorbaat niet onacceptabel, met dien verstande dat ieder onderzoek tevoren zorgvuldig moet worden afgewogen en voorbereid en het bepaald niet waarschijnlijk is dat een individuele computer die onderdeel vormt van een botnet, wordt binnengedrongen om het botnet onschadelijk te maken. In plaats daarvan ligt het voor de hand om de opsporingshandelingen op de server te richten, door middel waarvan de verschillende computers worden aangestuurd. Daarbij krijgt de politie, anders dan Bof veronderstelt, geen toegang tot de gegevens van alle personen die gebruik maken van die server. De toegang tot de gegevens van de server is beperkt tot de gegevens die nodig zijn voor de bestrijding van het botnet. De te verrichten handelingen, het deel van de server en de categorie van gegevens ten aanzien waarvan het bevel tot het binnendringen wordt gegeven, moeten in het bevel van de officier van justitie worden vermeld. De logging maakt het mogelijk de uitvoering te controleren zodat, als de politie buiten de kaders van het bevel zou treden, dit achteraf vastgesteld kan worden. Hieruit vloeit tevens voort dat de politie niet ontelbare onderzoekshandelingen kan uitvoeren, nadat een geautomatiseerd werk is binnengedrongen. In de eerste plaats is het binnentreden gekoppeld aan bepaalde handelingen of opsporingsbevoegdheden. De feitelijk te verrichten handelingen, zoals het aanzetten van een keylogger of GPS, moeten nodig zijn voor de uitvoering van de concrete handeling of bevoegdheid. Als het gaat om het aftappen van communicatie dan ligt, bijvoorbeeld, het gebruik van een gps niet voor de hand. Voorafgaande wordt de proportionaliteit en subsidiariteit van de feitelijk te verrichten handelingen getoetst in het licht van de concrete handeling of bevoegdheid en het daarmee te bereiken resultaat. Voor de geldigheidsduur van het bevel is rekening gehouden met de mogelijkheid dat het bevel niet direct ten uitvoer kan worden gelegd, vanwege de noodzaak van een zorgvuldige voorbereiding en de mogelijke complicaties bij het binnendringen in een geautomatiseerd werk. De tenuitvoerlegging van het bevel tot een onderzoek in een geautomatiseerd werk omvat het binnendringen in dat werk en de uitvoeringshandeling waarvoor de machtiging is afgegeven. Dit betekent dat binnen die periode de identiteit of locatie van het geautomatiseerde werk of de gebruiker wordt bepaald, de gegevens worden vastgelegd en/of ontoegankelijk gemaakt. Een bevel tot het aftappen van telecommunicatie of het direct afluisteren wordt gegeven voor een periode van ten hoogste vier weken (artikelen 126l, vijfde lid, en 126m, vijfde lid, Sv), een bevel tot observatie wordt gegeven voor een periode van ten hoogste drie maanden (artikel 126g, vierde lid, 126l, vijfde lid, en 126m, vijfde lid, Sv). De voorgestelde duur van vier weken voor het onderzoek in een geautomatiseerd werk betreft een maximale termijn, de officier van justitie dient de duur van het bevel af te stemmen op de verwachte duur van de voorgenomen inzet van de

bevoegdheid. Daarbij kan nog worden opgemerkt dat een bevel tot het vorderen van toekomstige gegevens over een gebruiker van een telecommunicatiedienst en het telecommunicatieverkeer met betrekking tot die gebruiker wordt gedaan voor een periode van ten hoogste drie maanden (artikel 126n, derde lid, Sv).

Op de door BoF naar voren gebrachte bezwaren rond nut en noodzaak van de voorgestelde bevoegdheid en het gebruik van de software is in paragraaf 2.5. nader ingegaan.

8.2. De ontoegankelijkmaking van gegevens

Het College wijst op het advies naar aanleiding van een vergelijkbaar voorstel in een eerder conceptwetsvoorstel, dat in 2010 voor advies aan het College is voorgelegd. Bij die gelegenheid heeft het College geadviseerd om geen aparte bevelsbevoegdheid in het Wetboek van Strafvordering op te nemen, omdat de gedragscode «Notice and take Down» in de praktijk goed functioneerde. Inmiddels is in deze situatie verandering gekomen omdat er veel internetproviders zijn bijgekomen die de gedragscode niet ondersteunen. Het OM wordt in toenemende mate geconfronteerd met internetproviders die niet wensen mee te werken aan het ontoegankelijk maken van strafbare gegevens. Het College is derhalve van oordeel dat het voorliggende voorstel thans in een behoefte voorziet. Wel adviseert het College de bevoegdheid te beperken tot ernstige strafbare feiten. Dit advies is overgenomen, dit is in paragraaf 3.2. aan de aan de orde gekomen.

De NOvA meent dat de voorgestelde tekst teveel ruimte laat voor bagatelzaken en doet te dien aanzien een tekstvoorstel ter verbetering. Mede naar aanleiding van dit advies is de voorgestelde tekst aangepast, dit is eveneens in paragraaf 3.2. aan de orde gekomen.

8.3. Het wederrechtelijk overnemen en helen van gegevens

Het College van procureurs-generaal constateert dat met dit voorstel wordt voorzien in een al lang bestaande behoefte uit de praktijk. Met deze artikelen wordt de rechthebbende een betere strafrechtelijk bescherming geboden tegen personen die gegevens overnemen, aan anderen beschikbaar stellen en openbaar maken zonder dat er sprake is van computervredebreuk.

De korpschef van de politie is positief over de voorgestelde strafbaarstelling van zowel het «stelen» als het «helen» van gegevens. Nu gegevens in de moderne maatschappij qua belang steeds meer gelijk komen te liggen met het fysieke komt aan gegevens een gelijkwaardige bescherming toe als goederen. Daarbij wordt benadrukt dat het kwalijke van het «stelen» van gegevens niet alleen is gelegen in de verspreiding daarvan via internet, ook de diefstal van gegevens die niet aan grote groepen openbaar worden gemaakt kunnen zeer schadelijk zijn. Bij onderzoeken naar computercriminaliteit worden nog al eens grote hoeveelheden gegevens aangetroffen waar geen redelijke verklaring voor is. Het bezit van creditcardgegevens van honderden mensen of toegangsgegevens van honderden PayPal accounts bieden thans geen aanknopingspunt voor vervolging. Dit voorstel biedt de mogelijkheid om hackers, die niet betrapt kunnen worden tijdens het hacken of overnemen van de gegevens, alsnog strafvorderlijk aan te pakken voor hun activiteiten.

De NOvA acht de voorgestelde bepalingen onduidelijk en in technische zin onder de maat. In de voorgestelde vorm kunnen deze niet worden ingevoerd. Naar aanleiding van het advies van de NOvA is de voorge-

stelde nummering van de betreffende artikelen evenals de toelichting op die artikelen aangepast. Dit komt elders in deze memorie van toelichting nader aan de orde.

BoF meent dat de gevolgen van de voorgestelde strafbaarstelling voor de vrijheid van meningsuiting moeilijk zijn te overzien en deels onwenselijk zijn. Met name de reikwijdte van het begrip niet-openbare gegevens zal in de praktijk tot problemen leiden. De uitzondering van het «algemeen belang» is te beperkt voor personen die een belangrijke functie vervullen in onze democratische samenleving, zoals journalisten en klokkenluiders. De noodzaak van het voorstel is onvoldoende onderbouwd. Naar aanleiding van dit advies is de voorgestelde bepaling over de heling van gegevens aangepast en de memorie van toelichting aangevuld.

Tijdens de consultatie is door het College van procureurs-generaal en SIDN (Stichting Internet Domeinregistratie Nederland) gewezen op de mogelijkheid van misbruik van een domeinnaam. Met de keuze voor een domeinnaam die lijkt op die van een bekende instelling kan een bezoeker van een website in de waan worden gebracht zich op de website van die instelling te bevinden. Daardoor kunnen onbevoegden de inloggegevens van de klanten of relaties van die instellingen bemachtigen. Geadviseerd wordt in het wetsvoorstel een regeling op te nemen voor het bevel tot het doorhalen van een domeinnaam. Aan dit advies is geen gevolg gegeven omdat, zoals SIDN zelf ook opmerkt, de verwijdering van de domeinnaam er niet toe zal leiden dat de website niet meer bereikbaar is. Door aan de website een andere domeinnaam te koppelen kan deze weer snel vindbaar worden gemaakt. Hier komt bij dat de verwijdering van een domeinnaam een rechterlijke beslissing veronderstelt, zeker in gevallen waarin beoogd wordt dat een dergelijke beslissing een definitief karakter heeft. Een dergelijke maatregel vereist dan ook nader onderzoek voordat aanpassing van de wetgeving kan worden overwogen.

8.4. De strafbaarheid van grooming en van het verleiden van minderjarigen tot ontucht

Het College van procureurs-generaal wijst erop dat met de strafbaarstelling van grooming het online, via bijvoorbeeld chatrooms of nieuwsrooms, benaderen en verleiden van kinderen met als uiteindelijk doel het plegen van seksueel misbruik van een kind, strafbaar is gesteld. Ten behoeve van de bestrijding van grooming maakt de politie gebruik van een zogenaamde «lokpuber». Dit is in werkelijkheid een rechercheur die zich online voordoet als minderjarige onder de zestien jaar. Als gevolg van de huidige rechtspraak is deze werkwijze echter niet meer mogelijk, omdat in de rechtspraak is geoordeeld dat voor een strafbaar handelen rechtens als voorwaarde heeft te gelden dat het beoogde slachtoffer de leeftijd van zestien jaren nog niet heeft bereikt. Met de inzet van een lokpuber wordt aan dit vereiste niet voldaan. Het College is verheugd dat voorgesteld wordt de delictsomschrijving van artikel 248e Sr aan te passen. Wel merkt het College op dat uit de voorgestelde tekst voortvloeit dat de chatpartner en de ontmoetingspartner dezelfde persoon zijn. Dit vereiste van «identiciteit» veroorzaakt in de praktijk echter de problemen. Wat het College betreft is voor de gevaarzetting voldoende dat de verdachte aantoonbaar zijn zinnen heef gezet op willekeurig welke zestienminner. Naar aanleiding van dit advies is de voorgestelde tekst voor artikel 248e Sr aangepast, zodat het vereiste van de identiciteit is losgelaten. Verder vraagt het College zich af waarom wordt voorgesteld om de strafbaarstelling van het corrumperen van minderjarigen te verruimen, nu voor dit feit in de praktijk geen lokpuber wordt ingezet. Naar aanleiding van dit advies wordt voorgesteld om de voorgestelde verruiming van artikel 248d

Sr te laten vervallen. In plaats daarvan wordt voorgesteld de reikwijdte van artikel 248a Sr te verruimen, dit wordt elders nader toegelicht.

De NVvR wijst erop dat voorgesteld wordt de strafbaarheid van grooming uit te breiden door tevens strafbaar te stellen het ten onrechte aannemen dat een persoon de leeftijd van zestien jaar nog niet heeft bereikt. Daarmee wordt de intentie gericht op de jeugdige leeftijd van het slachtoffer strafbaar gesteld en niet de werkelijke leeftijd van de betrokkene. Daarmee raakt het voorstel naar het oordeel van de NVvR aan een principieel punt, omdat het uitgangspunt steeds is geweest dat de werkelijke leeftijd bepalend is. Naar aanleiding van dit advies moet worden opgemerkt dat de doelstelling van de strafbaarstelling van grooming is om minderjarigen te beschermen tegen de pogingen van volwassenen om hen tot ontucht te bewegen. Voor het voltooide delict van grooming is een uitvoeringshandeling vereist. Het valt dan ook niet goed in te zien dat hiermee de intentie strafbaar zou worden gesteld.

De Rvdr merkt op dat bij de inzet van de lokpuber logischerwijs de grens met de niet-toegestane uitlokking in beeld komt. Het is daarbij onduidelijk welke maatregelen de wetgever voor ogen heeft om de bewijsrechtelijke- en integriteitsrisico's, die samenhangen met het zich voordoen als lokpuber, beheersbaar en controleerbaar te maken. Naar aanleiding van deze opmerkingen is de memorie van toelichting aangevuld.

De NOvA heeft een aanvullend principieel bezwaar op het gebied van de systematiek, omdat het hier in wezen gaat om het mogelijk maken van een bepaalde opsporingsmethode. Dat behoort volgens de NOvA plaats te vinden door een aanpassing van strafvordering, maar gebeurt thans door aanpassing van het materiele strafrecht. De NOvA maakt hiertegen bezwaar. Naar aanleiding van dit advies wordt opgemerkt dat de inzet van een lokpuber plaats kan vinden op grond van de algemene taakstelling van de politie, bedoeld in artikel 3 Politiewet 2012. Op dit punt vertoont de inzet van een lokpuber gelijkenis met de inzet van een lokauto of lokfiets. Daarbij is van belang dat de binnen de grenzen blijft die aan rechtmatige opsporing dienen te worden gesteld. Een belangrijke voorwaarde is dat de verdachte door hen niet wordt gebracht tot andere handelingen dan die waarop zijn opzet reeds was gericht (ECLI:NL:HR:2008:BE9817).

8.5. De online handelsfraude

Het College van procureurs-generaal is het eens met de voorgestelde strafbaarstelling van de online handelsfraude. Wel wijst het College erop dat voorwaarde voor een geïntegreerde aanpak van deze vorm van fraude is dat alle betrokken private en publieke organisaties nauw samenwerken, zodat optimaal gebruik wordt gemaakt van elkaars capaciteit, informatie, deskundigheid en bevoegdheden. Naar aanleiding van dit advies is in de toelichting duidelijk tot uitdrukking gebracht dat de bestrijding van online handelsfraude een gedeelde, samenhangende verantwoordelijkheid is van zowel private- als publieke partijen.

De Rvdr vraagt zich af of de bestaande strafbaarstelling van oplichting niet toereikend is wijst erop dat diverse rechtscolleges de afgelopen twaalf maanden uitspraken hebben gedaan die ertoe strekken dat gedragingen als in de thans voorgestelde strafbaarstelling omschreven, reeds als oplichting strafbaar zijn. Naar aanleiding van dit advies kan worden opgemerkt dat de Hoge Raad zich inmiddels, in het arrest van 9 december 2014 (ECLI:NL:HR:2014:3546), nader heeft uitgesproken over de reikwijdte van het delict oplichting bij de online handelsfraude. Deze uitspraak onderstreept de noodzaak van wetswijziging. Elders in deze toelichting

wordt nader ingegaan op de noodzaak van de voorgestelde verruiming van de strafbaarstelling en de stand van de rechtspraak.

8.6. Internetconsultatie

Het oorspronkelijke conceptwetsvoorstel, dus zonder de voorstellen rond de strafbaarheid van grooming en van verleiding van minderjarigen tot ontucht en van de online handelsfraude, is op de website «overheid.nl» geplaatst, ten behoeve van de internetconsultatie. Dit heeft geleid tot 54 reacties, afkomstig van burgers en bedrijven. De reacties hebben voornamelijk betrekking op de voorgestelde bevoegdheid tot het onderzoek in een geautomatiseerd werk. De reacties op dit voorstel zijn overwegend negatief; de respondenten plaatsen kanttekeningen bij de noodzaak en proportionaliteit van de voorgestelde bevoegdheid, de inbreuk op de persoonlijke levenssfeer van burgers, de mogelijkheid tot misbruik van deze bevoegdheid door de politie, het belang van de politie bij het onveilig houden van computersystemen, de mogelijkheid van manipulatie van gegevens door de politie, de mogelijkheid van schade ten gevolge van het onderzoek in het geautomatiseerde werk en de aansprakelijkheid voor die schade. Wat betreft opsporingshandelingen in cyberspace rond gegevens waarvan de feitelijke locatie niet is te achterhalen, wordt gewezen op de mogelijk verstrekkende diplomatieke gevolgen van dergelijk handelen. Daarnaast hebben een aantal reacties betrekking op het decryptiebevel aan de verdachte. Dit onderdeel is inmiddels geschrapt.

De reacties van de internetconsultatie komen voor een belangrijk deel overeen met de punten die in de adviezen van de geconsulteerde instanties naar voren zijn gebracht. De reacties van de internetconsultatie zijn betrokken in de bespreking van die adviezen.

II ARTIKELSGEWIJZE TOELICHTING

Artikel I, onderdeel A

Zoals in hoofdstuk 3 van het algemeen deel van de toelichting is toegelicht, wordt de bevoegdheid om te bevelen dat gegevens ontoegankelijk worden gemaakt, als zelfstandige bevoegdheid naar het Wetboek van Strafvordering overgeheveld (artikel II, onderdeel D). De vervolgingsuitsluitingsgrond van artikel 54a Sr wordt in aangepaste vorm – in het thans toegelichte onderdeel – gehandhaafd.

Het begrip «tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn» is in artikel 54a Sr gehandhaafd. Zoals blijkt uit de memorie van toelichting bij het wetsvoorstel dat ten grondslag lag aan de wet waarbij artikel 54a Sr ter implementatie van de Richtlijn inzake elektronische handel in het Wetboek van Strafrecht werd opgenomen, worden door dit begrip de in afdeling 4 van die richtlijn bedoelde diensten van de informatiemaatschappij gedekt (Kamerstukken II 2001/02, 28 197, nr. 3, blz. 62).

In hun adviezen hebben KPN en Nederland ICT aandacht gevraagd voor de verhouding tussen de regeling van de voorgestelde artikelen 54a Sr en 125p Sv enerzijds en het in artikel 7.4a Tw neergelegde beginsel van netneutraliteit anderzijds. Op grond van de laatstgenoemde bepaling is het de aanbieders van openbare elektronische communicatienetwerken waarover internettoegangsdiensten worden geleverd en aanbieders van internettoegangsdiensten niet toegestaan diensten of toepassingen op het internet te belemmeren of te vertragen. Er zijn echter enkele uitzonde-

ringen op dit verbod, waaronder belemmering of vertraging ter uitvoering van een wettelijk voorschrift of rechterlijk bevel (artikel 7a, eerste lid, onderdeel d, Tw). De opvolging van een bevel als bedoeld in het voorgestelde artikel 125p van het Wetboek van Strafvordering, dat wordt gegeven op basis van artikel 54a Sr, geldt als de uitvoering van een wettelijk voorschrift of rechterlijk bevel als bedoeld in artikel 7.4a Tw. De ontoegankelijkmaking van gegevens op bevel van de officier van justitie vormt dan ook geen belemmering van de netneutraliteit.

Artikel I, onderdeel B

Dit onderdeel betreft een verruiming van het begrip geautomatiseerd werk in artikel 80sexies. Met de Wet computercriminaliteit is een omschrijving van het begrip geautomatiseerd werk in het Wetboek van Strafrecht opgenomen. Hieronder werd verstaan elke inrichting die met technische middelen geschikt is gemaakt voor de opslag en verwerking van gegevens. Hieronder vielen computers, netwerken van aan elkaar verbonden computers en geautomatiseerde inrichtingen voor telecommunicatie. Met de Wet computercriminaliteit II is het vereiste van de overdracht toegevoegd aan de begripsomschrijving. De termen «verwerken» en «overdragen» overlappen elkaar ten dele. De term «overdragen» heeft betrekking op het transport van gegevens naar een ander geautomatiseerd werk, de term «verwerken» heeft ook betrekking op bewerkingen van gegevens binnen een geautomatiseerd werk. Volgens de memorie van toelichting is de overdrachtsfunctie een wezenskenmerk van een geautomatiseerd werk. Opslag, verwerking en overdracht van gegevens zijn cumulatieve voorwaarden (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 44). Met dit begrip worden op zichzelf staande computers aangeduid, maar ook netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie. Van belang is dat de inrichting zowel gegevens kan opslaan als deze verwerken en overdragen (Kamerstukken II 2004/05, 26 671, nr. 10, blz. 31). Een inrichting die enkel als bestemming heeft om gegevens over te dragen, zoals bijvoorbeeld een eenvoudig telefoontoestel, valt buiten de begripsomschrijving. Hierbij kan nog worden opgemerkt dat in de wetsgeschiedenis op verschillende plaatsen wordt uitgegaan van een alternatieve opsomming van de verschillende handelingen (Kamerstukken II 1989/90, 21 551, nr. 3, blz. 6, 1998/99, 26 671, nr. 3, blz. 28, 2004/05, en 26 671, nr. 10, blz. 5).

Inmiddels heeft de Hoge Raad bepaald dat uit de wetsgeschiedenis volgt dat het begrip geautomatiseerd werk niet is beperkt tot apparaten die zelfstandig voldoen aan de cumulatie van functies, te weten opslag, verwerking en overdracht van gegevens (HR 26 maart 2013, LJN BY9718). Naar het oordeel van het hoogste rechtscollege heeft de wetgever ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen onder het begrip «geautomatiseerd werk» willen brengen.

Niettemin bestaat er aanleiding tot aanpassing van het begrip «geautomatiseerd» werk vanwege de technologische ontwikkelingen, die ertoe leiden dat apparaten zelfstandig op basis van een programma automatisch gegevens verwerken, zonder dat deze onderdeel vormen van een netwerk. In het conceptwetsvoorstel dat in consultatie is gegeven was voorgesteld de definitie van geautomatiseerd werk over te nemen van artikel 2, onderdeel a, van de Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad (Pb EU L 218/8). Deze definitie omvatte niet enkel apparaten maar tevens de gegevens die met dat apparaat werden verwerkt met het oog op de werking, het gebruik, de beveiliging en het onderhoud daarvan. De Afdeling advisering heeft geadviseerd af te zien van het gebruik van het

begrip «computergegevens» in de definitie van geautomatiseerd werk. Aan dit advies is gevolg gegeven. Met de voorgestelde definitie van het begrip «geautomatiseerd» werk wordt aangesloten bij de terminologie van het Cybercrime Verdrag (artikel 1, onderdeel a). In de voorgestelde begripsomschrijving vormt het op basis van een programma automatisch verwerken van computergegevens een essentieel vereiste. Deze definitie omvat computers, servers, modems, routers, smartphones en tablets. In het advies van Bof wordt erop gewezen dat in het conceptwetsvoorstel voorgestelde de begripsomschrijving van het conceptwetsvoorstel dat in consultatie is gegeven ook technische apparaten omvat die in verbinding staan met een netwerk, zoals de SCADA-systemen die worden gebruikt bij industriële productiesystemen, navigatiesystemen, televisies, een digitaal fototoestel met Wifi-compatibiliteit of een pacemaker. Deze apparaten vallen ook onder de thans voorgestelde begripsomschrijving. Dit is echter niet zozeer een gevolg van de wens tot verruiming van de omschrijving van het geautomatiseerd werk als wel van de ontwikkeling van de techniek, die ertoe leidt dat steeds meer apparaten beschikken over functies die voorheen waren voorbehouden aan de computer. In die gevallen waarin dergelijke apparaten worden gebruikt voor de verwerking van gegevens met betrekking tot ernstige strafbare feiten, kan de toepassing van de bevoegdheden van de zevende afdeling van het Wetboek van Strafvordering (voorgesteld wordt dat die komt te luiden: «Doorzoeking ter vastlegging van gegevens en onderzoek in een geautomatiseerd werk») noodzakelijk zijn. Het ligt niet voor de hand dat een pacemaker of een televisie in beslag wordt genomen omdat daarop gegevens zijn opgeslagen of verwerkt die kunnen dienen om de waarheid aan de dag te brengen, bij voorbaat is dit echter evenmin uitgesloten. Dit is sterk afhankelijk van de ontwikkeling van zowel de techniek als de modus operandi van de misdaad.

Artikel I, onderdeel C

Artikel 138c

Voorgesteld wordt te voorzien in een zelfstandige strafbaarstelling van het wederrechtelijk overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, zonder dat er – zoals bij computervredebreuk – sprake behoeft te zijn van het binnendringen van het desbetreffende geautomatiseerde werk door degene die de gegevens (vervolgens) wederrechtelijk overneemt. Voor de toelichting kan worden verwezen naar paragraaf 4.2. van het algemeen deel van de toelichting, waarin uitvoering is ingegaan op de achtergronden van deze wijziging. Met de voorgestelde strafbedreiging van gevangenisstraf van ten hoogste een jaar wordt aangesloten bij de strafbedreiging voor opzetten en wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk (artikel 139c Sr). De NVvR is van mening dat de voorgestelde strafbedreiging te laag is vanwege de strafbepaling van artikel 310 Sr (gevangenisstraf van ten hoogste vier jaren) en de maatschappelijke impact van de handelingen, zoals bedrijfsspionage. Te dien aanzien kan worden opgemerkt dat de schending van een bedrijfsgeheim (artikel 273 Sr) strafbaar is gesteld met een gevangenisstraf van ten hoogste zes maanden. Daarbij kan worden aangetekend dat in geval de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, volgens de in paragraaf 4.2. van het algemeen deel van de toelichting vermeldde uitspraken van enkele feitenrechters kan worden aangenomen dat van diefstal van een goed sprake is.

Het moet gaan om het overnemen van gegevens die «niet-openbaar» zijn. Met «niet-openbaar» is bedoeld dat de gegevens die worden overgenomen niet al openbaar moeten zijn gemaakt, waarbij in het bijzonder is gedacht aan het internet. Voorkomen moet worden dat het wederrechtelijk overnemen – door downloaden – van op het internet openbaar gemaakte gegevens in het algemeen strafbaar wordt gesteld. Van strafbaarheid van downloaden is alleen sprake als bijzondere bepalingen daarin voorzien. Zo is het downloaden van afbeeldingen van kinderporno strafbaar op grond van artikel 240b Sr. En het downloaden van auteursrechtelijk beschermde gegevens is strafbaar op grond van de Auteurswet.

Met betrekking tot de voorgestelde strafbaarstelling van het wederrechtelijk overnemen van gegevens is tijdens de consultatie van het eerdere conceptwetsvoorstel versterking bestrijding computercriminaliteit bepleit deze te beperken tot gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat openbaarmaking of verspreiding de persoonlijke levenssfeer kan schenden. Dit zou echter te beperkend zijn. Hoewel bescherming van de persoonlijke levenssfeer een belangrijke doelstelling van het wetsvoorstel is, kunnen ook gegevens worden overgenomen uit overwegingen van geldelijk gewin zonder dat schending van de persoonlijke levenssfeer daarbij aan de orde is. In het advies over het voorliggende wetsvoorstel heeft de NJCM bepleit de strafbaarstelling te betrekken op gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat openbaarmaking of verspreiding de persoonlijke levenssfeer kan schenden en gegevens die worden overgenomen uit overwegingen van geldelijk gewin. Het vereiste van de overwegingen van geldelijk gewin vormt echter reeds onderdeel van de voorgestelde strafbaarstelling, in de vorm van het winstbejag. De dader zal dan stellen dat hij geen geldelijk gewin beoogde en evenmin wist dat de persoonlijke levenssfeer zou kunnen worden geschonden. Door het subjectieve element te betrekken op de reikwijdte van de bepaling, wordt deze reikwijdte te veel beperkt.

Artikel I, onderdeel D

Artikel 139f

Nu voor de heling van gegevens een strafbedreiging van een jaar gevangenisstraf wordt voorgesteld, ligt het in de rede om die strafbedreiging ook te laten gelden voor het wederrechtelijk opnemen van beeldmateriaal in een woning. Daarom wordt voorgesteld de maximale gevangenisstraf, die is voorzien in artikel 139f Sr, te verhogen van zes maanden naar een jaar. Met de voorgestelde verhoging wordt de maximale gevangenisstraf gelijk aan die van het wederrechtelijk aftappen of opnemen van gegevens die via telecommunicatie of een geautomatiseerd werk worden verwerkt of overgedragen (artikel 139c Sr). In vergelijking met de strafbepalingen betreffende heling van een goed is het verhoogde strafmaximum voor het bezitten of bekendmaken van de hierboven genoemde gegevens in evenwicht; op schuldheling is een maximale gevangenisstraf gesteld van een jaar (artikel 417bis Sr) en op opzetheling vier jaar (artikel 416 Sr). Zoals bij de toelichting op het voorgestelde artikel 139g wordt opgemerkt, ligt het in de lijn van de jurisprudentie inzake de diefstal van gegevens dat de helingbepalingen van toepassing kunnen zijn op gegevens waarover de rechthebbende de beschikkingsmacht heeft verloren. In geval van opzettelijk handelen is in dat geval bij deze gegevens het strafmaximum van vier jaar beschikbaar.

Omdat in het voorgestelde artikel 139g (nieuw) Sr onverschillig is uit welk misdrijf de gegevens zijn verkregen, kunnen de huidige artikelen 139f, onderdeel 2°, en 139g vervallen. Deze artikelen betreffen namelijk het

beschikken over en bekend maken van een specifieke categorie van gegevens (afbeeldingen) die met gebruikmaking van een technisch hulpmiddel waarvan de aanwezigheid niet op duidelijke wijze is kenbaar gemaakt, zijn vervaardigd.

De NVvR is van mening dat de strafbaarstelling van het heimelijk vervaardigen van afbeeldingen te ruim is geformuleerd. De NOvA stelt vast dat de voorgestelde bepaling in het geheel niet wordt toegelicht. Zonder nadere toelichting zijn nut, noodzaak en proportionaliteit van de voorgestelde bepaling niet inzichtelijk. Naar aanleiding van deze adviezen merk ik allereerst op dat de voorgestelde wijziging van dit artikel uitsluitend betrekking heeft op de verhoging van de strafbedreiging en de schrapping van onderdeel 2°. De inhoud van deze bepaling, die met de wet uitbreiding heimelijk cameratoezicht van 8 mei 2003 (Stb. 2003, 198) als artikel 139f in het Wetboek van Strafrecht is opgenomen, wordt overigens niet gewijzigd. Op grond van de ervaring met deze bepaling in de praktijk bestaat daartoe vooralsnog geen aanleiding. Verder merk ik op dat in het conceptwetsvoorstel, dat in consultatie is gegeven, ten onrechte werd voorgesteld om het thans geldende artikel 139f Sr te vernummeren tot artikel 139e Sr. Naar aanleiding van de inbreng van de bovengenoemde adviesorganen is het wetsvoorstel aangepast, doordat voorgesteld wordt het thans geldende artikel 139f te wijzigen en artikel 139g (nieuw) in de plaats te doen komen van het thans geldende artikel 139g. Tevens is de toelichting aangepast.

Artikel I, onderdeel E

Artikel 139g Sr

Voorgesteld wordt een nieuwe bepaling op te nemen die het helen van gegevens strafbaar stelt. Dit is in het algemeen deel reeds aan de orde gekomen.

Eerste lid

In dit lid is de strafbaarstelling opgenomen van het voorhanden hebben en bekend maken van door misdrijf verkregen gegevens. Deze strafbaarstelling bouwt voort op het huidige artikel 139e Sr. In lijn met opmerkingen die prof. dr. E.J. Koops, verbonden aan het eerdergenoemde TILT – Tilburg Institute for Law, Technology, and Society – van de Universiteit van Tilburg, heeft gemaakt (zie «Tijd voor Computercriminaliteit III», *NJB* 2010, blz. 2465–2466) is de delictsomschrijving vereenvoudigd door daarin te spreken over gegevens die «door misdrijf» zijn verkregen en niet naar afzonderlijke soorten gegevens en soorten misdrijven te verwijzen, zoals thans in het geldende artikel 139e Sr. Een vergelijkbare constructie is opgenomen in de artikelen 273, 416 en 417bis Sr. Hoewel het onverschillig is door welk misdrijf de gegevens zijn verkregen, moet met name worden gedacht aan de misdrijven die thans zijn opgenomen in de artikelen 138ab, 139a, 139b, 139c en 139e Sr. In bepaalde gevallen kunnen gegevens ook zijn verkregen door andere misdrijven. Gegevens die zijn ontleend aan een eerder gestolen laptop zijn evenzeer door misdrijf verkregen (te weten: het misdrijf dat in artikel 310 Sr is omschreven).

In het voorgestelde artikel is ook wat betreft de delictsgedragingen meer aansluiting gezocht bij de artikelen 273, 416 en 417bis Sr. De delictsgedragingen zijn: het verwerven, voorhanden hebben, ter beschikking van een ander stellen, aan een ander bekend maken, en uit winstbejag voorhanden hebben of gebruiken. Onder «aan een ander bekend maken» valt ook het aan meerdere personen bekend maken alsook het openbaar maken van de gegevens op bijvoorbeeld het internet.

Het moet gaan om gegevens waarvan de dader «wist of redelijkerwijs had moeten vermoeden» dat deze door misdrijf zijn verkregen. Mede naar aanleiding van de hierboven genoemde opmerkingen van hoogleraar Koops is van de artikelen 416 en 417bis Sr overgenomen dat deze wetenschap of het redelijkerwijs moeten vermoeden dient te bestaan «ten tijde van de verwerving of het voorhanden krijgen» van de gegevens. Het ter beschikking van een ander stellen, aan een ander bekend maken of uit winstbejag voorhanden hebben of gebruiken van de gegevens is – in lijn met de artikelen 139e, 273, 416 en 417bis Sr – strafbaar, ongeacht op welk moment de dader weet of redelijkerwijs moet vermoeden dat deze gegevens door misdrijf zijn verkregen (zie onderdeel b). Zo maakt het voor de strafbaarheid van het via het internet openbaar maken van de gegevens niet uit dat degene die deze gegevens voorhanden heeft pas later tot de ontdekking is gekomen dat deze door misdrijf zijn verkregen.

Door opneming van het begrip «niet-openbare» gegevens is het voorhanden hebben van gegevens die reeds openbaar gemaakt zijn, niet op grond van deze bepaling strafbaar. Degene die door misdrijf verkregen gegevens via het internet openbaar maakt is op grond van deze bepaling strafbaar, maar niet de persoon die via het internet openbaar gemaakte gegevens download. Zonder deze beperking zou het van het internet downloaden van gegevens die eerder door misdrijf zijn verkregen en door een ander zijn geupload in het algemeen strafbaar worden. Voor bepaalde gegevens, zoals afbeeldingen van kinderporno en auteursrechtelijk beschermd materiaal dat niet onder het thuiskopiestelsel valt, is downloaden overigens uit anderen hoofde strafbaar. In dat geval is onverschillig of deze gegevens al op het internet openbaar zijn gemaakt.

Voorts is het bestanddeel «voorwerp» niet overgenomen uit het geldende artikel 139e Sr. Door niet te verwijzen naar de gegevensdrager waarop de gegevens zijn vastgelegd, wordt zeker gesteld dat niet alleen het voorhanden hebben van gegevens die op een usb-stick of een portable harde schijf staan strafbaar is, maar ook het beschikken over gegevens die op een e-mailaccount staan.

Daarnaast wordt, anders dan in het geldende artikel 139e Sr, een maximale gevangenisstraf voorgesteld van een jaar. Deze strafbedreiging geldt ook voor zover het gaat om beeldmateriaal dat door misdrijf is verkregen. Hiermee wordt de maximale gevangenisstraf gelijk aan die van het wederrechtelijk aftappen of opnemen van gegevens die via telecommunicatie of een geautomatiseerd werk worden verwerkt of overgedragen (artikel 139c Sr). In vergelijking met de strafbepalingen betreffende heling van een goed is het verhoogde strafmaximum voor het bezitten of bekendmaken van de hierboven genoemde gegevens in evenwicht; op schuldheling is een maximale gevangenisstraf gesteld van een jaar (artikel 417bis Sr) en op opzetheling vier jaar (artikel 416 Sr). Daarbij kan worden aangetekend dat, ingeval de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, op grond van de in paragraaf 5 van deze toelichting genoemde uitspraken van enkele feitenrechters kan worden aangenomen dat van diefstal van een goed sprake is; in die lijn ligt dat de helingsbepalingen van toepassing kunnen zijn op gegevens waarover de rechthebbende de beschikkingsmacht heeft verloren. Ingeval van opzettelijk handelen is in dat het geval bij deze gegevens het strafmaximum van vier jaar beschikbaar.

Ten opzichte van het geldende artikel 139e Sr blijft ongewijzigd dat het bekend maken aan een ander strafbaar is zowel in geval de dader de gegevens zelf eerder door misdrijf heeft verkregen als ingeval een ander dat heeft gedaan.

Tweede lid

Van strafbaarheid is geen sprake als betrokkene te goeder trouw heeft kunnen aannemen dat het algemeen belang bekendmaking van de gegevens vereiste. Deze uitzondering is besproken in paragraaf 4.3. van het algemeen deel van de toelichting.

In het voorgestelde artikel 139g Sr is de strafbaarstelling opgenomen van het voorhanden hebben en bekend maken van door misdrijf verkregen gegevens. Zoals hierboven reeds is opgemerkt, kan het huidige artikel 139g Sr vervallen omdat in het voorgestelde artikel 139g onverschillig is uit welk misdrijf de gegevens zijn verkregen.

Artikel I, onderdelen F en G

Artikelen 248a en 248e

Met de voorgestelde wijzigingen van deze artikelen zijn verleiding van een minderjarige tot ontucht en grooming ook strafbaar als de dader iemand die zich voordoet als een minderjarige benadert voor seksuele doeleinden.

Voor de strafbaarheid van verleiding van een minderjarige tot ontucht is in de eerste plaats vereist dat sprake is van verleiding (giften of beloften van geld of goed), misbruik van uit feitelijke verhoudingen voorvloeiend overwicht of misleiding. In de tweede plaats dient de dader de minderjarige (of degene die zich als zodanig voordoet) door middel van voornoemde middelen opzettelijk te bewegen tot het plegen of dulden van ontuchtige handelingen. In de derde plaats dient het opzet gericht te zijn op het plegen van ontuchtige handelingen of het dulden van zodanige handelingen van de verdachte door de minderjarige of degene die zich als zodanig voordoet. Uit de bewijsmiddelen zal moeten blijken dat er tussen verdachte en de (zich als zodanig voordoende) minderjarige enigerlei voor het plegen van ontucht relevante interactie is geweest. Hierbij kan gedacht worden aan het zich naakt voor de webcam tonen of het verrichten van ontuchtige handelingen voor de camera.

Voor de strafbaarheid van grooming zijn de volgende elementen essentieel. In de eerste plaats dient de dader door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst in contact te komen met een kind beneden de leeftijd van zestien jaren of iemand die zich als zodanig voordoet. In de tweede plaats is bij de dader het oogmerk vereist om ontuchtige handelingen te plegen met een persoon die de leeftijd van zestien jaren nog niet bereikt heeft of een afbeelding van een seksuele gedraging te vervaardigen waarbij een persoon die de leeftijd van zestien jaren nog niet bereikt heeft is betrokken. In de derde plaats dient de dader enige handeling te ondernemen gericht op het verwezenlijken van een ontmoeting met een vorenbedoelde persoon.

Of sprake is van een oogmerk om ontuchtige handelingen te plegen met een persoon die de leeftijd van zestien jaren nog niet heeft bereikt of een afbeelding te vervaardigen van een seksuele gedraging waarbij een persoon die de leeftijd van zestien jaren nog niet heeft bereikt is betrokken, kan uit feiten en omstandigheden worden afgeleid. Zo kan het – zich als zodanig voordoende – kind onder de zestien aan de verdachte kenbaar hebben gemaakt dat hij of zij de leeftijd van zestien jaren nog niet heeft bereikt, maar dit kan ook uit de uitlatingen van de verdachte blijken, bijvoorbeeld omdat hij door middel van handelingen of uitlatingen tot uitdrukking heeft gebracht op zoek te zijn naar een kind onder de zestien

jaar. Voor het bewijs van het oogmerk is dus voldoende dat de verdachte aantoonbaar zijn zinnen heeft gezet op willekeurig welke zestienminner.

Voor het voltooide delict van de grooming is een voorstel voor een ontmoeting, met het oogmerk van seksueel misbruik vereist, alsmede een handeling gericht op het verwezenlijken van die ontmoeting. Voor het voltooide delict van grooming is niet vereist dat de ontmoeting heeft plaatsgevonden. De Hoge Raad heeft in een uitspraak van 11 november 2014 (ECLI:NL:HR:2014:3140) geoordeeld dat ook zonder concrete afspraak voor een ontmoeting sprake kan zijn van grooming. Volgens de Hoge Raad kan veroordeling wegens grooming plaatsvinden als er bij herhaling wordt aangedrongen op een ontmoeting op concrete tijdstippen en plaatsen, bij herhaling wordt aangedrongen op het snel plaatsvinden van die ontmoeting waarbij het slachtoffer onder druk wordt gezet en een telefoonnummer aan het slachtoffer wordt gegeven om een afspraak te maken.

In de jurisprudentie wordt poging tot grooming steeds vaker niet strafbaar geacht[5]. Artikel 24 van het eerdergenoemde Verdrag van Lanzarote verplicht tot het strafbaar stellen van poging tot (onder andere) grooming, tenzij een partij zich het recht heeft voorbehouden de poging niet toe te passen (artikel 24, derde lid). Nederland heeft zich in het kader van het ratificatietraject van het verdrag (Kamerstukken II 2008/09, 31 808 (R1872), nr. 3; artikelsgewijze toelichting bij artikel 24) op het standpunt gesteld, onder verwijzing naar artikel 45 Sr, dat poging tot het plegen van misdrijven in Nederland strafbaar is. Er is geen gebruik gemaakt van de uitzonderingsmogelijkheid die het verdrag biedt. Bij wet is de strafbaarheid van de poging tot grooming derhalve niet uitgesloten. Er kan sprake zijn van een strafbare poging tot grooming als de communicatie heeft geleid tot het voorstel voor een ontmoeting maar geen handeling is ondernomen gericht op het verwezenlijken van die ontmoeting. Dit kan bijvoorbeeld het geval zijn bij een voorstel voor een ontmoeting met het oogmerk ontuchtige handelingen te verrichten, waarbij de minderjarige of degene die zich voordoet als minderjarige daar niet op in gaat of waarbij een ouder bijtijds heeft ingegrepen. Het voorstel voor de ontmoeting met het oogmerk ontuchtige handelingen te plegen of een afbeelding van een seksuele gedraging te vervaardigen waarbij het slachtoffer is betrokken, vormt dan het begin van uitvoering van het delict grooming.

Artikel I, onderdeel H

Artikel 273d

Dit betreft een wijziging van meer technische aard. In het voorgestelde artikel 138e Sv, dat inhoudelijk gelijk is aan het huidige artikel 126l Sv, is een omschrijving opgenomen van de begrippen «openbaar communicatienetwerk» of «openbare communicatiedienst». Voor deze begripsomschrijvingen is nauw aangesloten bij het Cybercrime Verdrag. Het Cybercrime Verdrag verplicht ertoe de bevoegdheid te creëren om communicatie op te nemen die plaatsvindt met gebruikmaking van de diensten van een serviceprovider in de zin van het verdrag, dat wil zeggen degene die aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst (Kamerstukken II 2004/05, 26 671, nr. 7, blz. 41). De begripsomschrijving van het Cybercrime Verdrag wijkt af van die van de Telecommunicatiewet waarin, ter implementatie van de zogenoemde ONP-richtlijnen, wordt

[5] Poging tot grooming niet strafbaar: ECLI:NL:RBAMS:2013:4000, ECLI:NL:RBOBR:2014:7494. Poging tot grooming wel strafbaar: ECLI:NL:RBOBR:2013:CA2959.

uitgegaan van het begrip elektronische communicatiedienst (Kamerstukken II 2002/03, 28 851, nr. 3, blz. 89). Dit begrip heeft betrekking op het overbrengen van signalen (artikel 1.1, onderdeel f, Tw). De afwijkende begripsomschrijving van het Cybercrime Verdrag hangt samen met het specifieke doel van dit verdrag, namelijk het doeltreffender maken van strafrechtelijke onderzoeken en procedures met betrekking tot strafbare feiten die verband houden met computersystemen en computergegevens. Het ligt in de rede om voor de strafbaarstelling van de schending van het briefgeheim rond gegevens die worden opgeslagen, verwerkt of overgedragen aan te sluiten bij het begrip communicatieaanbieder, zoals dat is omschreven in artikel 126la Sv. Hiermee wordt verduidelijkt dat de strafbaarstelling geldt voor degene die werkzaam is bij een aanbieder van een openbaar communicatienetwerk of een openbare communicatiedienst, in aansluiting op de omschrijving van deze begrippen in artikel 126la van het Wetboek van Strafvordering.

Artikel I, onderdeel I

Artikel 326d

Met het voorstel tot opneming van dit artikel wordt strafbaar gesteld het maken van een beroep of gewoonte van het door middel van een geautomatiseerd werk met gebruikmaking van een communicatiedienst verkopen van goederen of verlenen van diensten tegen betaling en met het oogmerk om die goederen of diensten niet te leveren en zichzelf of een ander te verzekeren van de betaling. Het kwalijke van deze gedraging betreft de moedwillige wanprestatie: het voornemen om niet te leveren, maar wel de betaling te incasseren.

Voor de strafbaarheid van de online handelsfraude zijn de volgende elementen van belang. In de eerste plaats het maken van een beroep of gewoonte van het te koop aanbieden van een goed of het aanbieden van een dienst. Voor een gewoonte is vereist het meermalen verrichten van gelijksoortige feiten. Onder gewoonte pleegt te worden verstaan een pluraliteit van feiten die niet slechts toevallig op elkaar volgen, maar onderling in zeker verband staan en wel (objectief) wat de aard van de feiten betreft, en (subjectief) wat de psychische gerichtheid van de dader aangaat: de neiging om telkens weer zo'n feit te begaan (Noyon-Langemeier-Remmelink, Het Wetboek van Strafrecht, artikel 250, aantekening 7 (supplement 130)). Dit kan aan de orde zijn als bij verschillende gelegenheden goederen of diensten worden aangeboden op een website. Dit kan ook aan de orde zijn als bij verschillende gelegenheden gebruik wordt gemaakt van een website om goederen of diensten aan te bieden. Niet uitgesloten is dat in het geval van een enkele website, met behulp waarvan gedurende korte tijd een groot aantal afzonderlijke transacties tot verkoop wordt aangegaan, sprake is van het meermalen verrichten van soortgelijke feiten, te weten het aanbieden van goederen of diensten zonder de intentie tot leveren. Het eenmalig te koop aanbieden van een voorwerp of aanbieden van een dienst valt hier echter niet onder. In de tweede plaats moet het gaan om het door middel van een geautomatiseerd werk met gebruikmaking van een communicatiedienst aanbieden. Dit betekent dat het aanbod van de verkoop via internet (inclusief email) tot uitdrukking wordt gebracht. De verkoop aan de deur, in een winkel, in een kantoor of telefonische colportage valt hier niet onder.

De NVvR heeft opgemerkt dat het bij internetoplichting niet zozeer gaat om het aanbieden via een geautomatiseerd werk, maar via internet. In reactie hierop merk ik op dat internetoplichting een vorm van computercriminaliteit is. Met het gebruik van het begrip «geautomatiseerd werk»,

dat gedefinieerd is in artikel 80sexies Sr, wordt aangesloten bij de gebruikelijke systematiek in het Wetboek van Strafrecht waarmee computerdelicten strafbaar worden gesteld. Niet wordt beoogd om telefonische verkoop onder de strafbaarstelling te laten vallen. Gelet hierop is de toevoeging «met gebruikmaking van een communicatiedienst», de Rvdr vroeg hiernaar in het advies, niet wenselijk. In de derde plaats dient het oogmerk bij het verkopen van goederen of diensten erop gericht te zijn niet of niet volledig te leveren en zichzelf of een ander de beschikking te verzekeren over de betaling. Ook de intentie om na betaling gedeeltelijk te leveren kan worden aangemerkt als het oogmerk om na betaling niet te leveren. In navolging van een advies van de Afdeling advisering is dit in de tekst van het voorgestelde artikel 326d Sr geëxpliciteerd.
Zoals eerder opgemerkt is essentieel het vereiste dat in de rechtspraak wel wordt aangeduid als de moedwillige wanprestatie. De aanbieder die failliet is gegaan voor de levering van de verkochte goederen of diensten, valt niet onder de voorgestelde strafbaarstelling.
Niet is vereist dat de koper daadwerkelijk heeft betaald, de adviezen van de Rvdr en de NVvR op dit punt hebben mede aanleiding gegeven tot een wijziging van de voorgestelde bepaling. De strafbaarheid treedt in als nadeel kan ontstaan. Hiervoor is niet vereist dat daadwerkelijk betaling is gevolgd. Het oogmerk van de verkoper om niet of volledig te leveren en zichzelf of een ander van de betaling te verzekeren staat centraal. Zoveel mogelijk is aangesloten is bij de formulering van (het spiegelbeeldige) artikel 326a Sr (flessentrekkerij) waarin het oogmerk van de koper om niet of niet volledig te betalen en het voor zichzelf of een ander zekerstellen van een goed centraal staat. Anders dan bij de flessentrekkerij omvat de strafbaarstelling ook het aanbieden van goederen of diensten. De strafbaarstelling omvat het aanbieden van boeken, reizen, tickets voor concerten of treinkaartjes en cadeau- of verrassingspakketten.

In de gevallen waar de verkoper om betaling heeft verzocht maar de koper (nog) niet heeft betaald kan sprake zijn van een strafbare poging tot online handelsfraude, de Rvdr vroeg hiernaar. De voorgestelde strafbaarstelling laat het opportuniteitsbeginsel onverlet. Het OM kan afzien van strafvervolging indien het daartoe termen aanwezig acht.

De Rvdr stelt voor om voorlopige hechtenis mogelijk te maken wanneer ernstig gevreesd moet worden voor voortzetting van online handelsfraude, terwijl er nog geen vijf jaren verstreken zijn sinds een onherroepelijke veroordeling. Dit voorstel is overgenomen.

Artikel II, onderdeel A

Artikel 67

Dit betreft een aanvulling van dit artikel. Artikel 67 Sv bevat de gevallen waarin een bevel tot voorlopige hechtenis kan worden gegeven, te weten een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaar of meer is gesteld of een aantal specifiek opgesomde misdrijven. Dwangmiddelen als aanhouden buiten heterdaad, inverzekeringstelling en voorlopige hechtenis kunnen nodig zijn bij de bestrijding van de ernstiger verschijningsvormen van het in het voorgestelde artikel 139g Sr omschreven misdrijf van de «heling» van gegevens. Vanwege het op dit misdrijf gestelde strafmaximum wordt voorgesteld dit misdrijf in artikel 67, eerste lid, onderdeel b, Sv afzonderlijk te noemen als een misdrijf bij verdenking waarvan een bevel tot voorlopige hechtenis kan worden gegeven.

Artikel II, onderdeel B

Artikel 67a

De toevoeging van het misdrijf online handelsfraude (nieuw artikel 326d Sr) aan artikel 67a, tweede lid, onder 3°, Sv, maakt het mogelijk om voorlopige hechtenis te bevelen bij ernstige vrees voor recidive.

Artikel II, onderdeel C

Artikel 125m

De voorgestelde wijziging van artikel 125m Sv betreft de opneming van een verplichting tot geheimhouding, conform de regeling van artikel 126bb, vijfde lid, Sv. In zijn advies heeft het College van procureurs-generaal erop gewezen dat degene, tot wie het bevel is gericht tot het verschaffen van toegang tot de aanwezige geautomatiseerde werken of delen daarvan, op grond van artikel 125k, eerste lid, Sv, niet is gehouden tot geheimhouding jegens de verdachte. Dit maakt dat er een afbreukrisico bestaat omdat verdachten voortijdig bekend raken met tegen hen verrichte opsporingshandelingen. In de praktijk blijkt dat een aantal webhostingbedrijven hun klanten actief informeren omtrent een doorzoeking van een geautomatiseerd werk. Het College adviseert derhalve om artikel 125i Sv op te nemen in artikel 126bb, vijfde lid, Sv, dat een geheimhoudingsverplichting bevat voor degene jegens wie een vordering is gericht tot het verstrekken van gegevens.

Met de invoering van artikel 126bb, vijfde lid, Sv is destijds uitvoering gegeven aan artikel 4 van het protocol bij het EU-rechtshulpverdrag (Kamerstukken II 2001/02, 28 353, nr. 3, blz. 15). Het is namelijk in het belang van de opsporing dat de cliënt niet wordt geïnformeerd over de toepassing van de bevoegdheden tot het vorderen van gegevens. Dit belang is eveneens aan de orde bij het bevel aan een derde tot het verschaffen van toegang tot een geautomatiseerd werk, op grond van artikel 125k Sv. Dit artikel vormt echter onderdeel van Titel IV van het Wetboek van Strafvordering, dat een zelfstandige bepaling bevat over de kennisgeving aan betrokkene (artikel 125m Sv). Vanuit oogpunt van de wetssystematiek ligt opneming van een verwijzing naar artikel 125k Sv in artikel 126bb Sv, zoals geadviseerd door het College, dan ook minder voor de hand. Naar aanleiding van het advies van het College wordt daarom voorgesteld aan artikel 125m Sv een nieuw vijfde lid toe te voegen, dat voorziet in een verplichting tot geheimhouding voor degene – anders dan de verdachte – tot wie het bevel is gericht toegang te verschaffen tot een geautomatiseerd werk.

Artikel II, onderdeel D

Artikel 125p

Eerste lid

In dit lid is vastgelegd dat de officier van justitie, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv aan de aanbieder van een communicatiedienst het bevel kan richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven ontoegankelijk te maken, teneinde het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen. Doorgaans kan de politie door middel van feitelijk optreden strafbare feiten beëindigen of nieuwe strafbare feiten voorkomen, door bijvoorbeeld voorwerpen in beslag te nemen of

personen aan te houden. Bij de beëindiging van strafbare feiten met behulp van een geautomatiseerd werk is echter in veel gevallen de medewerking van een derde vereist die de beschikkingsmacht heeft over de gegevens die op het internet zijn geplaatst of in een geautomatiseerd werk zijn opgeslagen. Dat is degene die een website op het internet geplaatst heeft en die in staat moet worden geacht die website aan te passen of de inhoud daarvan van het internet te verwijderen.

Indien gegevens eenmaal op het internet zijn geplaatst, is het buitengewoon moeilijk deze gegevens volledig van het internet te verwijderen als zij inmiddels zijn verspreid. Daarom is het van belang dat, in de gevallen waarin daartoe aanleiding bestaat, snel kan worden ingegrepen om de schadelijke effecten zoveel mogelijk te beperken. Dit komt ook tot uitdrukking in de Richtlijn inzake elektronische handel, die ervan uitgaat dat de aanbieder van een hosting-dienst alleen dan niet aansprakelijk is indien hij, zodra hij daadwerkelijk kennis heeft of krijgt, «prompt» handelt om de informatie te verwijderen of de gegevens ontoegankelijk te maken. In lijn daarmee wordt in het eerste lid bepaald dat de aanbieder gehouden is «terstond» alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens ontoegankelijk te maken. Daarmee wordt tot uitdrukking gebracht dat van de aanbieder van een communicatiedienst wordt verwacht dat deze zo snel mogelijk alle maatregelen neemt die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken, ter beëindiging van een strafbaar feit of ter voorkoming van strafbare feiten. Tijdens de consultatie heeft KPN geadviseerd het woord «terstond» te schappen omdat dit een verruiming van de bevoegdheid is. Aan dit advies is geen gevolg gegeven, met de invoeging van het woord «terstond» is niet beoogd de bevoegdheid te verruimen maar deze in overeenstemming te brengen met de tekst van de Richtlijn inzake elektronische handel.

Het bevel zal, als direct optreden jegens degene die de beschikking heeft over het geautomatiseerde werk met behulp waarvan het strafbare feit wordt begaan niet mogelijk blijkt, aan de aanbieder van een communicatiedienst worden gericht.

De algemene vereisten van proportionaliteit en subsidiariteit stellen grenzen aan de bevoegdheidsuitoefening. Daaruit vloeit voort dat het bevel wordt gericht tot degene die daarvoor het meest in aanmerking komt. Als de gewraakte gegevens in Nederland worden gehost zal dit in de eerste plaats de hosting provider zijn. Als de gegevens in het buitenland worden gehost en ontoegankelijkmaking noodzakelijk is, kan het bevel tot de access provider worden gericht. De kosten en inspanningen aan de kant van de aanbieder, die voortvloeien uit de ontoegankelijkmaking vormen een factor die bij het bevel mede betrokken moet worden: de aanbieder kan op grond van het eerste lid uitsluitend worden bevolen dat hij alle redelijkerwijs van hem te vergen maatregelen treft om gegevens ontoegankelijk te maken.

In zijn advies heeft de Rvdr gevraagd hoe om te gaan met de situatie waarin de aanbieder van de communicatiedienst niet in Nederland is gevestigd en waarin het strafbare feit niet in Nederland wordt begaan. De Telecommunicatiewet is van toepassing op degene die een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst aanbiedt dan wel bijbehorende faciliteiten aanlegt of aanbiedt (artikel 2.1 Tw). Als de aanbieder van de inhoud niet kan worden aangesproken, bijvoorbeeld omdat de gegevens in het buitenland worden gehost, dan zal het OM proberen tot afspraken te komen met de bevoegde buitenlandse autoriteiten met het oog op de ontoegankelijkmaking van de gegevens.

Tweede lid

Het bevel moet voldoen aan een aantal eisen die in dit lid zijn opgenomen. Allereerst geldt het vereiste dat het bevel schriftelijk is. In zijn advies heeft de NVvR zich afgevraagd of de voorgestelde mogelijkheid in dit artikel voldoende slagvaardig is. Doordat digitale informatie snel kan worden verspreid kan het afwachten van een schriftelijke machtiging van de rechter-commissaris teveel tijd kosten. De NVvR is derhalve van mening dat het mondeling geven van een bevel en machtiging, of het mondeling geven van een voorlopig bevel mogelijk moet zijn en verzoekt deze mogelijkheid op te nemen in de wet. Aan dit advies is geen gevolg gegeven omdat de betekenis van een mondeling bevel en een mondelinge machtiging in de praktijk vooralsnog van onvoldoende belang wordt geacht om een dergelijke mogelijkheid in de wet op te nemen. Het bevel tot ontoegankelijkmaking van gegevens betreft een verstrekkende bevoegdheid waarbij de vrijheid van meningsuiting in het geding kan zijn. Daarom wordt voorzien in de nodige procedurele waarborgen, onder meer het vereiste van een machtiging van de rechter-commissaris, waarbij degene tot wie het bevel is gericht in de gelegenheid wordt gesteld te worden gehoord. De aanbieder tot wie het bevel is gericht is bevoegd zich bij het horen door een raadsman te doen bijstaan. De mogelijkheid van een mondeling bevel lijkt niet goed te verenigen met deze procedurele eisen en aldus met een zorgvuldige procedure ter voorbereiding van het bevel.

Het bevel zal duidelijk moeten maken welk strafbaar feit het betreft (onderdeel a). Naar aanleiding van het advies van het College van procureurs-generaal is het vereiste van de naam, of anders een zo nauwkeurige mogelijke aanduiding van de verdachte, geschrapt. Zoals door het College wordt opgemerkt, heeft dit vereiste geen relevantie voor de noodzaak van een bevel tot verwijdering van de gegevens. De ratio achter de vorderingsbevoegdheid is dat de samenleving wordt beschermd doordat gegevens ontoegankelijk worden gemaakt met het oog op de beëindiging van een ernstig strafbaar feit of de voorkoming van nieuwe strafbare feiten. Het bevel kan dan ook worden gegeven in gevallen waarin geen verdachte bekend is.
Het bevel zal ook duidelijkheid moeten verschaffen over de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens nodig is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen (onderdeel b). Om – in geval van uitingsdelicten – te voorkomen dat de vrijheid van meningsuiting verder dan noodzakelijk wordt ingeperkt, zal de officier van justitie nauwkeurig bepalen welke gegevens een strafbaar feit behelzen en – dus – ontoegankelijk moeten worden gemaakt door degene tot wie het bevel is gericht (onderdeel c). Dit kan gebeuren aan de hand van IP-adressen. De officier van justitie zal hierbij rekening houden met de technische mogelijkheden om onderdelen van pagina's of websites te kunnen verwijderen. Hiermee kan voorkomen worden dat tot de aanbieder een bevel wordt gericht dat technisch niet kan worden uitgevoerd.

Derde lid

Met dit lid wordt artikel 125o, tweede en derde lid, Sv van overeenkomstige toepassing verklaard. Daarmee wordt onder het «ontoegankelijk maken» van gegevens hetzelfde verstaan als in het geldende artikel 125o, tweede lid, Sv, te weten het treffen van maatregelen ter voorkoming dat de beheerder van een geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Aangezien het in bepaalde gevallen technisch niet goed mogelijk kan zijn om de gegevens effectief

ontoegankelijk te maken, is de verplichting tot het ontoegankelijk maken, evenals in het geldende artikel 54a Sr het geval is, geclausuleerd. De ontoegankelijkmaking van de gegevens kan plaatsvinden door de desbetreffende gegevens te verwijderen, dan wel de toegang daartoe te blokkeren. Blokkering kan aan de orde zijn als de gegevens niet kunnen worden verwijderd, zodat de gegevens voor de gebruikers niet raadpleegbaar zijn. Om aan het bevel tot ontoegankelijkmaking te voldoen, dient de blokkering voort te duren zolang de gegevens worden aangeboden.
Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de ontoegankelijkmaking moet tot opheffing worden over gegaan door de gegevens weer ter beschikking te stellen van de beheerder van het geautomatiseerde werk. Het belang van strafvordering verzet zich niet meer tegen de opheffing als de ontoegankelijkmaking niet langer noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe feiten. Als het belang van strafvordering wel duurzaam, aanwezig blijft, zal dit leiden tot een definitieve beslissing tot vernietiging via de procedure van artikel 354 of artikel 552fa Sv.

Vierde lid

De officier van justitie behoeft voor het bevel aan de aanbieder een schriftelijke machtiging van de rechter-commissaris. De rechter-commissaris weegt de in het geding zijnde belangen af. Het betreft de belangen die zijn gediend bij strafrechtelijke handhaving van de rechtsorde, de belangen van degene die de gegevens op het internet heeft gepubliceerd, het belang van de vrijheid van meningsuiting alsmede de belangen van de aanbieder indien het bevel tot hem is gericht.

Naar aanleiding van het advies van BoF is bepaald dat de rechter-commissaris de machtiging niet afgeeft dan nadat de aanbieder tot wie de vordering is gericht, in de gelegenheid is gesteld te worden gehoord. In de consultatieversie van het conceptwetsvoorstel was bepaald dat de officier van justitie het bevel tot ontoegankelijkmaking slechts kon geven nadat degene toe wie het bevel was gericht, in de gelegenheid was gesteld te worden gehoord. Bij nader inzien ligt het in de rede dat de rechter-commissaris wordt belast met het horen van degene tot wie het bevel is gericht, zodat de rechter-commissaris zich een goed beeld kan vormen van de noodzaak en rechtmatigheid van het bevel van de officier van justitie. De aanbieder tot wie de vordering is gericht is bevoegd zich bij het horen te doen bijstaan door een raadsman. De aanbieder moet op deze bevoegdheid worden gewezen. Doorgaans zal er een spoedeisend belang zijn bij het bevel tot het ontoegankelijk maken van gegevens. Indien geen gebruik wordt gemaakt van de mogelijkheid te worden gehoord of het horen niet mogelijk blijkt, kan de rechter-commissaris op vordering van de officier van justitie een beslissing nemen over de afgifte van een machtiging.

Artikel II, onderdeel E

Artikel 126g

De wijziging van het derde lid van dit artikel strekt ertoe de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt, zodat de rechter-commissaris hiermee in zijn toetsing

rekening kan houden. Dit wordt geregeld in artikel 126nba, eerste lid, onder c, en tweede lid, onder h, Sv.

Artikel II, onderdeel F

Artikel 126la

Dit onderdeel betreft de schrapping van artikel 126la, vanwege de opneming van de begrippen «aanbieder van een communicatiedienst» en «gebruiker van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering. Voor de toelichting op dit onderdeel kan worden verwezen naar de toelichting op de artikelen 138e en 138f Sv.

Artikel II, onderdeel G

Voorgesteld wordt aan Titel IVA van het Eerste Boek een nieuwe afdeling toe te voegen. Dit houdt verband met de opneming van de bevoegdheid van het onderzoek in een geautomatiseerd werk in deze titel. Weliswaar omvat deze bijzondere opsporingsbevoegdheid deels enkele reeds bestaande bijzondere opsporingsbevoegdheden, deze bevoegdheid kan echter zelfstandig worden uitgeoefend, waarbij aan specifieke voorwaarden dient te zijn voldaan, hetgeen plaatsing in een afzonderlijke afdeling rechtvaardigt.

Artikel 126nba

Eerste lid

Dit betreft het bevel tot onderzoek in een geautomatiseerd werk. Het bevel kan worden gegeven aan een daartoe aangewezen opsporingsambtenaar. Dit kunnen ambtenaren zijn van eenheden die behoren tot de politie, de Koninklijke marechaussee of de bijzondere opsporingsdiensten, en die worden belast met de technische handelingen ter uitvoering van het bevel tot het onderzoek in een geautomatiseerd werk. Het is gewenst dat een ingrijpende en risicovolle bevoegdheid als deze alleen kan worden opgedragen aan een beperkte categorie opsporingsambtenaren die over specialistische kennis beschikken. Hiervoor kan worden verwezen naar het algemeen deel van deze toelichting. De verzamelde onderzoeksgegevens kunnen worden verwerkt door een opsporingsambtenaar die is belast met de opsporing van strafbare feiten.

Het onderzoek kan plaatsvinden in een geautomatiseerd werk. In het licht van de jurisprudentie van de Hoge Raad kan dit ook een gegevensdrager betreffen die daarmee in verbinding staat. Voor een gegevensdrager kan worden gedacht aan een usb-stick, een op afstand te bereiken server (bij Clouddiensten) of een externe harde schijf die aangesloten is op een computer.

Vereist is dat het geautomatiseerde werk bij de verdachte in gebruik is. Dit betekent dat het op grond van feiten of omstandigheden aannemelijk dient te zijn dat de verdachte gebruik maakt van het geautomatiseerde werk. Niet is vereist dat de verdachte de enige gebruiker is. Dit betekent bijvoorbeeld dat een router, die bij de meerdere personen in gebruik is, kan worden binnengedrongen mits deze ook bij de verdachte in gebruik is. Dit betekent ook dat een geautomatiseerd werk, dat in verbinding staat met het geautomatiseerde werk dat is binnengedrongen, kan worden binnengedrongen en onderzocht mits dit geautomatiseerde werk bij de verdachte in gebruik is en een bevel tot het binnendringen van dat werk is afgegeven. De ontwikkeling van de technologie maakt het eenvoudig mogelijk om gegevens in de Cloud op te slaan. Een server kan, op grond

van de definitie in artikel 80sexies Sr, worden aangemerkt als een geautomatiseerd werk. De gegevens zijn dan opgeslagen in een ander geautomatiseerd werk dat bij de verdachte in gebruik is, namelijk de server waarop de gegevens zijn opgeslagen. Voor de vastlegging van die gegevens is dan een specifiek bevel tot het binnendringen van dat geautomatiseerde werk vereist, vanwege de beperking van de bevoegdheid tot vastlegging van gegevens tot de gegevens die in het geautomatiseerde werk zijn opgeslagen. Wel kan een bevel tot het binnendringen van een geautomatiseerd werk tevens betrekking hebben op een ander geautomatiseerd werk, zoals een server die vanuit het geautomatiseerde werk kan worden benaderd, zodat dan kan worden «doorgestapt» naar een ander geautomatiseerd werk.

In zijn advies over het conceptwetsvoorstel heeft de korpschef van de politie bezwaar gemaakt tegen de beperking van de bevoegdheid tot systemen die bij de verdachte in gebruik zijn, omdat een dergelijke beperking niet goed past in het systeem van de bijzondere opsporingsbevoegdheden en in de opsporingspraktijk voor de nodige onduidelijkheid en discussie zal gaan zorgen. Dit bezwaar deel ik niet. De voorgestelde bevoegdheid vormt een ingrijpende aantasting van de persoonlijke levenssfeer van de betrokkene, het ligt dan ook in de rede dat strikte voorwaarden worden verbonden aan de inzet daarvan. Vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer is het niet goed verdedigbaar dat een computer wordt binnengedrongen die niet in gebruik is bij de persoon die wordt verdacht van betrokkenheid bij ernstige misdrijven. Overigens kan worden opgemerkt dat dit vereiste feitelijk moet worden uitgelegd. Dit wil zeggen dat er op basis van het opsporingsonderzoek voldoende feiten en omstandigheden voor de veronderstelling (of: aanwijzingen) dat de verdachte het geautomatiseerde werk gebruikt of gaat gebruiken. Dit is ook het geval als hij gebruik maakt van een geautomatiseerd werk van een ander, bijvoorbeeld van een huisgenoot of partner. In het geval dat de boekhouding in de Cloud wordt bijgehouden, kan de politie op basis van de voorgestelde bevoegdheid binnendringen in het gedeelte van de Cloud, en daarmee ook de server, waar de gegevens rond de boekhouding worden opgeslagen of verwerkt. De NOvA vreest dat het onderzoek in een geautomatiseerd werk met het oog op de vaststelling van de identiteit van de gebruiker wordt toegepast in situaties waarin niet bekend is in hoeverre de betrokken persoon daadwerkelijk de gebruiker van het geautomatiseerde werk is. Dit is echter niet toegestaan; op grond van feiten en omstandigheden dient voldoende aannemelijk te zijn dat de verdachte het geautomatiseerde werk gebruikt of heeft gebruikt, voordat de bevoegdheid tot het binnendringen kan worden toegepast. Wel kan in het kader van een dergelijk onderzoek de identiteit van de verdachte worden vastgesteld. Dit kan van belang zijn voor het inzetten van bijzondere opsporingsbevoegdheden of het bepalen van de richting van het opsporingsonderzoek.

Voor de toelichting op de doelen van het onderzoek in een geautomatiseerd werk kan worden verwezen naar het algemeen deel van deze toelichting. Aanvullend kan nog worden opgemerkt dat, anders dan voor de huidige doorzoeking ter vastlegging van gegevens, de vastlegging van gegevens ook betrekking kan hebben op gegevens die na het tijdstip van afgifte van het bevel worden opgeslagen. De beperking tot de gegevens die op de plaats van de doorzoeking aanwezig zijn volgde uit het feit dat de bevoegdheid tot de doorzoeking ter vastlegging van gegevens is afgeleid van de bevoegdheid tot inbeslagneming van daarvoor vatbare voorwerpen (zoals een computer). De inbeslagnemingsbevoegdheid mag uit de aard der zaak slechts worden uitgeoefend indien redelijkerwijs kan worden vermoed dat op de te doorzoeken plaats daarvoor vatbare voorwerpen aanwezig zijn. Indien de doorzoekingsbevoegdheid wordt

gebruikt om gedurende enige tijd (tijdens de doorzoeking) binnenkomende en uitgaande gegevens te onderscheppen, dan zou feitelijk sprake zijn van het opnemen of aftappen van telecommunicatie (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 49). Op dit punt wordt met dit wetsvoorstel een andere afweging gemaakt. De informatietechnologie biedt de mogelijkheid om stromende gegevens op te slaan zonder dat er sprake is van communicatie. Daarvoor kan worden gedacht aan het uitwisselen van strafbare afbeeldingen, zoals kinderpornografie. Het is voor de criminaliteitsbestrijding van essentieel belang dat ook dergelijke gegevens kunnen worden vastgelegd ten behoeve van de waarheidsvinding. Daarbij geldt onverkort dat voor het opnemen van communicatie altijd een afzonderlijk bevel is vereist, op grond van de bevoegdheid tot het aftappen van communicatie of het direct afluisteren. Hiervoor kan ook worden verwezen naar het algemeen deel van deze toelichting. Met het gebruik van de term «vastlegging» van gegevens wordt gedoeld op het overnemen (of: kopiëren) van gegevens die zijn opgeslagen, zonder dat deze uit de beschikkingsmacht van de bezitter raken. Hiermee wordt ook het onderscheid met het aftappen van communicatie tot uitdrukking gebracht.

De toepassing van de maatregel van de ontoegankelijkmaking van gegevens is in het algemeen deel van deze toelichting aan de orde gekomen. De rechter kan gelasten dat de gegevens worden vernietigd. De voorwaarden daarvoor zijn identiek aan die van de ontoegankelijkmaking, dat wil zeggen dat het moet gaan om gegevens met betrekking tot welke of met behulp waarvan een strafbaar feit is begaan of dat de vernietiging noodzakelijk is ter voorkoming van nieuwe strafbare feiten. In de andere gevallen gelast de rechter de opheffing van de ontoegankelijkmaking.

Met de formulering dat in het belang van het onderzoek gegevens kunnen worden vastgelegd wordt tot uitdrukking gebracht dat de gegevens uitsluitend kunnen worden vastgelegd voor zover dat noodzakelijk is voor de waarheidsvinding dan wel ter beëindiging van een strafbaar feit of de voorkoming van nieuwe strafbare feiten. Dit laatste is aan de orde bij de ontoegankelijkmaking van gegevens.

De Rvdr onderschrijft de expliciete uitsplitsing naar een aantal verschillende doelen omdat hiermee wordt bewerkstelligd dat reeds bij het vragen van een machtiging aan de rechter-commissaris concreet en helder wordt gemotiveerd waarvoor deze ingrijpende bevoegdheid zal worden toegepast. Het College van procureurs-generaal merkt echter op dat het bevel tot het onderzoek in een geautomatiseerd werk facilitair moet worden gezien aan de uitoefening van de bevoegdheden, genoemd in de (voormalige) onderdelen d. tot en met e., thans de onderdelen b. en c., en vraagt of de (voormalige) onderdelen a., b. en c., thans de onderdelen a., d. en e., ook moeten worden gezien als facilitair aan andere opsporingsbevoegdheden en onderzoekshandelingen. In reactie hierop kan worden opgemerkt dat de inzet van de bevoegdheden, thans genoemd in de onderdelen b. en c. (het aftappen van communicatie en de stelselmatige observatie), de inzet van afzonderlijk geregelde bijzondere opsporingsbevoegdheden betreft. Dit vereist een afzonderlijk bevel. Naar aanleiding van het advies van het College is dit in het algemeen deel van deze toelichting verhelderd. De inzet van de bevoegdheden, genoemd in de onderdelen a., d. en e. betreffen echter geen zelfstandige opsporingsbevoegdheden. Deze handelingen kunnen dan ook worden verricht op basis van het bevel tot het onderzoek in een geautomatiseerd werk. Daarvoor is uiteraard wel vereist dat het bevel van de officier van justitie de desbetreffende handelingen vermeld. Naar aanleiding van het advies van het College is de tekst van dit onderdeel verhelderd, dit komt hieronder, bij de toelichting op het tweede lid, aan de orde.

In onderdeel c wordt geregeld dat de officier van justitie ter uitvoering van het bevel, bedoeld in artikel 126g kan bepalen dat een technisch hulpmiddel op een persoon wordt bevestigd in het kader van de stelselmatige observatie van een geautomatiseerd werk.

Gekozen is voor de term «onderzoek in een geautomatiseerd werk», omdat de term «doorzoeking» verband houdt met het doorzoeken van een fysieke plaats, als bedoeld in artikel 96 e.v. Sv. Ook in artikel 125i Sv is door de wetgever om die reden de term «doorzoeken» gebruikt. Omdat de voorgestelde bevoegdheid ziet op het inzetten van opsporingsbevoegdheden in een digitale omgeving, zorgt de term «onderzoek in een geautomatiseerd werk» voor een duidelijk onderscheid met de opsporingsbevoegdheden die in de fysieke wereld kunnen worden toegepast.

In artikel 11.7a van de Telecommunicatiewet (Tw) is kort gezegd geregeld dat indien iemand door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van die gebruiker, deze daaraan voorafgaand de gebruiker dient te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens en van de gebruiker toestemming dient te hebben verkregen voor de desbetreffende handeling. Het vooraf informeren en verkrijgen van toestemming bij een onderzoek in een geautomatiseerd werk van iemand die verdacht wordt van een misdrijf als omschreven in artikel 67, eerste lid, Sv zou vanzelfsprekend onwenselijk zijn, omdat dit het onderzoek in gevaar zou brengen. Daarom wordt artikel 11.7a Tw buiten toepassing verklaard op handelingen ter uitvoering van een bevel van de officier van justitie. Artikel 11.7a Tw vormt de implementatie van artikel 5, derde lid, van de richtlijn betreffende privacy en elektronische communicatie (Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, Pb EU L 201/37). Deze richtlijnbepaling beoogt de persoonlijke levenssfeer van de gebruiker van elektronische communicatienetwerken te beschermen. Op de in artikel 5 bedoelde rechten en plichten kunnen uitzonderingen worden gemaakt indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van bepaalde zwaarwegende belangen, zoals de openbare veiligheid en het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten (artikel 15 van richtlijn 2002/58/EG). Met de afwijking van artikel 11.7a Tw wordt in een dergelijke uitzondering voorzien. De noodzaak van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk in het belang van de openbare veiligheid en de voorkoming en vervolging van strafbare feiten is eerder, in paragraaf 2.9.1., aan de orde gekomen.

Tweede lid

Het bevel tot onderzoek van een geautomatiseerd werk wordt schriftelijk gegeven. Het bevel moet de nodige informatie bevatten ten behoeve van de toetsing door de rechter-commissaris. Dit betreft in de eerste plaats de aard en ernst van het misdrijf en de personalia van de verdachte. Dit betreft in de tweede plaats het nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd, zoals het IP-adres, het MAC-adres, het IMEI-nummer, de hardware ID of de User Agent. Van belang is dat het object van het binnentreden voldoende precies kan worden vastgesteld. Zo zal «een server van een universiteit» te vaag zijn als basis voor de inzet van de bevoegdheid. Indien het binnendringen van een server, die onderdeel vormt van een serverpark,

wordt overwogen zal de toepassing van de bevoegdheid beperkt moeten zijn tot die bepaalde server. In het bevel zal een zodanige, objectief bepaalbare begrenzing moeten zijn opgenomen dat de rechter-commissaris de machtiging voldoende kan begrenzen. Indien bekend is dat de gegevens niet in Nederland zijn opgeslagen, dient dit in het bevel te worden vermeld. Bij de afgifte van de machtiging mag de rechter-commissaris ervan uitgaan dat de officier van justitie de regels op het gebied van de internationale samenwerking respecteert. Zoals ook in het algemeen deel aan de orde is gekomen, behoeft dit niet bij voorbaat in de weg te staan aan onverwijld optreden als de omstandigheden daartoe aanleiding geven. De uitvoering van de machtiging betreft echter vooraleerst de verantwoordelijkheid van de officier van justitie; deze functionaris dient de machtiging op zorgvuldige wijze uit te voeren en de uitvoering bij de rechter te verantwoorden. Dit betreft in de derde plaats de feiten en omstandigheden waaruit blijkt dat de voorwaarden voor onderzoek in het geautomatiseerd werk zijn vervuld. Het moet gaan om een ernstig misdrijf waarvoor voorlopige hechtenis mogelijk is en dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Het opsporingsonderzoek dient het onderzoek in een geautomatiseerd werk dringend te vorderen. Vastgesteld moet worden dat de gegevens niet op een minder ingrijpende wijze kunnen worden verkregen. Hierbij moet rekening worden gehouden met de mogelijke gevolgen voor het geautomatiseerde werk. Ook zijn de proportionaliteit en subsidiariteit van belang voor de beoordeling van het voorgenomen onderzoek in het geautomatiseerde werk. Dit betreft in de vierde plaats de aard en functionaliteit van het technische hulpmiddel. Dit vereist een aanduiding van de aard en functionaliteiten van de te gebruiken software en de functionaliteiten die in het concrete onderzoek ingeschakeld worden (zoals het opnemen van geluid, het maken van screenshots of het vastleggen van toetsaanslagen). In de vijfde plaats moet het doel of de doelen op het gebied van de opsporing van strafbare feiten worden gespecificeerd. Dit is in het algemeen deel reeds aan de orde gekomen. Naar aanleiding van het advies van het College van procureurs-generaal is in onderdeel d verhelderd dat in de gevallen waarin het onderzoek in een geautomatiseerd werk wordt verricht met het oog op de handelingen, genoemd in het eerste lid, onderdeel a, d of e, in het bevel een omschrijving van de te verrichten handelingen moet worden opgenomen. Dit betreft de vaststelling van de identiteit van de gebruiker of het geautomatiseerde werk, het vastleggen van gegevens of het ontoegankelijk maken van gegevens. Anders dan bij de onderdelen b. en c. is voor het verrichten van deze handelingen geen afzonderlijk bevel vereist. Om de rechter-commissaris in staat te stellen tot een zorgvuldige toetsing van de proportionaliteit en subsidiariteit van de voorgenomen inzet, is het van belang dat deze in het bevel worden omschreven. Voorts dient te worden vermeld voor welk deel van het geautomatiseerde werk en voor welke categorie van gegevens aan het bevel uitvoering wordt gegeven. Dit vereist een aanduiding van de aard van het geautomatiseerde werk (bijvoorbeeld een personal computer, een server of een smartphone) en van de aard van de gegevens (bijvoorbeeld gegevens van een e-mailbox of van een harde schijf, msn-berichten of Skype communicatie). Voorts wordt vermeld het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven. Met deze formulering wordt, net als bij de bevoegdheden in een besloten plaats (artikelen 126k en 126r Sv), rekening gehouden met een lange voorbereidingstijd voordat het onderzoek in een geautomatiseerd werk daadwerkelijk wordt verricht. Ten slotte wordt, indien het een bevel tot stelselmatige observatie betreft waarbij een technisch hulpmiddel op een persoon wordt bevestigd, een melding van dit voornemen opgenomen.

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

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

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

Derde lid

Het bevel kan worden gegeven voor een periode van ten hoogste vier weken. Een dergelijke periode lijkt voldoende voor het verrichten van onderzoekshandelingen. Hiermee wordt tevens aangesloten bij de duur van een bevel tot het opnemen van vertrouwelijke communicatie of het aftappen van communicatie (artikelen 126l en 126m Sv). Deze termijn is korter dan die voor de bevoegdheid van de stelselmatige observatie, een dergelijk bevel kan worden gegeven voor een periode van ten hoogste drie maanden (artikel 126g, vierde lid Sv). Vanwege de ingrijpendheid van

de voorgestelde bevoegdheid, waarbij wordt binnengedrongen in een geautomatiseerd werk, is een kortere termijn gerechtvaardigd.

Vierde lid

De officier van justitie behoeft voor het bevel tot onderzoek in een geautomatiseerd werk een schriftelijke machtiging van de rechter-commissaris. Hiervoor kan worden verwezen naar het algemeen deel van deze toelichting.

Vijfde lid

Wanneer tijdens de inzet van de bevoegdheid blijkt dat de bevoegdheid alsnog voor een ander doel moet worden ingezet dan omschreven in het bevel waarvoor de machtiging is gegeven, dan kan het bevel worden gewijzigd of aangevuld. Dit kan aan de orde zijn als blijkt dat er aanleiding bestaat tot het verrichten van andere onderzoekshandelingen, dan waarvoor reeds een bevel is afgegeven. Een voorbeeld daarvan is een bevel tot de ontoegankelijkmaking van gegevens nadat een bevel is afgegeven dat strekt tot de vaststelling van de aanwezigheid van gegevens in het desbetreffende geautomatiseerde werk. Tevens is verlenging van het bevel mogelijk. Een dergelijke aanpassing vereist een machtiging van de rechter-commissaris.

Voorzien is in de mogelijkheid van een mondeling bevel tot wijziging, aanvulling, verlenging of beëindiging van het bevel tot onderzoek van een geautomatiseerd werk. Er kan een namelijk spoedeisend belang zijn dat strekt tot een mondeling bevel, dat verenigbaar is met de reeds doorlopen procedure voor de toepassing van de bevoegdheid. Een mondeling bevel is ook mogelijk bij andere bijzondere opsporingsbevoegdheden, zoals de stelselmatige observatie (artikelen 126g, zesde lid, en 126o, vijfde lid, Sv), de bevoegdheden in een besloten plaats (artikelen 126k en 126r, derde lid, Sv), het opnemen van vertrouwelijke communicatie (artikelen 126l en 126s, zesde lid, Sv) en het aftappen en opnemen van communicatie (artikelen 126m en 126t, achtste lid, Sv). Anders dan bij deze bijzondere opsporingsbevoegdheden is het mondelinge bevel voor onderzoek van een geautomatiseerd werk beperkt tot de aanpassing van een reeds gegeven schriftelijk bevel. Dit houdt verband met de procedurele eisen en waarborgen die zijn verbonden aan de inzet van het onderzoek in een geautomatiseerd werk. Dit onderzoek vereist een gedegen voorbereiding, inclusief het adviestraject van de CTC. Daarmee is een mondeling bevel tot onderzoek in een geautomatiseerd werk niet goed verenigbaar. In het geval van een wijziging, aanvulling, verlenging of beëindiging van het bevel kan ook de machtiging van de rechter-commissaris mondeling worden gegeven. Een mondelinge machtiging is eveneens mogelijk bij de machtiging voor het opnemen van vertrouwelijke communicatie (artikelen 126l en 126s, zevende lid, Sv), het aftappen en opnemen van communicatie (artikelen 126m en 126t, achtste lid, Sv) en het vorderen van gegevens van een aanbieder van een communicatiedienst (artikelen 126ng en 126ug, vierde lid, Sv). Anders dan bij deze bijzondere opsporingsbevoegdheden is de mogelijkheid van een mondelinge machtiging voor onderzoek in een geautomatiseerd werk beperkt tot de aanpassing van een reeds gegeven schriftelijk bevel.

De officier van justitie is gehouden tot de kennisgeving zodra het belang van het onderzoek dat toelaat. De kennisgeving blijft achterwege, indien uitreiking van de mededeling redelijkerwijs niet mogelijk is. Voor deze uitzonderingsgronden is aangesloten bij de regeling van de notificatie-plicht (artikel 126bb, eerste lid, Sv). Met de kennisgeving wordt tevens aan die notificatieplicht voldaan.

Zesde lid

In het algemeen deel van deze toelichting is de noodzaak van verwijdering van het technische hulpmiddel, nadat het onderzoek in een geautomatiseerd werk is afgerond, aan de orde gekomen. Om ieder risico uit te sluiten zal de politie de nodige inspanningen verrichten om te voorkomen dat sporen van de gebruikte software in het geautomatiseerde werk achterblijven.
In beginsel wordt een technisch hulpmiddel verwijderd nadat het onderzoek is beëindigd. De verwijdering kan langs verschillende wegen worden gerealiseerd. Op basis van de verzamelde informatie kan bijvoorbeeld worden overgegaan tot inbeslagneming van het geautomatiseerde werk. Om bij voorbaat zeker te stellen dat de software na afloop van het onderzoek wordt verwijderd of onklaar wordt gemaakt kan gebruik worden gemaakt van software waarin een functionaliteit is ingebouwd die het mogelijk maakt dat de software zichzelf vernietigt na verloop van een bepaalde, vooraf ingestelde, periode. Indien verwijdering niet kan worden gerealiseerd, en het achterblijven van (de sporen van) die software een risico zou opleveren voor het functioneren van het geautomatiseerde werk stelt de officier van justitie de beheerder van het geautomatiseerde werk daarvan in kennis en stelt de nodige informatie ter beschikking ten behoeve van de volledige verwijdering van de (sporen van de) software. De beheerder is uit hoofde van zijn functie primair verantwoordelijk voor het behoud en het gebruik van de gegevens die zijn opgeslagen in de aan zijn zorg toevertrouwde computers (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 51).

Zevende lid

Het onderzoek in een geautomatiseerd werk kan worden verricht met behulp van een technisch hulpmiddel, in de vorm van een software-applicatie. De plaatsing van de software vindt uitsluitend plaats door de daartoe aangewezen opsporingsambtenaren, ook wel aangeduid als het technische team. Deze opsporingsambtenaren dienen te voldoen aan de bij of krachtens algemene maatregel van bestuur te stellen deskundigheidseisen. Onderdeel a, biedt hiervoor een wettelijke grondslag. De eisen op het gebied van de deskundigheid van de opsporingsambtenaren worden uitgewerkt in het Besluit technische hulpmiddelen strafvordering. Voorts kunnen hierin eisen worden uitgewerkt over de samenwerking met de opsporingsambtenaren, die belast zijn met het operationele onderzoek, het zogenoemde tactische team, aan wie de resultaten van de onderzoekshandelingen ter beschikking worden gesteld.

Onderdeel b bevat een wettelijke grondslag voor het nader bij algemene maatregel van bestuur regelen van eisen aan de geautomatiseerde vastlegging (logging) van de onderzoekshandelingen die al dan niet met behulp van een technisch hulpmiddel worden verricht. De logging van de gegevens over de uitvoering van een bevel van de officier van justitie maakt het mogelijk achteraf controle uit te oefenen op de integriteit van deze handelingen en van de informatie die met behulp daarvan is vastgelegd.

Achtste lid

In paragraaf 2.8 is ingegaan op het onderzoek in een geautomatiseerd werk in het licht van de uitvoerende rechtsmacht. Daarbij is de situatie aan de orde gekomen dat de locatie van gegevens niet altijd bekend is, noch de staat die betrokken is bij de opslag of verwerking van de gegevens. Het optreden in dergelijke gevallen kan onder omstandigheden betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd

werk waarvan niet bekend is waar zich dit bevindt. Aangegeven is dat een dergelijk optreden zeer zorgvuldig dient te worden ingekaderd, op basis van een zoveel mogelijk stapsgewijze aanpak. Het optreden in concrete gevallen zal worden afgewogen op basis van criteria, die betrekking hebben 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, de aard van de te verrichten opsporingshandelingen, de risico's voor het geautomatiseerde werk en de rechtshulprelatie met het betreffende land. Dit lid biedt de mogelijkheid voor nadere uitwerking van deze criteria bij algemene maatregel van bestuur.

Artikel II, onderdelen H en I

Artikel 126ng en 126ni

De wijziging van de artikelen 126ng, eerste lid, en 126i, tweede lid, hangen samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel J

Artikel 126o

De wijziging van het derde lid van dit artikel strekt ertoe de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt, zodat de rechter-commissaris hiermee in zijn toetsing rekening kan houden. Dit wordt geregeld in de artikel 126uba, eerste lid, onder c, en tweede lid, onder h, Sv.

Artikel II, onderdeel K

Artikel 126t

De wijziging van het tweede lid van dit artikel hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel L

Artikel 126uba

Dit artikel betreft de overeenkomstige toepassing van artikel 126nba op een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven. Voor de toelichting op dit artikel wordt verwezen naar de toelichting op artikel 126nba, met dien verstande dat in het artikel voor de toepassing van de bevoegdheden van het aftappen van communicatie, het opnemen van vertrouwelijke communicatie en de stelselmatige observatie (artikelen 126s, 126t en 126o Sv) telkens wordt verwezen naar de bestaande bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden.

Artikel II, onderdeel M

Artikel 126zd

De wijziging van het vierde lid van dit artikel strekt ertoe de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt, zodat de rechter-commissaris hiermee in zijn toetsing rekening kan houden. Dit wordt geregeld in het voorgestelde artikel 126zpa, eerste lid, onder c, en tweede lid, onder f, Sv.

Artikel II, onderdeel N

Artikel 126zg

De wijziging van het eerste lid van dit artikel hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel O

Artikel 126zi

De wijziging van het eerste lid hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «gebruiker van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel P

Artikel 126zo

De wijziging van het eerste lid hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel Q

Dit onderdeel betreft de toevoeging van een nieuwe afdeling aan de Derde afdeling van Titel VB van het Eerste Boek. Dit betreft de bijzondere bevoegdheden tot opsporing van terroristische misdrijven.

Artikel 126zpa

In dit artikel wordt het bepaalde in artikel 126nba in geval van aanwijzingen van een terroristisch misdrijf. Voor de toelichting wordt verwezen naar de toelichting op artikel 126nba, met dien verstande dat in het artikel voor de toepassing van de bevoegdheden van het aftappen van communicatie, het opnemen van vertrouwelijke communicatie en de stelselmatige observatie (artikelen 126zf, 126zg en 126zd, eerste lid, onder a Sv) telkens wordt verwezen naar de bestaande bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden.

Artikel II, onderdeel R

Artikel 126bb

Dit onderdeel strekt ter reparatie van artikel 126bb Sv. Het betreft de mededelingsplicht van de officier van justitie met betrekking tot de toepassing van bijzondere opsporingsbevoegdheden. In het tweede lid, onderdeel b, van dit artikel wordt verwezen naar de artikelen 126m, derde lid, onderdeel c, en 126t, derde lid, onderdeel c, Sv. Dit moet echter zijn: de artikelen 126m, tweede lid, onderdeel c, en 126t, tweede lid, onderdeel c, Sv. Met de voorgestelde aanpassing wordt deze omissie hersteld.

Artikel II, onderdeel S

Titel VD Derde afdeling

Deze wijziging houdt verband met de voorgestelde aanvulling van de regeling voor de bewaring en de vernietiging van processen-verbaal en andere voorwerpen en het gebruik van gegevens voor een ander doel dient het opschrift van de Derde afdeling te worden gewijzigd. Dit wordt hieronder, bij artikel 126cc, toegelicht.

Artikel II, onderdeel T

Artikel 126cc

Dit artikel bevat regels voor de bewaring en de vernietiging van processen-verbaal en andere voorwerpen en het gebruik van gegevens voor een ander doel.

Voorgesteld wordt aan dit artikel regels toe te voegen in het vijfde en zesde lid over de bevoegdheid van de officier van justitie om te bepalen dat gegevens, die zijn aangetroffen bij het onderzoek in een geautomatiseerd werk, ontoegankelijk worden gemaakt. De maatregel van de ontoegankelijkmaking van gegevens is geregeld in artikel 125o, voor de doorzoeking ter vastlegging van gegevens. Met het voorgestelde vijfde lid is het bepaalde in artikel 125o, tweede en derde lid, van overeenkomstige toepassing.

De maatregel van ontoegankelijkmaking van gegevens betreft een maatregel met een voorlopig karakter, vergelijkbaar met de inbeslagneming tot onttrekking aan het verkeer. De ontoegankelijkmaking heeft ten doel te voorkomen dat de gegevens kunnen worden gebruikt voor het beramen of plegen van strafbare feiten. Indien het belang van strafvordering zich daartegen niet verzet moet tot opheffing van de maatregel worden overgegaan door de gegevens ter beschikking te stellen aan de verdachte. Dit is aan de orde als de ontoegankelijkmaking niet langer noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. In andere gevallen zal de rechter een definitieve beslissing moeten nemen over vernietiging van de gegevens, op basis van de procedure van artikel 354 of 552fa Sv. Hiervoor kan ook worden verwezen naar het algemeen deel van deze toelichting.

In artikel 125n Sv is de vernietiging geregeld van gegevens die zijn vastgelegd tijdens een doorzoeking ter vastlegging van gegevens. Het is wenselijk dat deze regeling ook van toepassing is op de ontoegankelijkmaking van gegevens, in het kader van een onderzoek in een geautomatiseerd werk. Met het voorgestelde zesde lid is het bepaalde in artikel 125n, tweede lid, van overeenkomstige toepassing. Dit betekent dat de

vastgelegde gegevens worden vernietigd zodra blijkt dat zij van geen betekenis zijn voor het strafvorderlijk onderzoek dat tot vastlegging heeft geleid.

Op grond van de regeling van artikel 126dd Sv kan de officier van justitie bepalen dat de gegevens, die zijn verkregen in het kader van het aftappen van communicatie, het direct afluisteren en de stelselmatige observatie met een technisch hulpmiddel worden gebruikt voor een ander strafrechtelijk onderzoek of voor de verwerking van gegevens met het oog op de verkrijging van inzicht in de betrokkenheid van personen bij ernstige strafbare feiten. Deze regeling is eveneens van toepassing als deze bevoegdheden worden uitgeoefend in het kader van een onderzoek in een geautomatiseerd werk.

Artikel II, onderdeel U

Artikel 126ee

Dit artikel biedt een grondslag voor het stellen van eisen aan technische hulpmiddelen die gebruikt worden bij de inzet van de bevoegdheden in de titels IVA tot en met VC. Door middel van wijziging van de onderdelen a en b wordt geregeld dat regels kunnen worden gesteld over de technische hulpmiddelen die gebruikt worden bij het onderzoek in een geautomatiseerd werk.
De regels over de opslag, plaatsing, verstrekking en verwijdering van het technische hulpmiddel zullen worden opgenomen in het Besluit technische hulpmiddelen strafvordering. Het Besluit geeft regels voor de inzet van camera's en richtmicrofoons die worden gebruikt bij de observatie (artikelen 126g, 126o en 126zd, eerste lid, onder a, Sv), het opnemen van vertrouwelijke communicatie (artikelen 126l, 126s en 126zf Sv) en het aftappen en opnemen van communicatie zonder medewerking van de aanbieder (artikelen 126m, 126t en 126zg Sv). Daarnaast bevat het Besluit eisen voor de inzet van deze technische hulpmiddelen. Aanvullend op de normen voor de camera en de richtmicrofoon zullen regels worden vastgelegd voor de opslag, plaatsing, verstrekking en verwijdering van de softwareapplicatie die kan worden gebruikt voor onderzoek in een geautomatiseerd werk en de technische eisen voor de softwareapplicatie. Daarbij zullen de volgende uitgangspunten worden gehanteerd:

- De wettelijke verankering van de eisen voor de keuring van de software brengt met zich dat de mogelijkheid bestaat om technische hulpmiddelen van verschillende leveranciers te betrekken, op voorwaarde dat deze middelen aan de wettelijke eisen voldoen.
- Er zullen eisen worden gesteld aan de voor de inrichting en de werking van de softwareapplicatie met het oog op de vastlegging van de gegevens en het voorkomen van misbruik door derden. Daarbij zal het uitgangspunt van «privacy enhancing technology» voorop staan. Dit wil zeggen dat de inrichting en werking van de softwareapplicatie de persoonlijke levenssfeer van burgers beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodig dan wel ongewenst gebruik van persoonsgegevens, zonder verlies van functionaliteit. Een belangrijk aspect vormt het vereiste dat de werking van de software kan worden gedifferentieerd naar het gebruik van verschillende functionaliteiten. Afhankelijk van het te bereiken doel zullen de in het bevel van de officier van justitie aangegeven functionaliteiten worden ingeschakeld.
- Het transport van de signalen vanuit het geautomatiseerde werk naar de server van de politie vindt plaats door middel van een beveiligde verbinding, waarbij de gegevens worden versleuteld op een wijze die met de thans beschikbare technieken niet of nauwelijks is te kraken. Daarvoor kan bij de huidige stand van de techniek worden gedacht aan

een versleuteling met een crypto grafische sterkte van ten minste,AES256. De gegevens worden onverwijld naar de politieserver gezonden en automatisch voorzien van een digitale handtekening (hashcode), zodat de gegevens daarna niet kunnen worden gewijzigd zonder dat dit zichtbaar is. De server bij de politie dient binnen een beveiligde omgeving te zijn geplaatst en aan bepaalde eisen te voldoen ter voorkoming van manipulatie van de gegevens.

- Om vast te stellen of een technisch hulpmiddel aan de normen voldoet dient dit te zijn goedgekeurd door de keuringsdienst van de politie. Alleen wanneer een technisch hulpmiddel is gecontroleerd en gecertificeerd, mag het door de politie worden gebruikt. Hiermee wordt aangesloten bij de rol die de keuringsdienst heeft bij de keuring van technische hulpmiddelen die op grond van de bestaande bevoegdheid tot het opnemen van vertrouwelijke communicatie worden ingezet. De keuringsdienst maakt daarbij gebruik van een keuringsprotocol waarin de eisen zijn opgenomen waaraan een technisch hulpmiddel moet voldoen. Zodra de keuringsdienst een technisch hulpmiddel heeft goedgekeurd wordt aan de voorziening een referentienummer gekoppeld. Dit referentienummer kan gedurende het verdere verloop van het opsporingsonderzoek worden gebruikt om het desbetreffende hulpmiddel aan te duiden in het proces-verbaal. Hiermee wordt aangesloten bij de werkwijze die wordt gevolgd bij de inzet van technische hulpmiddelen bij het opnemen van vertrouwelijke communicatie. Zo kan worden gewaarborgd dat de specificaties van technische hulpmiddelen niet worden prijsgegeven. Dit is van groot belang voor de afscherming van gevoelige opsporingsmethoden.
- De ontwikkeling en inzet van de software is erop gericht om zoveel mogelijk te voorkomen dat het binnendringen, installeren of functioneren van de software digitale sporen achterlaat in het desbetreffende geautomatiseerde werk. Het is echter bij voorbaat niet uitgesloten dat dit het geval is. In het geval dat de software wordt herkend, is het van essentieel belang dat deze niet te herleiden is tot de politie. Om misbruik door derden van de software te voorkomen, zullen regels gesteld worden omtrent het beveiligen van het gebruik van de software.

Artikel II, onderdeel V

Artikelen 138e en 138f

Naar aanleiding van het Cybercrime Verdrag is een begripsomschrijving van de begrippen «aanbieder» en «gebruiker» ingevoegd in het Wetboek van Strafvordering. Dit betreft artikel 126la, dat van toepassing is op de zevende afdeling («Onderzoek van communicatie door middel van geautomatiseerde werken») van Titel IVA van het Wetboek van Strafvordering (Bijzondere bevoegdheden tot opsporing»). De beperking van het toepassingsgebied tot de eerdergenoemde zevende afdeling blijkt echter te beperkt, omdat de begrippen «aanbieder» en «gebruiker» ook elders worden gebruikt. Dit betreft bijvoorbeeld de Titel V («Bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van misdrijven in georganiseerd verband») en Titel en Tiel VB (Bijzondere bevoegdheden tot opsporing van terroristische misrijven). Wat betreft Titel V kan worden gewezen op de artikelen 126t, 126u, 126ua en 126ug Sv. Wat betreft Titel VB kan worden gewezen op de artikelen 126zg, 126zh, 126zi, 126zj en 126zo Sv.
Met het voorgestelde artikel 125p wordt het begrip «aanbieder» geïntroduceerd in Titel IV («Enige bijzondere dwangmiddelen») van het Wetboek van Strafvordering. Nu de begrippen «aanbieder» en «gebruiker» op verschillende plaatsen in het Wetboek van Strafvordering worden

gehanteerd, ligt het in de rede om de omschrijving van deze begrippen op te nemen in Titel VI, dat betrekking heeft op de betekenis van sommige in het wetboek voorkomende uitdrukkingen. Hiermee wordt tevens gevolg gegeven aan het advies van KPN over het voorgestelde artikel 125p Sv (punt 15).

Artikel II, onderdeel W

Artikel 354

Eerste lid

In dit artikel is geregeld dat de rechtbank, in geval van een beslissing over inbeslaggenomen voorwerpen, tevens een beslissing neemt over de met toepassing van artikel 125o Sv ontoegankelijk gemaakte gegevens. Nu in dit wetsvoorstel wordt voorgesteld in de Derde Afdeling van Titel VD een bevoegdheid op te nemen voor de officier van justitie tot het ontoegankelijk maken van gegevens die zijn aangetroffen bij een onderzoek in een geautomatiseerd werk, dient dit lid te worden aangevuld. Daartoe strekt de voorgestelde wijziging van het eerste lid.

Derde lid

De voorgestelde wijziging van het derde lid van dit artikel regelt dat in het geval dat de rechtbank een veroordeling, vrijspraak of ontslag van alle rechtsvervolging uitspreekt, tevens een beslissing wordt genomen over het bevel tot ontoegankelijkmaking van gegevens indien een dergelijk bevel nog niet is opgeheven. Het bevel kan zijn opgeheven doordat de raadkamer van de rechtbank, naar aanleiding van het beklag van een belanghebbende, heeft besloten tot opheffing van het bevel. Als het bevel nog niet is opgeheven dan wordt alsnog een beslissing over het bevel genomen. Het bevel kan geheel of gedeeltelijk worden opgeheven.

Artikel II, onderdeel X

Artikel 552a

Eerste lid

Dit lid bevat het herstel van enkele omissies. In de eerste plaats wordt in dit artikel aan belanghebbenden de mogelijkheid geboden zich schriftelijk te beklagen over de inbeslagneming van voorwerpen. De reikwijdte van deze bepaling is uitgebreid naar aanleiding van de opneming van de artikelen over de doorzoeking ter vastlegging van gegevens (artikelen 125i tot en met 125o Sv) en het vorderen van gegevens (artikelen 126nc tot en met 126nh en 126uc tot en met 126uh Sv). Daarbij is onder meer voorzien in de mogelijkheid voor belanghebbenden om zich te beklagen over de vordering medewerking te verlenen aan het ontsleutelen van gegevens op grond van de artikelen 125k, tweede lid, en 126nh en 126uh, eerste lid, Sv. Dit betreft echter geen vordering, maar een bevel tot het ontsleutelen van gegevens. In de tweede plaats is de verwijzing naar artikel 125o niet volledig, nu wordt voorgesteld in Titel VD een bevoegdheid op te nemen voor de officier van justitie tot het ontoegankelijk maken van gegevens die zijn aangetroffen bij een onderzoek in een geautomatiseerd werk. In de derde plaats is ten onrechte niet voorzien in de mogelijkheid voor belanghebbenden om zich te beklagen over de vordering tot het verschaffen van toegang tot de aanwezige geautomatiseerde werken of delen daarvan, dan wel het ter beschikking stellen van kennis omtrent de beveiliging, op grond van artikel 125k, eerste lid, Sv. Voorgesteld wordt

deze mogelijkheid aan het eerste lid van artikel 552a, eerste lid, Sv toe te voegen.

Derde lid

Het is van belang dat belanghebbenden zich ook kunnen beklagen over een door de rechter-commissaris afgegeven bevel tot ontoegankelijkmaking van gegevens, op grond van het voorgestelde artikel 125p Sv. Met dit lid wordt de belanghebbenden de mogelijkheid geboden van beklag tegen een dergelijk bevel. Dit betreft in de eerste plaats de aanbieder tot wie het bevel is gericht, maar dit kan ook andere belanghebbenden betreffen, zoals personen die de gegevens beschikbaar hebben gesteld voor de verspreiding door middel van het internet. Het beklag kan zich richten op het ontbreken van de noodzaak tot ontoegankelijkmaking om strafbare feiten te beëindigen of om nieuwe strafbare feiten te voorkomen.

Tegen de beschikking op het klaagschrift staat voor zowel de officier van justitie als de klager beroep in cassatie open (artikel 552d, tweede lid, Sv). Het cassatieberoep moet door de klager binnen veertien dagen na de betekening worden ingesteld.

De Rvdr adviseert uitdrukkelijk te voorzien in een schadevergoedingsprocedure in het geval het beklag door de raadkamer van de rechtsbank gegrond wordt verklaard of indien de strafrechter in zijn uitspraak alsnog besluit tot gehele of gedeeltelijke opheffing van de maatregel. Naar aanleiding hiervan wordt opgemerkt dat het Wetboek van Strafvordering in een specifieke procedure voorziet voor de vergoeding van schade als gevolg van inverzekeringstelling of voorlopige hechtenis en de zaak is geëindigd zonder oplegging van straf of maatregel. Het lijkt minder wenselijk te voorzien in een afzonderlijke procedure, specifiek voor de ontoegankelijkmaking van gegevens, op grond van artikel 54a Sr. Zoals in het algemeen deel van deze toelichting is opgemerkt (paragraaf 2.5) kan een benadeelde eventuele schade verhalen op de Staat der Nederlanden op grond van onrechtmatige daad (artikel 6:162 Burgerlijk Wetboek), en daartoe een claim indienen bij het arrondissementsparket of het Parket-Generaal.

Vierde lid

Dit betreft een aanvulling van dit lid met het bevel tot ontoegankelijkmaking van gegevens. Het klaagschrift moet zo spoedig mogelijk na de kennisneming van het bevel van de rechter-commissaris worden ingediend. Het is de bedoeling dat de klager daarvoor niet meer tijd neemt dan hij in redelijkheid geacht kan worden nodig te hebben. Onder omstandigheden is denkbaar dat de rechter een kennelijk door nalatigheid vertraagde klacht op die grond niet ontvankelijk acht.

Negende lid

In het geval het beklag gegrond wordt verklaard kan de belanghebbende desgewenst bij de civiele rechter schadevergoeding vorderen.

Artikel II, onderdeel Y

Artikel 552fa

De verwijzing in het eerste lid van dit artikel naar artikel 125o is niet volledig, nu wordt voorgesteld in Titel VD een bevoegdheid op te nemen voor de officier van justitie tot het ontoegankelijk maken van gegevens die

zijn aangetroffen bij een onderzoek in een geautomatiseerd werk. Daarom wordt voorgesteld in dit artikel een verwijzing naar artikel 126cc, vijfde lid, op te nemen.

Artikel II, onderdelen Z en AA

Artikelen 552ww en 552dddd

De wijziging van het derde lid van deze artikelen hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «gebruiker van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel BB

Artikel 577bb

De wijziging van het eerste lid van dit artikel hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel CC

Artikel 577be

De wijziging van het eerste lid van dit artikel hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «gebruiker van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel DD

Artikel 577bf

De wijziging van het eerste lid van dit artikel hangt samen met de schrapping van artikel 126la, vanwege de opneming van het begrip «aanbieder van een communicatiedienst» in Titel VI van het Wetboek van Strafvordering.

Artikel II, onderdeel EE

Artikel 592

Het tweede lid van dit artikel geeft een regeling voor de vergoeding van de kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 126m, 126n, 126nc tot en met 126ni, 126t, 126u, 126uc tot en met 126ui, en 126zja tot en met 126zp Sv. In deze opsomming zijn de artikelen 126na, 126ua, 126zg, 126zh en 126zi Sv ten onrechte niet vermeld. Met de opneming van een verwijzing naar deze artikelen wordt deze omissie hersteld.

Artikel III

In het wetsvoorstel is een evaluatiebepaling opgenomen. Daarvoor is aangesloten bij het model van de Aanwijzingen voor de regelgeving (Ar 164).

Artikel IV

Dit artikel voorziet in een samenloopbepaling. Diverse wijzigingen die met dit wetsvoorstel worden gemaakt, lopen samen met wetswijzigingen in thans aanhangige wetsvoorstellen. Dit artikel voorziet in aanpassing van onderhavig wetsvoorstel, indien de aanhangige wetsvoorstellen eerder in werking treden dan dit wetsvoorstel.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff