

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)

INHOUDSOPGAVE MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding
2. Onderzoek in een geautomatiseerd werk
 - 2.1. De noodzaak van de voorgestelde bevoegdheid
 - 2.2. De reikwijdte van de voorgestelde bevoegdheid en de plaatsing in het Wetboek van Strafvordering
 - 2.3. De doelen van het onderzoek in een geautomatiseerd werk
 - 2.4. De juridische voorwaarde voor de inzet van de voorgestelde bevoegdheid
 - 2.5. De inzet van de bevoegdheid
 - 2.6. De toetsing van de inzet van de voorgestelde bevoegdheid
 - 2.7. De wettelijke regeling in buurlanden (België, Duitsland en Frankrijk)
 - 2.8. Onderzoek in een geautomatiseerd werk en rechtsmacht
 - 2.8.1. Inleiding
 - 2.8.2. Opsporingshandelingen met betrekking tot gegevens en rechtshulp
 - 2.8.3. Ontwikkelingen in het internationale recht
 - 2.8.4. Conclusie
 - 2.9. De bescherming van grondrechten
 - 2.9.1. Het recht op eerbiediging van de persoonlijke levenssfeer
 - 2.9.2. Het recht op bescherming van het brief-, telefoon- en telegraafgeheim
3. De ontoegankelijkmaking van gegevens
 - 3.1. Algemeen
 - 3.2. De noodzaak tot aanpassing van de huidige wettelijke regeling
 - 3.3. De uitvoering van een bevel tot ontoegankelijkmaking van gegevens
 - 3.4. De bescherming van grondrechten
 - 3.4.1. Het recht op vrijheid van meningsuiting
4. Het decryptiebevel aan de verdachte

- 4.1. De noodzaak en de reikwijdte van de voorgestelde bevoegdheid
- 4.2. De voorwaarden voor een decryptiebevel aan de verdachte
- 4.3. De inzet en uitvoering van een decryptiebevel aan de verdachte
- 4.4. De strafbedreiging van het opzettelijk niet voldoen aan een decryptiebevel
- 4.5. De regeling in andere landen
- 4.6. De bescherming van grondrechten
 - 4.6.1. Het beginsel van nemo tenetur
 - 4.6.2. Het recht op bescherming van de persoonlijke levenssfeer

- 5. De heling van gegevens
 - 5.1. Algemeen
 - 5.2. De voorgestelde strafbaarstellingen
 - 5.3. Wederrechtelijkheid

- 6. Financiële paragraaf

II. ARTIKELSGEWIJZE TOELICHTING

I ALGEMEEN

1. *Inleiding*

Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Het wetsvoorstel vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer alsmede van het in het regeerakkoord van dit kabinet 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 (Bruggen slaan, Regeerakkoord VVD – PvdA, 29 oktober 2012, blz. 28). Daartoe wordt voorgesteld te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen.

Het 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 bepaalde opsporingsambtenaren te creëren om 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. 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. In dit verband wordt tevens voorgesteld de omschrijving van het begrip 'geautomatiseerd werk' te verruimen. Deze bevoegdheid kan onder omstandigheden ook worden toegepast ten aanzien van een geautomatiseerd werk dat zich niet op het Nederlandse grondgebied bevindt maar waarbij de gevolgen van het strafbare feit zich in Nederland voordoen. Daarbij worden de regels van het internationale volkenrecht gerespecteerd.

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. Dit 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 een afzonderlijke wettelijke bevoegdheid te creëren tot het geven van een bevel aan een verdachte tot het toegankelijk maken van versleutelde elektronische gegevens (hierna ook te noemen: decryptiebevel). Met de wettelijke regeling van het decryptiebevel aan de verdachte wordt het juridisch instrumentarium van politie en justitie om

toegang te kunnen verkrijgen tot versleutelde gegevens aangepast aan de eisen van deze tijd in verband met de opsporing van ernstige strafbare feiten en de waarheidsvinding. Mede in het licht van de eisen van artikel 6 EVRM wordt de uitoefening beperkt tot het maken van een beroep of gewoonte van de vervaardiging, verspreiding en het bezit van kinderpornografie (artikel 240b, tweede lid, Sr) en het plegen van terroristische misdrijven (artikel 83 Sr). Het publieke belang van de bestrijding van dergelijke vormen van criminaliteit, waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van de versleuteling van elektronische gegevens, noopt tot een specifieke bevoegdheid tot het toegankelijk maken van dergelijke gegevens.

In de vierde 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 door misdrijf verkregen 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.

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

Met dit wetsvoorstel wordt aangesloten bij de snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit. Deze ontwikkelingen roepen voortdurend de vraag op of de juridische instrumenten voldoende zijn toegesneden op een effectieve bestrijding van computercriminaliteit. Met de Wet computercriminaliteit, in werking getreden op 1 maart 1993, is het Wetboek van Strafvordering aangevuld met bevoegdheden op het gebied van onderzoek van geautomatiseerde werken en zijn specifieke strafbepalingen, zoals computervredebreuk toegevoegd aan het Wetboek van Strafrecht. Met de Wet computercriminaliteit II, in werking getreden op 1 september 2006, is hieraan een vervolg gegeven en zijn het Wetboek van Strafrecht en het Wetboek van Strafvordering aangepast aan de nieuwe ontwikkelingen in de informatietechnologie. Met die wet is voorts 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.

Tijdens het Algemeen Overleg Nationale Veiligheid van 1 juni 2011 (Kamerstukken II 2010/11, 28 684, nr. 323) heb ik aan de Tweede Kamer onder meer een juridisch kader cybersecurity met een inventarisatie van de juridische knelpunten daarbinnen toegezegd. Bij brief van 23 december 2011 (Kamerstukken II 2011/12, 26 643, nr. 220) is de Tweede Kamer nader geïnformeerd over dit juridische kader. Wat betreft de strafrechtelijke opsporingsbevoegdheden wordt in deze brief beschreven dat er zowel nationaal als internationaal trajecten lopen waar gekeken wordt naar de noodzakelijkheid om wet- en regelgeving aan te passen die nodig is om ook op internet voldoende mogelijkheden te hebben voor de opsporing. De brief meldt voorts dat door het toenmalige kabinet in 2010 een aantal conceptwetsvoorstellen in consultatie is gegeven en dat de uitkomst van dit adviestraject ertoe heeft geleid dat er meer tijd nodig was om te komen tot daadwerkelijke

wetsvoorstellen. Ook zouden andere in de praktijk voorkomende onderwerpen, waaronder het online onderzoeken van gegevens, nader moeten worden verkend.

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 rechtsstatelijkheid, proportionaliteit, subsidiariteit en eerbiediging van de persoonlijke levenssfeer van burgers, 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. Dit wetsvoorstel bevat de uitwerking van de in de brief genoemde voorstellen.

Voorts wordt met dit wetsvoorstel uitvoering gegeven aan het bij brief van 27 november 2012 (Kamerstukken II 2012/13, 33 400 VI, nr. 68) aangekondigde voornemen om een afzonderlijke wettelijke bevoegdheid te creëren om een verdachte te bevelen dat hij versleutelde gegevens toegankelijk maakt.

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 het voorgestelde nieuwe artikel 125ja Sv (artikel II, onderdeel C) en de voorgestelde wijziging van artikel 80sexies Sr (artikel I, onderdeel B) en van de artikelen 125m, 125n en 125o Sv (artikel II, onderdeel E). 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 F). In hoofdstuk 4 komt de bevoegdheid tot het geven van een bevel aan de verdachte tot ontsluiting van gegevens aan de orde. Dit betreft de voorgestelde wijziging van artikel 125k Sv (artikel II, onderdeel D) en het voorgestelde nieuwe artikel 184b Sr (artikel I, onderdeel G). In hoofdstuk 5 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 de voorgestelde wijziging van artikel 139f Sr (artikel I, onderdeel E). Hoofdstuk 6 bevat de financiële paragraaf. Daarna volgt de artikelsgewijze toelichting.

2. Onderzoek in een geautomatiseerd werk

2.1 De noodzaak van de voorgestelde bevoegdheid

Dit wetsvoorstel introduceert een nieuwe bevoegdheid voor opsporingsambtenaren om, onder strikte 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 (hierna ook te noemen: onderzoek in een geautomatiseerd werk). Dit betreft de vaststelling van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker, het overnemen van gegevens, de

ontoegankelijkmaking van gegevens, het opnemen van communicatie of van vertrouwelijke communicatie en de stelselmatige observatie. 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). Ook 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. 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 gegevensbestanden. Het versleutelen van gegevensbestanden vereist steeds minder technische kennis. Het programma TrueCrypt 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 - 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. Er zijn wereldwijd inmiddels ongeveer 171 miljoen geregistreerde Skype-gebruikers. 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. De wet voorziet 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). Daaronder vallen ook aanbieders van communicatiediensten. Ondanks de mogelijkheid van een ontsleutelbevel kan de aanbieder het communicatieverkeer 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 bevel kan evenmin tot de verdachte worden gericht (artikel 125k, derde lid, Sv). Weliswaar wordt in dit wetsvoorstel ook voorgesteld om deze beperking in gevallen van verdenking van een terroristisch misdrijf of van kinderporno op te heffen en voor die gevallen te voorzien in de bevoegdheid om een verdachte te bevelen medewerking te verlenen aan het ontsleutelen van gegevens, maar een dergelijk bevel biedt geen zekerheid dat de versleutelde gegevens daadwerkelijk beschikbaar komen. Op de verhouding tussen de bevoegdheid van onderzoek in een geautomatiseerd werk en het decryptiebevel aan een verdachte wordt hieronder, in hoofdstuk 4, nader ingegaan. De opsporing heeft dringend behoefte 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.

De effectiviteit van het aftappen en opnemen van communicatie wordt ernstig verminderd door de encryptie van gegevens. Het aftappen en opnemen van communicatie kan plaatsvinden door middel van een telefoon-, e-mail-, of internettap (artikelen 126m, 126t en 126zg Sv). De inzet van deze bevoegdheid biedt echter geen resultaat in gevallen waarin gebruik wordt gemaakt van 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, Sv), maar de aanbieder is hiertoe soms zelf 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 ontsluiting van iedere laag in handen is van een aanbieder. 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 uitsluitend van belang in verband met de kosten daarvan. 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 betreden. Zoals hierboven is aangegeven, spoot dit niet

meer met de werkelijkheid in gevallen waarin smartphones en laptops worden gebruikt of de gegevens zich in de Cloud bevinden.

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.

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, 126u, 126ua, 126zh en 126zi 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 worden gedacht aan zogenaamde "bulletproof hosting providers" die hun klanten de mogelijkheid bieden om volledig anoniem, en vaak in resell constructies, illegale activiteiten te ontplooiën. 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 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. 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. Afscherming van de gegevens voor politie en justitie vormt een essentieel element 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.

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 technisch 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, 25403, 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. Daar komt bij dat het niet nodig is een woning te betreden om een technisch hulpmiddel te plaatsen, en er geen inbreuk behoeft te worden gemaakt op het grondwettelijke beschermde recht van onschendbaarheid van de woning (artikel 12 GW).

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 inblikoperatie (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 binnendringen van een geautomatiseerd werk dat bij een verdachte in gebruik is. Het binnendringen kan uitsluitend worden verricht met het oog op het verrichten van bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden. Met behulp van deze bevoegdheid kan de aanwezigheid van gegevens in het geautomatiseerde werk worden vastgesteld of kan het geautomatiseerde werk of de gebruiker worden geïdentificeerd ten behoeve van een meer gericht bevel tot het opnemen van telecommunicatie. Ook kunnen gegevens worden overgenomen 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.

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 hieronder 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, 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 computervrededreuk 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. Ook 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. 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.

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, is de voorgestelde bevoegdheid in de zevende afdeling van Titel IV ('Enige bijzondere dwangmiddelen') van het Wetboek van Strafvordering opgenomen. In de zevende afdeling is de doorzoeking ter vastlegging van gegevens geregeld. 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. De essentie 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 van Titel IV van het Wetboek van Strafvordering voor de doorzoeking ter vastlegging van gegevens.

De plaatsing in deze afdeling impliceert dat de overige in deze afdeling opgenomen regels over de uitvoering van de doorzoeking ter vastlegging van gegevens ook van toepassing zijn op het onderzoek in een geautomatiseerd werk. Dit betreft 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).

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 bedoeld op gegevens die in een computer zijn opgeslagen. Met het tweede wordt bedoeld 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 communicatiediensten 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, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden. De koppeling aan deze handelingen, maatregel en bevoegdheden houdt verband met het op afstand heimelijk binnendringen van een geautomatiseerd werk en betreft het volgende:

1. Het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker

Dit betreft de minst vergaande bevoegdheid rond het onderzoek in een geautomatiseerd werk. 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 tactisch optreden. Er is als het ware sprake van een virtuele plaatsopneming of inijkoperatie, waarbij de aanwezigheid van gegevensbestanden of van gegevens in het geautomatiseerde werk of de gegevensdrager wordt vastgesteld. 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 vaststelling van de aanwezigheid van gegevens 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.

De bevoegdheid kan tevens 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 of de daarmee in verbinding staande gegevensdrager 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 het overnemen van 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).

De vastlegging van gegevens is beperkt tot de vaststelling van de aanwezigheid van gegevens of de vastlegging van de identificerende gegevens in het belang van het onderzoek. Dit betreft de waarheidsvinding rond de desbetreffende strafbare feiten.

2. Het overnemen van gegevens

Een belangrijke bevoegdheid betreft het overnemen van gegevens, die in het geautomatiseerde werk, of in de daarmee in verbinding staande gegevensdrager, zijn of worden verwerkt. Het kan gaan om zowel gegevens die reeds op het geautomatiseerde werk zijn vastgelegd als om gegevens die gedurende de looptijd van het bevel worden verwerkt. Het gaat hierbij om opgeslagen en stromende gegevens, voor zover dit geen communicatie betreft. Zo 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. Voor het vastleggen van de gegevens kan gebruik worden gemaakt van een 'keylogger', die de toetsaanslagen op een toetsenbord vastlegt. Door middel van het vastleggen van bepaalde gegevens is het mogelijk om toegang te verkrijgen tot versleutelde gegevens. Hiermee kan worden voorkomen dat de officier van justitie zijn toevlucht moet nemen tot een decryptiebevel aan de verdachte, dat in hoofdstuk 4 wordt toegelicht.

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 aanwezig te zijn op het geautomatiseerde werk.

Het overnemen van gegevens, en daarmee ook de vastlegging, is beperkt tot de gegevens die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen. Anders dan bij het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of 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 het beramen of plegen van ernstige strafbare feiten of de vastlegging van identificerende gegevens. In de tweede plaats is de vastlegging van gegevens niet beperkt tot de gegevens die zijn verwerkt, dus tot gegevens die doorgaans zijn opgeslagen, maar kan de vastlegging ook betrekking hebben op gegevens die na het tijdstip van afgifte van het bevel worden verwerkt.

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. Hiervoor 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 toegangspoort 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). Hieruit 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 semi-autonoom 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.

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). Hiervoor kan worden verwezen naar paragraaf 3.3 van deze memorie van toelichting.

In het belang van het onderzoek kunnen gegevens worden vastgelegd. Het belang van het onderzoek betreft de beëindiging van het strafbare feit of de voorkoming van toekomstige strafbare feiten.

4. 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 af luisteren). 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').

In de eerste plaats kunnen stromende gegevens 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 is destijds een nieuw onderdeel e respectievelijk f toegevoegd, dat bepaalt dat in het bevel de aard van het technisch 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 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 technisch hulpmiddelen 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'. Deze wijze van aftappen is gebonden aan een uitgebreide voorbereiding, inclusief de voorafgaande toetsing van de voorgenomen inzet door de Centrale Toetsingscommissie van het openbaar ministerie. Daarnaast is de uitvoering van de bevoegdheid beperkt tot de door de korpschef aangewezen en ter zake deskundige opsporingsambtenaren. Ten slotte is het niet altijd mogelijk om heimelijk binnen te dringen in het geautomatiseerde werk vanwege, onder meer, de beveiliging daarvan.

In de tweede plaats kunnen stromende gegevens heimelijk worden opgenomen op grond van het eerdergenoemde bevel tot het opnemen van vertrouwelijke communicatie. Dit betreft de bevoegdheid van 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 moet worden 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.

5. De stelselmatige observatie

De voorgestelde bevoegdheid biedt de mogelijkheid om de locatie van het geautomatiseerde werk 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. Een éénmalige of incidentele locatiebepaling is bezwaarlijk aan te merken als het volgen of stelselmatig waarnemen van de aanwezigheid of het gedrag van een persoon. Bij het aftappen van communicatie worden de zogenaamde mastgegevens verkregen. Aan de hand daarvan kan worden bepaald met welke zendmast een mobiele telefoon in verbinding is geweest.

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) is zeer nauwkeurig. Dit 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. Vanwege de inbreuk op de persoonlijke levenssfeer is sprake van stelselmatige observatie, waarvoor een bevel van de officier van justitie is vereist (artikelen 126g en 126oSv).

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.

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 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). De softwareapplicatie zal moeten voldoen aan de eisen van deze algemene maatregel van bestuur. Daartoe zal het Besluit technische hulpmiddelen strafvordering worden aangepast.

In de wet is bepaald dat een technisch hulpmiddel niet op een persoon wordt bevestigd, tenzij met diens toestemming (artikelen 126g en 126o, derde lid, Sv). In de jurisprudentie is geoordeeld dat een telefoon geen heimelijk op het lichaam geplaatst hulpmiddel is in de zin van de wet. Er wordt namelijk gebruik gemaakt van een voorwerp dat de verdachte reeds voor een ander doel bij zich draagt (Rechtbank 's-Hertogenbosch, 14-06-2012, LJN: BW8619 en BW 8633). Deze jurisprudentie betreft de inzet van een technisch middel bij uitoefening van de bevoegdheid tot observatie, maar aangenomen kan worden dat dit eveneens geldt voor de inzet van een softwareapplicatie op een mobiele telefoon.

Voor een bevel tot observatie 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 de mogelijkheid van stelselmatige observatie door middel van deze bevoegdheid te binden aan een voorafgaande machtiging van de rechter-commissaris.

Anders dan bij de onderzoekshandeling van het overnemen van gegevens is deze bevoegdheid niet zozeer gericht op het overnemen en vastleggen van gegevens die in het geautomatiseerde werk worden verwerkt als wel op het bepalen van de locatie van het geautomatiseerde werk. Daarbij worden bepaalde sensoren in het geautomatiseerde werk geactiveerd. De vastlegging van gegevens in het belang van het onderzoek is beperkt tot gegevens over de plaatsbepaling van het geautomatiseerde werk (locatiegegevens).

Hierboven is een overzicht gegeven van opsporingshandelingen en opsporingsbevoegdheden die kunnen worden toegepast op basis 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).

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, betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid e.d. (artikelen 126nf, 126uf en 126zn, tweede lid, Sv).

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 of op de daarmee in verbinding staande gegevensdrager privégegevens zijn opgeslagen, worden verwerkt of overgedragen, zoals financiële administratie of vakantiefoto's. Ook 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 betreffende geautomatiseerde werk.

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. Daarnaast 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 of van de daarmee in verbinding staande gegevensdrager aan het bevel uitvoering wordt gegeven. Als het bevel betrekking heeft op de inzet van een afzonderlijke bijzondere opsporingsbevoegdheid, 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.

De inzet van de bevoegdheid van artikel 125ja Sv dient tevens te voldoen aan bepaalde procedurele eisen. Dit is van groot belang voor de waarborging van de integriteit van het opsporingsonderzoek. In de eerste plaats is het verrichten van handelingen ter uitvoering van het bevel van de officier van justitie beperkt tot de opsporingsambtenaren als bedoeld in artikel 141, onder b, en bijzondere opsporingsambtenaren als bedoeld in artikel 142, eerste lid, onder b, Sv. Het gaat om technische handelingen met betrekking tot het binnendringen van geautomatiseerde werken en het eventueel plaatsen van software waarmee gegevens kunnen worden vastgelegd. Binnen de kring van de ambtenaren van de politie zal het verrichten van de uitvoeringshandelingen zijn voorbehouden aan de opsporingsambtenaren die een speciale opleiding hebben gevolgd (hierna ook aangeduid als: het technische team). Dit betreft de door de korpschef aangewezen en ter zake deskundige opsporingsambtenaren. De aanwijzing van ter zake deskundige opsporingsambtenaren wordt de ervaring, capaciteit en technische kennis die is vereist voor een goede uitvoering van het onderzoek in een geautomatiseerd werk geconcentreerd, zodat gewaarborgd is dat de kwaliteit van de inzet van de voorgestelde bevoegdheid aan de hoogste maatstaven voldoet.

De opsporingsambtenaren van het technische team kunnen als ambtenaar van politie zijn belast met algemene opsporingsbevoegdheid (artikel 141, onderdeel b, Sv) maar vanwege de behoefte aan specifieke expertise op het gebied van informatie- en communicatietechnologie wordt de mogelijkheid geboden tot het aanwijzen van een opsporingsambtenaar die is belast met de uitvoering tot ondersteunende taken. Deze opsporingsambtenaren beschikken over buitengewone opsporingsbevoegdheid (artikel 142, eerste lid, onderdeel b, Sv). Het beleid ten aanzien van buitengewoon opsporingsambtenaren (BOA's) is neergelegd in de Circulaire Buitengewoon Opsporingsambtenaar. De beperking van de uitvoering van handelingen ter uitvoering van een bevel tot onderzoek in een geautomatiseerd werk tot de bepaald aangewezen opsporingsambtenaren wordt nader geregeld bij algemene maatregel van bestuur. Dit betreft het Besluit technische hulpmiddelen strafvordering.

De opsporingsambtenaren van het technische team, die zijn belast met het plaatsen van het technische hulpmiddel, 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 die zijn belast met de plaatsing van het technisch hulpmiddel 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 uitvoering van het onderzoek in een geautomatiseerd werk. Te allen tijde staat voorop dat de uitvoeringshandelingen op professionele wijze worden uitgevoerd, door daarvoor opgeleide specialisten.

In de tweede plaats zullen nadere eisen worden gesteld aan de software met behulp waarvan onderzoek in een geautomatiseerd werk kan worden verricht. Deze nadere eisen zullen worden uitgewerkt in een algemene maatregel van bestuur. Het Besluit technische hulpmiddelen strafvordering zal worden aangevuld met eisen voor de software die wordt gebruikt voor onderzoek 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 technische handelingen in het kader van de opsporing 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 de bevoegdheid. Dit betreft de elektronische vastlegging (logging) van gegevens over de verwerking van gegevens bij onderzoek in een geautomatiseerde werk.

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 geautomatiseerde werk daadwerkelijk wordt binnengedrongen, de fase waarin onderzoekshandelingen worden verricht of bepaalde opsporingsbevoegdheden worden toegepast en een eindfase waarin de inzet van de bevoegdheid wordt beëindigd.

Hiervoor is opgemerkt dat de voorgestelde bevoegdheid wordt uitgevoerd door de door de korpschef aangewezen opsporingsambtenaren. De concentratie brengt met zich mee dat, wanneer in regionale opsporingsonderzoeken de behoefte bestaat om de bevoegdheid tot onderzoek in een geautomatiseerd toe te passen, de advisering van de officier van justitie omtrent de afweging om in het concrete geval daadwerkelijk een onderzoek in een geautomatiseerd werk te verrichten is voorbehouden aan de daartoe aangewezen opsporingsambtenaren.

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 inijkoperatie (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 het technische hulpmiddel onopvallend kan worden geplaatst) en welk besturingsprogramma van toepassing is. 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 verdachte 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 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.

Voorts is het voor een succesvolle inzet van belang te weten welke programma's zijn geïnstalleerd op het desbetreffende geautomatiseerde werk. Hoe de logische opbouw van het systeem is vorm gegeven, zodat het technisch hulpmiddel onopvallend kan worden geplaatst, en welk besturingssysteem wordt gebruikt. Ook kan aan de hand van dit soort informatie een globale inschatting worden gemaakt van de barrières voor het onderzoek in het geautomatiseerde werk, in het bijzonder op het gebied van de beveiliging.

Er zijn verschillende technieken beschikbaar die 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. De technieken voor het binnendringen kunnen worden onderscheiden in zogenaamde "low end" en "high end" methodes, afhankelijk van de complexiteit van het desbetreffende geautomatiseerde werk. Een voor de hand liggende methode is het via internet zenden van een elektronisch bericht aan de betrokkene, met als doel de betrokkene ertoe te brengen de software te installeren die het geautomatiseerde werk opent voor de plaatsing van een "bug" of "keylogger" met behulp waarvan gegevens kunnen worden vastgelegd. Hierbij moet rekening worden gehouden met de beveiliging van de computer. In het geval dat het beveiligingssysteem van de computer de software herkent en de toegang weigert zal

de software aangepast moeten worden. Een andere methode betreft het binnendringen van een geautomatiseerd werk door middel van een gebruikersnaam en wachtwoord, die door middel van het tappen van communicatie of door "social engineering" van de verdachte of iemand in zijn nabije omgeving zijn verkregen. Deze techniek houdt in dat belangrijke gegevens, zoals wachtwoorden of pincodes, door middel van misleiding worden verkregen van de verstrekker. Niet uitgesloten is dat een geautomatiseerd zodanig is beveiligd dat het niet lukt om binnen te dringen. Dan resteert de toepassing van andere opsporingsbevoegdheden dan wel de beëindiging of onderbreking van het opsporingsonderzoek.

Op basis van de 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 bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking of het inzetten van bepaalde afzonderlijke 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 (CTC) en het verkrijgen van een schriftelijke machtiging van de rechter-commissaris, komt elders aan de orde.

II Het binnendringen en verrichten van 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.

Zodra in het geautomatiseerde werk is binnengedrongen kunnen bepaalde onderzoekshandelingen worden verricht, gegevens ontoegankelijk worden gemaakt of bepaalde afzonderlijke bijzondere opsporingsbevoegdheden worden toegepast. Hierbij moet gebruik worden gemaakt van een technisch hulpmiddel, zoals de hierboven genoemde "bug" of "keylogger". Doorgaans zal het gaan om een softwareapplicatie. De software die in deze fase wordt gebruikt kan verschillende functionaliteiten hebben waarmee de in het voorgestelde artikel 125ja, 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.

Het technische hulpmiddel moet zijn goedgekeurd en moet voldoen aan de normen het Besluit technische hulpmiddelen strafvordering, dat in verband met de voorgestelde bevoegdheid wordt aangepast. Het technische hulpmiddel wordt specifiek geprepareerd voor de inzet in het concrete geval en moet onder meer een functie bevatten die het functioneren van het technische hulpmiddel tijdens de inzet ervan technisch vastlegt, ook wel "logging" genoemd. Ook moet het technische hulpmiddel een zekere mate van voorspelbaarheid vertonen en moeten de authenticiteit en integriteit van de gegevens die door middel van het technische hulpmiddel worden vergaard, zijn gewaarborgd.

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 in deze fase controleerbaar.

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 geïnstalleerde technische hulpmiddel verwijderd door het technische team. De ambtenaren die betrokken zijn bij het tactische opsporingsonderzoek kunnen geen invloed uitoefenen op de verwijdering van het technische hulpmiddel. Na het verwijderen van het technische hulpmiddel zal de server aan de zijde van de politie geen gegevens meer kunnen ontvangen. Nadat het technisch hulpmiddel is verwijderd, kunnen 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, voordat het onderzoek in het geautomatiseerde werk plaatsvond.

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.

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. Op deze manier is het mogelijk om de ter terechtzitting gevoerde verweren over de integriteit van het verzamelde bewijsmateriaal te toetsen.

Van het beëindigen van de inzet van de bevoegdheid wordt door het technische team alsmede door de opsporingsambtenaren die betrokken zijn bij het operationele onderzoek proces-verbaal opgemaakt.

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 openbaar ministerie en de politie en is een intern adviesorgaan van het openbaar ministerie. De CTC adviseert het College van procureurs-generaal (hierna ook te noemen: het College) over de voorgenomen inzet van een aantal bijzondere opsporingsbevoegdheden. 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 afbreukrisico 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 openbaar ministerie en kan door het College worden voorgeschreven. In de Aanwijzing opsporingsbevoegdheden van het College van procureurs-generaal van 1 juni 2012 (registratienummer 2012AO12) 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. Het onderzoek is uitsluitend toegestaan met het oog op het verrichten van bepaalde onderzoekshandelingen, de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden met betrekking tot het geautomatiseerde werk. In de vordering dient te worden vermeld voor welk doel de bevoegdheid in een concreet opsporingsonderzoek wordt ingezet. Daarnaast moeten 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. 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 handelingen of bevoegdheden worden ingezet. 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 opsporingshandelingen zal aan een aantal eisen moeten worden voldaan. In de eerste plaats moet gegarandeerd zijn dat de authenticiteit en integriteit van de gegevens is gewaarborgd. Dit is mogelijk door de logging op een bepaalde wijze vorm te geven. Zoals hierboven in paragraaf 2.5 reeds is opgemerkt, zal daarvoor worden aangesloten bij reeds bestaande werkwijzen, gebaseerd op het Besluit technische hulpmiddelen strafvordering. In de tweede plaats moet een meer volledige logging plaatsvinden van de onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van de afzonderlijke opsporingsbevoegdheden met betrekking tot het geautomatiseerde werk. 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 rechterlijke macht over voldoende kennis beschikt op het gebied van de informatie- en communicatietechnologie. Op dit moment worden door het Studiecentrum Rechtspleging (SSR)

specifieke cursussen verzorgd voor het openbaar ministerie en de zittende magistratuur over de aanpak van computercriminaliteit en het aanwenden van dwangmiddelen in dit verband. De cursussen zullen worden bijgesteld naar aanleiding van de voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk. Daarnaast is er binnen het landelijk parket van het openbaar ministerie kennis, expertise en landelijke sturing georganiseerd, specifiek voor de aanpak van high tech crime. Binnen de rechtspraak is bij het Gerechtshof te 's-Gravenhage een kenniscentrum cybercrime opgericht. Met het SSR en de beide kenniscentra zal worden overlegd over de uitwerking van de opleidingen en begeleiding.

Aan de betrokkene dient, zodra het belang van het onderzoek dat toelaat, mededeling te worden gedaan van het onderzoek in het geautomatiseerde werk. Daarbij dient tevens mededeling te worden gedaan van de vastlegging of ontoegankelijkmaking van gegevens (artikel 125m Sv) of van het opnemen van communicatie of van vertrouwelijke communicatie (artikel 126bb Sv). 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.

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 overheidssdiensten 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 overheidssdiensten 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.

De Belgische regeling maakt het uitdrukkelijk mogelijk om de tijdens de zoeking aangetroffen gegevens, wanneer blijkt dat zij zich niet op Belgisch grondgebied bevinden, te kopiëren. De gegevens kunnen in dat geval niet ontoegankelijk worden gemaakt. Alleen de onderzoeksrechter is bevoegd om te besluiten hiertoe over te gaan. De Belgische wetgever heeft besloten de extraterritoriale netwerkzoeking alsnog toe te laten, omdat met het instellen van internationale rogatoire commissies voor het zoeken buiten de landsgrenzen veel kostbare tijd verloren dreigde te gaan. Deze vereenvoudigde procedure kan volgens het Belgische College van Procureurs-generaal enkel worden gevolgd wanneer de buitenlandse gegevens op een toevallige of onopzettelijke manier zijn aangetroffen of in het bekende geval van de "hot pursuit", namelijk in spoedeisende gevallen om de teloorgang van het bewijsmateriaal te voorkomen. Ook kan de procedure worden toegepast wanneer de opsporingsdiensten er redelijkerwijs niet in slagen om de betrokken staat te identificeren. Buiten deze gevallen moet volgens de Belgische regeling alsnog de klassieke internationaalrechtelijke regelgeving worden gevolgd (T. Incalza, 'Strafonderzoek in het digitale tijdperk: zoeking en inbeslagneming', uit: Jura Falconis Jg. 47, 2010/11, nummer 2, blz. 378).]

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. Deze verwijdering moet worden vastgelegd.

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 dat niets te maken heeft met de strafbare feiten als omschreven in de machtiging voor de maatregel mag in het onderzoeksdossier worden bewaard. Ten slotte bevat de Franse regeling de verplichting om de vastleggingen van de elektronische gegevens na het verstrijken van de verjaringstermijn te vernietigen.

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. Voor politie en justitie is het lastig om gegevens te achterhalen die door middel van computers worden verwerkt. 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 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.

Centrale grondslag voor 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 (artikel 5, eerste lid, 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 benadeeld, is dat zij zich vaak gedeeltelijk in Nederland voordoen. 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 02-02-2010, 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 (het verspreiden van kinderpornografie) als de slachtoffers (phishing door Nigeriaanse bendes). In de gevallen waarin kan worden aangenomen dat Nederland op grond van de artikelen 2 tot en met 8 Sr over

rechtsmacht beschikt, geldt dat er krachtens artikel 539a Sv een bevoegdheid is om opsporingshandelingen te verrichten. Op grond van dit artikel kan worden opgetreden buiten het rechtsgebied van een rechtbank, binnen de grenzen van het volkenrecht en het internationale recht.

Bij het toepassen van dwangmaatregelen jegens personen (arrestatie voor verhoor, in verzekeringstelling, huiszoeking e.d.) 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 feitelijk niet mogelijk zonder hulp van de staat waar de dader zich bevindt of waar uitvoeringshandelingen hebben plaatsgevonden. In een dergelijk geval is rechtshulp aan de orde. 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. Een rechtshulpverzoek heeft betrekking op het respecteren van 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.

2.8.2 Opsporingshandelingen met betrekking tot gegevens en rechtshulp

Vanwege de dikwijls ruime regelingen van 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. De botnets vormen hiervan een goed voorbeeld. De schadelijke gevolgen van het gebruik van dergelijke botnets kunnen zich in een groot aantal staten manifesteren.

Voor opsporingshandelingen in cyberspace met betrekking tot gegevens geldt in veel gevallen dat de feitelijke locatie van gegevens redelijkerwijs niet is te achterhalen. Dit komt in het bijzonder veelvuldig voor vrijwel alle gegevens die op de Cloud worden opgeslagen of bewaard. Zoals in paragraaf 2.1 aan de orde is gekomen, is de feitelijke locatie van de gegevens ook voor de dienstenaanbieder niet altijd bekend. Dit geldt ook voor gegevens die via het Tor-netwerk worden gerouteerd en voor gegevens 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. Het is dan niet mogelijk om bij een onderzoek in een geautomatiseerd werk in overleg te treden met een belanghebbende staat. In een dergelijk geval kunnen de gegevens die in het kader van het onderzoek zijn aangetroffen, worden vastgelegd of ontoegankelijk gemaakt, ongeacht de locatie waar de gegevens zich bevinden.

Ook in het geval er bij de politie wel wetenschap bestaat van de feitelijke locatie van gegevens, kan – binnen de grenzen van artikel 539a Sv en onder de voorwaarde van (extra) territoriale

rechtsmacht - zelfstandig worden opgetreden. Het zal sterk van de aard van de feitelijke handeling afhangen onder welke omstandigheden het volkenrecht zich verzet tegen zelfstandig optreden van de handhavende staat. Ook andere staten zien, gelet op hun wetgeving, meer ruimte voor zelfstandig optreden als het gaat om opsporingshandelingen met betrekking tot gegevens.

2.8.3 Ontwikkelingen in het internationale recht

Het Cybercrime Verdrag van de Raad van Europa bevat een specifieke regeling voor de grensoverschrijdende toegang tot computergegevens. Het Cybercrime Verdrag is ondertekend door de leden van de Raad van Europa. Naast de EU-lidstaten hebben ook Japan en de Verenigde Staten het verdrag ondertekend. Ook in dit verdrag wordt ervan uitgegaan dat de verdragspartijen nader over leg 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 betreft niet uitsluitend de verdachte of een andere individuele persoon, het kan ook de aanbieder zijn van een dienst. De aangezochte persoon dient zich op het grondgebied van de verzoekende partij te bevinden (Discussion paper 'Cloud Computing and cybercrime investigations: territoriality vs. the power of disposal?', Version 31 August 2010). De verdragspartijen konden 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. Nadeel van deze rechtshulpvoorschriften is dat de opsporingsdiensten in het aangezochte land hun eigen prioriteiten hebben. Dit veroorzaakt afhankelijkheid en vertraging in een onderzoek waardoor informatie verloren gaat of onnodig schade wordt aangericht (Criminaliteitsbeeldanalyse High Tech Crime, blz. 143).

Vanwege de beperkingen van de regeling van het Cybercrimeverdrag wordt in de Raad van Europa verder gesproken over de verhouding tussen het grensoverschrijdend vastleggen van gegevens en de 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". Een Begeleidende Notitie ('Guidance Note') over artikel 32 van het Cybercrime Verdrag kan daaraan bijdragen. Hiermee kan op korte termijn duidelijkheid worden geboden over de ruimte van bestaande bevoegdheden die op grond van het Cybercrime Verdrag kunnen worden uitgeoefend.

Voorts wordt geconcludeerd dat 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. Met een Aanvullend Protocol ('Additional Protocol') bij het Cybercrime Verdrag kan 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. Deze maatregelen zouden in het Aanvullend Protocol bij het Cybercrime Verdrag vastgelegd kunnen worden.

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. Daarnaast 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. Reeds hieruit vloeit voort dat enige voorzichtigheid past bij het zelfstandig optreden ter handhaving. Aangenomen wordt dat bevoegdheden als de ontoegankelijkmaking of het veiligstellen van gegevens tot de eigen territoriale beschikkingsmacht behoort voor zover de Nederlandse strafwet toepasselijk is op het strafbare feit dat wordt opgespoord. De noodzaak tot onverwijld optreden maakt dit onvermijdelijk en ook volkenrechtelijk goed verdedigbaar. Dit betekent dat wanneer de plaats van opslag van de gegevens niet bekend is, zelfstandig kan worden opgetreden. Maar het betekent ook dat als de plaats van opslag wel bekend is, zelfstandig optreden van de belanghebbende staat niet bij voorbaat is uitgesloten.

2.9 De bescherming van grondrechten

De voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk 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 van deze toelichting 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 vergaande 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 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 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. Hierbij heeft de staat een zekere ruimte voor beoordeling ('margin of appreciation'). 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 of in een daarmee in verbinding staande gegevensdrager met het oog op de in het voorgestelde artikel 125ja, 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 of in de daarmee in verbinding staande gegevensdrager 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 125ja, eerste lid, Sv omschreven doelen. Deze doelen zijn limitatief omschreven. Dit betreft het

verrichten van bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het toepassen van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden, 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, de maatregel van de ontoegankelijkmaking van gegevens en de inzet van de afzonderlijke bijzondere opsporingsbevoegdheden. Deze handelingen, maatregel en bevoegdheden zijn limitatief omschreven.

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. 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 van deze toelichting. 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 subsidiariteitsvereiste.

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 125ja Sv wordt aan deze eis voldaan. Artikel 125ja, eerste lid, Sv vormt de grondslag voor het verrichten van onderzoek in een geautomatiseerd werk. De doelen waarvoor de bevoegdheid kan worden toegepast zijn limitatief omschreven in het voorgestelde artikel 125ja, eerste lid, Sv.

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 125ja 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 de inzet van het technische hulpmiddel en de opsporingsambtenaren die betrokken zijn bij het operationele opsporingsonderzoek. 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 verzonden. Dit kan aan de orde zijn bij het vaststellen van de aanwezigheid van gegevens, het overnemen van gegevens die in het geautomatiseerde werk zijn of worden verwerkt 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 van 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 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 125ja Sv, worden aangetroffen. Dit is geregeld in artikel 125o 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 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 wetsystematisch 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 wetsystematisch 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. De daartoe strekkende bijstellingen worden artikelsgewijs toegelicht.

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 strafvervolgning, 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.

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 tussenkomsst van de rechter-commissaris wordt hieraan voldaan.

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 geveerd 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 verstreckende consequenties van een bevel tot de 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 het ontoegankelijk maken 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 artikel 125o, eerste 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 openbaar ministerie 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

3.4.1 Het recht op vrijheid van meningsuiting

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 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 officier van justitie degene tot wie de vordering is gericht, in de gelegenheid stelt om te worden gehoord.

4. *Het decryptiebevel aan de verdachte*

4.1 De noodzaak en de reikwijdte van de voorgestelde bevoegdheid

De opsporing van computercriminaliteit wordt belemmerd doordat gebruik wordt gemaakt van encryptie. Door gegevens te versleutelen kan worden voorkomen dat derden, die niet beschikken over een elektronische sleutel, kennis nemen van de inhoud van de gegevens. De stand der techniek maakt het gebruik van encryptie minder ingewikkeld voor de gebruiker. De sleutellengtes nemen toe, waardoor het steeds lastiger wordt om encryptie te kraken. Een sleutellengte van 256 bits is op dit moment met de beschikbare rekencapaciteit vrijwel niet te kraken. Er zijn cryptografieprogramma's op de markt die specifiek zijn gericht op het ondermijnen van het forensisch onderzoek. Dit zijn zogenaamde open source-programma's die de mogelijkheid bieden gegevens in een container op te slaan. Dit is onder andere het geval bij het eerdergenoemde programma TrueCrypt. De container kan andere containers bevatten, die op zodanige wijze zijn opgeslagen dat de aanwezigheid van die containers, evenals de daarin opgenomen gegevens, niet goed vast te stellen zijn voor personen die onderzoek verrichten naar de inhoud van de container. Dit houdt verband met het gebruik van zogenaamde willekeurige bits, waardoor het voor een forensisch onderzoeker moeilijk is om met voldoende zekerheid onderscheid te maken tussen delen van de harde schijf die versleuteld zijn en delen die leeg zijn. Door de bestanden te ontsleutelen kan meer zekerheid worden verkregen over de aanwezigheid van andere containers.

Het gebruik van encryptie komt voornamelijk voor binnen bepaalde netwerken van kinderpornogebruikers en -verspreiders. Dit is in het kader van de Rotterdamse proeftuin kinderpornografie aan de orde gekomen. Ook het opsporingsonderzoek in de Amsterdamse zedenzaak bleek dat de verdachte Robert M. grote hoeveelheden kinderpornografie in versleutelde vorm op zijn computer had opgeslagen.

Met de Wet computercriminaliteit is de bevoegdheid opgenomen tot doorzoeking ter vastlegging van gegevens (art. 125i Sv). Ingeval van een doorzoeking kan aan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de beveiliging van een geautomatiseerd werk, een bevel worden gericht tot het verschaffen van toegang tot de aanwezige geautomatiseerde werken of delen daarvan (artikel 125k, eerste lid Sv). Een soortgelijk bevel kan worden gegeven indien in een geautomatiseerd werk versleutelde gegevens worden aangetroffen (artikel 125k, tweede lid, Sv). Een dergelijk bevel kan echter niet aan de verdachte worden gericht (artikel 125k, derde lid, Sv).

In het ontwerp van het toenmalige wetsvoorstel Computercriminaliteit was de mogelijkheid opgenomen om een bevel tot medewerking aan de ontsleuteling van gegevens ook aan de verdachte te richten. Naar aanleiding van de adviezen was de toenmalige minister van Justitie van oordeel dat het verplichten van de verdachte tot medewerking aan ontsleuteling een stap te ver ging. Bij de meeste encryptieprogramma's zal dit namelijk neerkomen op het verplicht vertellen van een slechts in het geheugen van de verdachte opgeslagen code of wachtwoord. Hiermee zijn de verklaringsvrijheid en het zwijgrecht van de verdachte in het geding. Daarom is toen bepaald dat het bevel tot medewerking niet aan de verdachte wordt gegeven (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 26).

Inmiddels zijn er echter nieuwe redenen om te komen tot een andere afweging ter zake. Alvorens tot het in voorbereiding nemen van het hier toegelichte onderdeel van het wetsvoorstel te besluiten, is nader onderzoek verricht naar de verenigbaarheid van een decryptiebevel aan verdachten met het in artikel 6 van het EVRM vervatte beginsel van nemo-tenetur. Het beginsel van nemo tenetur betekent dat een persoon niet kan worden gedwongen mee te werken aan zijn eigen veroordeling. Aan het Tilburg Institute for Law, Technology and Society van de Universiteit van Tilburg (TILT) is opdracht gegeven een nader onderzoek te verrichten (In de brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 27 november 2012 wordt abusievelijk gesproken van het Centrum voor Recht, Technologie en Veiligheid. Dit moet zijn: het Centrum voor Recht, Technologie en Samenleving; Kamerstukken II 2012/13, 33 400 VI, nr. 68, blz. 2). Inmiddels is het onderzoek van het TILT afgerond en is het rapport, getiteld 'Decryptiebevel en artikel 6 EVRM', aan de Tweede Kamer aangeboden. In de brief van 27 november 2012 is tevens een reactie gegeven op de bevindingen van het onderzoek. In het TILT-rapport worden verschillende opties voor een ontsleutelplicht onderzocht. De eerste optie (optie A) betreft een decryptieregeling conform de regeling van het verhoor in het Wetboek van Strafvordering. Dit betekent dat artikel 125k, derde lid, van het Wetboek van Strafvordering wordt gewijzigd zodat een bevel tot het ontsleutelen van gegevens aan een verdachte kan worden gegeven. Vanwege het zwijgrecht van de verdachte – dat in artikel 29 van het Wetboek van Strafvordering is vastgelegd – is een verdachte niet gehouden aan een dergelijk bevel medewerking te verlenen. Het bevel heeft materieel dus de betekenis van een formeel verzoek. De tweede optie (optie B) betreft een decryptiebevel met bewijsuitsluiting. Hierbij kan onderscheid worden gemaakt tussen een verzoek en een bevel tot het ontsleutelen van gegevens. De mogelijkheid van een verzoek vereist geen wettelijke regeling; de officier van justitie kan toezeggen de resultaten van de medewerking van de verdachte niet als bewijs tegen hem te zullen gebruiken. De bevoegdheid tot het geven van een bevel vereist echter een wettelijke regeling, conform optie A. Desgewenst kan de niet-nakoming van een bevel strafbaar worden gesteld. Gemeenschappelijk kenmerk van deze beide varianten is dat er gering risico bestaat voor inbreuk op het beginsel van nemo tenetur, omdat er geen sprake is van zelfbelasting. De derde optie (optie C) betreft een decryptiebevel met strafbaarstelling van weigering. Dit betekent dat aan de verdachte een bevel kan worden gegeven tot het ontsleutelen van gegevens. Als de verdachte medewerking weigert, kunnen aan een dergelijke weigering verschillende consequenties worden verbonden zoals strafbaarstelling van weigering, het verbinden van belastende gevolgtrekkingen aan weigering bij de waardering van de bewijsmiddelen of bij de straftoemeting of de opnemingsgrond van een expliciete strafverhogingsgrond voor het betreffende gronddelict in het Wetboek van Strafrecht.

In de eerdergenoemde brief is aangegeven dat het voor een adequate bestrijding van zeer ernstige vormen van criminaliteit waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van de encryptie van elektronische gegevens, zoals het bezit en de handel in kinderpornografie, van groot belang is dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens. De toegang tot de ontsleutelde gegevens is essentieel om de strafbare feiten te beëindigen en de daders aan te houden. Dit is ook in het belang van de veelal minderjarige slachtoffers. Met behulp van de beelden

kan het openbaar ministerie in contact komen met de ouders of verzorgers van de slachtoffers en informatie en voorlichting verschaffen over de gepleegde strafbare feiten en over de mogelijkheden op het gebied van hulpverlening.

Een zwaarwegend bezwaar van optie A is dat de medewerking van de verdachte niet afdwingbaar is. Dit zal de effectiviteit van de regeling ernstig kunnen aantasten. Een ontsleutelverzoek zal waarschijnlijk niet werken bij berekenende criminelen die geen medewerking willen verlenen. Juist bij verdachten van het bezit en de handel in kinderpornografie zal dit aan de orde kunnen zijn. Bij het decryptiebevel met bewijsuitsluiting (optie B) wordt een verdachte niet gedwongen zichzelf te belasten omdat er sprake is van een verzoek om op vrijwillige basis mee te werken. Om het bevel afdwingbaar te doen zijn is strafbaarstelling van de niet-nakoming vereist. Daarmee is eenzelfde afweging aan de orde als bij een decryptiebevel met strafbaarstelling, namelijk de aard en hoogte van de strafbedreiging. Bovendien past een systeem waarbij een verdachte immuniteit voor strafvervolging verkrijgt door medewerking te verlenen aan het opsporingsonderzoek niet goed in het Nederlandse stelsel van strafvordering. Mijn voorkeur gaat dan ook uit naar opnemingsrecht in het Wetboek van Strafvordering van een bevoegdheid tot het geven van een bevel aan een verdachte tot het verschaffen van toegang tot versleutelde elektronische gegevens en het toegankelijk maken van die gegevens. Een zelfstandige strafbaarstelling van het, in geval van verdenking van bepaalde zeer ernstige strafbare feiten, opzettelijk niet voldoen aan een bevoegd gegeven bevel tot het toegankelijk maken van versleutelde gegevens is nodig om het bevel effectief te doen zijn. Een persoon die de nodige inspanningen heeft verricht om zijn strafbare gedragingen te verhullen moet rekening houden met de inzet van zwaardere middelen om de waarheid aan de dag te brengen.

De bevoegdheid tot het geven van een decryptiebevel aan een verdachte is wenselijk in alle zaken waarin verdachten van misdrijven die worden gepleegd met behulp van een geautomatiseerd werk - beter bekend als computercriminaliteit - gebruik maken van cryptografie om computergegevens te versleutelen. Vanwege het ingrijpende karakter van de voorgestelde bevoegdheid en de ernst van de feiten is gekozen voor een beperking van de toepassing tot het maken van een beroep of gewoonte van het bezit, de vervaardiging of de verspreiding van kinderpornografie (artikel 240b, tweede lid, Sr) en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens (artikel 138d Sv). Het publieke belang van de bestrijding van dergelijke vormen van criminaliteit, waarmee de geestelijke gezondheid en de lichamelijke integriteit van slachtoffers ernstig kunnen worden aangetast en waarbij gebruik wordt gemaakt van encryptie van elektronische gegevens, noopt tot een specifieke bevoegdheid tot het toegankelijk maken van dergelijke gegevens. Voor een adequate bestrijding van deze strafbare feiten is het van groot belang dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens.

De bevoegdheid is beperkt tot elektronische gegevens. Dit betekent dat aan een verdachte geen bevel kan worden gericht tot het overhandigen van een sleutel van een niet-virtuele kluis, waarin zich gegevens kunnen bevinden die van groot belang kunnen zijn voor het opsporingsonderzoek naar de bovenbedoelde misdrijven. Een niet-virtuele kluis is met behulp van geschikte hulpmiddelen binnen een redelijke termijn te openen. De afweging van belangen is dan een andere.

In vergelijking met de eerdergenoemde bevoegdheid tot het doen ontsleutelen van gegevens, op grond van artikel 125k Sv, is de medewerking van de verdachte niet bij voorbaat beperkt tot het ter beschikking stellen van kennis omtrent de beveiliging. De medewerking kan ook bestaan in het daadwerkelijk verschaffen van toegang tot de versleutelde gegevens. De verplichting tot ontsleuteling heeft betrekking op versleutelde gegevens, die onderdeel kunnen vormen van een gegevensbestand dat op een geautomatiseerd werk of een gegevensdrager is opgeslagen. Dit betreft een vereenvoudiging van de bestaande bevoegdheid, waarbij onderscheid wordt gemaakt tussen een geautomatiseerd werk of delen daarvan (artikel 125k, eerste lid, Sv) en versleutelde gegevens (artikel 125k, tweede lid, Sv). In vergelijking met de bestaande bevoegdheid zullen enkele belangrijke beperkingen gelden. Dit betreft in de eerste plaats de strafbare feiten, met het oog op de opsporing waarvan het bevel kan worden gegeven. Dit betreft in de tweede plaats de functionaris die het bevel kan geven. Dit betreft in de derde plaats de nadere voorwaarden aan het geven van een decryptiebevel aan de verdachte. Dit wordt hieronder nader toegelicht.

4.2 De voorwaarden voor het geven van een decryptiebevel aan de verdachte

Een decryptiebevel kan uitsluitend worden gegeven bij verdenking van het maken van een beroep of gewoonte van het bezit, de vervaardiging of de verspreiding van kinderpornografie en bij verdenking van het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens. Hierboven is reeds aangegeven dat het publieke belang van de bestrijding van dergelijke vormen van criminaliteit noopt tot een specifieke bevoegdheid tot het toegankelijk maken van dergelijke gegevens.

Een decryptiebevel aan de verdachte kan uitsluitend worden gegeven door de officier van justitie; een opsporingsambtenaar is daartoe niet zelfstandig bevoegd. De officier van justitie is bij uitstek in staat om het belang van het opsporingsonderzoek af te wegen tegen het belang van de verdachte om gebruik te kunnen maken van zijn zwijgrecht en geen medewerking te hoeven verlenen aan zijn eigen veroordeling. Het decryptiebevel kan uitsluitend worden gegeven als het belang van het opsporingsonderzoek dat dringend vordert. Met deze voorwaarde worden de vereisten van proportionaliteit en subsidiariteit uitdrukkelijk in de wet vastgelegd. De bevoegdheid mag uitsluitend worden ingezet als niet met behulp van lichtere bevoegdheden eenzelfde resultaat kan worden bereikt. Omdat deze eis uitdrukkelijk wordt gesteld dient in het decryptiebevel te worden gemotiveerd dat aan deze eis is voldaan. Het bevel dient op schrift te worden gesteld, zodat verantwoording kan worden afgelegd over de feiten en omstandigheden die aanleiding hebben gevormd voor het geven van het bevel. Het bevel zal uitsluitend kunnen worden gegeven na schriftelijke machtiging van de rechter-commissaris. Daardoor is rechterlijke controle gewaarborgd voordat de bevoegdheid wordt ingezet. De toetsing betreft de wettelijke voorwaarden, de noodzaak van het bevel, de ongeschreven beginselen van een behoorlijke procesorde, waaronder de beginselen van proportionaliteit en subsidiariteit, en de overige voorwaarden rond het bevel, zoals de termijn voor de uitvoering en de wijze van uitvoering door de verdachte.

In het licht van de proportionaliteit en de subsidiariteit is de verhouding tussen het decryptiebevel aan de verdachte en de bevoegdheden van doorzoeking ter vastlegging van gegevens en – in het bijzonder - van onderzoek in een geautomatiseerd werk van belang. Deze bevoegdheden kunnen ook worden ingezet om elektronische sleutels of wachtwoorden van versleutelde gegevensbestanden te achterhalen. De verdenking van de ernstige strafbare feiten, in geval waarvan een decryptiebevel aan de verdachte kan worden gegeven, kan ook reden vormen voor de doorzoeking ter vastlegging van gegevens of een onderzoek in een geautomatiseerd werk. Doorgaans zal de officier van justitie de voorkeur geven aan de bevoegdheden van doorzoeking en onderzoek in een geautomatiseerd werk omdat dit de meeste kans biedt op het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing. Daar komt bij dat een verdachte, als aan hem een decryptiebevel wordt gericht, op de hoogte komt van het opsporingsonderzoek. Dit is doorgaans niet wenselijk, omdat de verdachte maatregelen kan treffen om het onderzoek te frustreren. In het geval van versleuteling van elektronische gegevens verdient het in zijn algemeenheid dan ook de voorkeur om te kiezen voor een onderzoek in een geautomatiseerd werk om de gegevens vast te leggen waarmee te versleuteling ongedaan gemaakt kan worden. Het is echter bepaald niet uitgesloten dat onderzoek in een geautomatiseerd werk niet tot het gewenste resultaat leidt, vanwege de beveiliging het werk of omdat de desbetreffende gegevens niet aangetroffen worden. In een dergelijk geval kan een decryptiebevel aan de verdachte uitkomst bieden. In het decryptiebevel zal de officier van justitie de feiten en omstandigheden moeten opnemen waaruit blijkt dat de wettelijke voorwaarden voor een dergelijk bevel zijn vervuld. Dit omvat de beslissing over de inzet van een doorzoeking ter vastlegging van gegevens of een onderzoek in een geautomatiseerd werk, de daarbij gemaakte afwegingen en – indien een dergelijke bevoegdheid is ingezet - het resultaat van die inzet.

De officier van justitie geeft het bevel niet dan nadat de verdachte in de gelegenheid is gesteld te worden gehoord. De verdachte is bevoegd zich bij het horen door een raadsman te doen bijstaan. Het ligt in de rede dat de officier van justitie bij de rechter-commissaris een machtiging vordert voor een decryptiebevel aan de verdachte, eerst nadat tijdens het horen is vastgesteld dat de verdachte volhardt in de weigering medewerking te verlenen aan het ontsleutelen van de gegevens.

4.3 De inzet en uitvoering van een decryptiebevel aan de verdachte

Een decryptiebevel aan de verdachte moet in schriftelijke vorm worden gedaan, ten behoeve van duidelijkheid over de aard en inhoud van de vordering. Dit is van belang voor de verdachte, zodat hij kan begrijpen wat er precies van hem wordt verwacht. In het bevel moeten een aantal gegevens worden vermeld, waaronder de feiten en omstandigheden waaruit blijkt dat de wettelijke voorwaarden voor het decryptiebevel zijn vervuld. De opneming van de nadere gegevens in het decryptiebevel heeft mede ten doel om de rechter-commissaris in staat te stellen het bevel te toetsen. Door de officier van justitie dient te worden vastgesteld dat het onderzoek niet op een andere, minder ingrijpende wijze, kan plaatsvinden. Hij dient van deze afweging in het decryptiebevel expliciet verantwoording af te leggen. Tevens dienen de versleutelde gegevens te worden vermeld waarop het bevel betrekking heeft. Dit zal doorgaans de elektronische sleutel

betreffen met behulp waarvan toegang kan worden verkregen tot de versleutelde gegevens. Voorts moet een termijn worden opgenomen waarbinnen uitvoering moet worden gegeven aan het bevel. Er moet aan de verdachte een redelijke termijn worden gegeven om aan het decryptiebevel te voldoen, waarbij rekening wordt gehouden met enerzijds de omstandigheden van de slachtoffers en anderzijds de aard en omvang van de te ontsleutelen gegevens. Als er aanwijzingen zijn dat het voortduren van de strafbare situatie risico's oplevert voor de geestelijke gezondheid of de lichamelijke integriteit van slachtoffers, dan ligt een kortere termijn in de rede. Dit zal echter ook afgewogen dienen te worden in relatie tot de aard en de hoeveelheid gegevens die moeten worden ontsleuteld. Tenslotte dient de wijze waarop door de verdachte aan het bevel uitvoering moet worden gegeven te worden opgenomen. De medewerking van de verdachte kan bestaan uit het ter beschikking stellen van de benodigde kennis omtrent de beveiliging. Alsdan kan hij de elektronische sleutels mondeling of schriftelijk ter beschikking stellen aan de officier van justitie, zodat opsporingsambtenaren daadwerkelijk toegang kunnen verkrijgen tot de versleutelde gegevens. De medewerking kan ook bestaan in het daadwerkelijk verschaffen van toegang tot de versleutelde gegevens door de verdachte. Alsdan kan hij de elektronische sleutel zelf invoeren, zodat opsporingsambtenaren daadwerkelijk toegang kunnen verkrijgen tot de versleutelde gegevens.

Van de uitvoering van het decryptiebevel dient door de officier van justitie proces-verbaal te worden opgemaakt (artikel 152 Sv). Als de verdachte gevolg geeft aan het decryptiebevel, dan wordt de inhoud van de ontsleutelde gegevens vermeld. Als de verdachte geen gevolg geeft aan het decryptiebevel, dan wordt de verklaring van de verdachte opgenomen, inclusief de reden van het niet voldoen aan het bevel.

Op grond van de regeling van het beklag, in artikel 552a Sv, kunnen de belanghebbenden zich beklagen over het bevel medewerking te verlenen aan het ontsleutelen van gegevens. Voorgesteld wordt dat de belanghebbenden zich ook kunnen beklagen over een decryptiebevel aan de verdachte; een dergelijk bevel leidt materieel tot eenzelfde gevolg als de ontsleuteling van gegevens door derden. Daartoe wordt voorgesteld de regeling van het beklag aan te vullen. Daarnaast kan de verdachte de rechtmatigheid van het bevel ter terechtzitting betwisten.

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.

4.4 De strafbedreiging voor het opzettelijk niet voldoen aan een decryptiebevel

De strafbedreiging voor het opzettelijk niet voldoen aan een decryptiebevel door de verdachte vereist een zorgvuldige afweging. Voorop gesteld moet worden dat een verdachte, die opzettelijk niet voldoet aan een decryptiebevel, zich daarmee niet schuldig maakt aan het misdrijf van het maken van een beroep of gewoonte van het bezit, de vervaardiging en verspreiding van kinderpornografie of het plegen van een terroristisch misdrijf. Dat betekent dat de strafmaxima van

die misdrijven, wanneer geen toereikend bewijs voorhanden is dat deze door de verdachte zijn begaan, niet beschikbaar zijn. In verhouding tot deze strafmaxima moeten de op het niet voldoen aan het bevel te stellen strafmaxima voldoende hoog zijn om effectief te kunnen zijn. De onderliggende misdrijven worden doorgaans gepleegd door doorgewinterde criminelen die bereid zijn om vergaande maatregelen te treffen om ontdekking van het strafbare feit te voorkomen. Het maken van een beroep of gewoonte van het bezit, de vervaardiging en verspreiding van kinderpornografie is strafbaar gesteld met een gevangenisstraf van ten hoogste acht jaar of geldboete van de vijfde categorie. Voor terroristische misdrijven gelden lange tot zeer lange gevangenisstraffen. Een aan het niet voldoen aan het decryptiebevel te verbinden strafbedreiging die onvoldoende afschrikwekkend is zal ertoe kunnen leiden dat een verdachte de voor- en nadelen van weigering tegen elkaar afweegt en eerder kiest voor de weigering. Dat is niet wenselijk. Daar komt bij dat het plegen van de onderliggende misdrijven ernstige consequenties kan hebben voor de geestelijke gezondheid of lichamelijke integriteit van de slachtoffers, als geen zekerheid kan worden verkregen over de vraag of beelden van hen zijn vastgelegd en verspreid. Ten behoeve van de hulpverlening aan slachtoffers is het van essentieel belang toegang te verkrijgen tot de versleutelde gegevens, zodat daadwerkelijk hulp kan worden geboden. Het is niet aanvaardbaar dat de hulpverlening aan slachtoffers onnodig wordt belemmerd doordat een verdachte bewust ervoor kiest niet aan het decryptiebevel te voldoen.

Het opzettelijk niet voldoen aan een ambtelijk bevel is thans strafbaar gesteld als wederspanning, met een gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie (artikel 184 Sr). Deze strafbepaling omvat een groot aantal gedragingen van uiteenlopende ernst of zwaarte. De voorgestelde strafbepaling is specifiek gericht op het niet voldoen aan een decryptiebevel, in geval van verdenking van bepaalde, zeer ernstige strafbare feiten en een dringend opsporingsbelang een dergelijk bevel rechtvaardigt. Gelet op de aard en ernst van de feiten en de belangen die hierbij in het geding zijn – het belang van de waarheidsvinding, van de hulpverlening aan slachtoffers en van de bestrijding van kinderpornografie en terrorisme – is een strafbedreiging, die substantieel hoger is dan de strafbedreiging voor het niet opvolgen van een bevoegd gegeven ambtelijk bevel, gerechtvaardigd. Om de strafbedreiging effectief te doen zijn is een gevangenisstraf van meerdere jaren gerechtvaardigd. De ratio van de verhoogde strafbedreiging is dat het opzettelijk belemmeren van de opsporing van de zeer ernstige strafbare feiten, ten behoeve van de opsporing waarvan een decryptiebevel aan de verdachte kan worden gegeven, niet opweegt tegen het belang van de betrijding van deze feiten en de hulpverlening aan de slachtoffers. Voor degene die een ademtest of bloedproef weigert, geldt eenzelfde strafbedreiging als voor degene die onder invloed een voertuig bestuurt. Het niet voldoen aan een bevoegd gegeven ambtelijk bevel om medewerking te verlenen aan een ademtest of bloedproef ten behoeve van het onderzoek naar de rijvaardigheid, is strafbaar is gesteld het rijden onder invloed (artikelen 8, 163, zesde lid, j.o. 176, derde lid, WVV 1994). Overigens kan, ter onderbouwing van de substantieel hogere strafbedreiging dan voor de wederspanning, erop worden gewezen dat op andere specifieke deel terreinen eveneens voor hogere strafmaxima is gekozen. Een voorbeeld daarvan is het opzettelijk niet voldoen van een vordering, krachtens enig voorschrift van de Wet economische delicten gedaan door een opsporingsambtenaar. Op grond van de Wet economische delicten kan daarvoor een

gevangenisstraf van maximaal twee jaar worden opgelegd (artikelen 1, onder 5°, j.o. 6, eerste lid, onder 2°, j.o. 26 WED). Dit alles afwegend wordt voorgesteld dat het opzettelijk weigeren te voldoen aan een decryptiebevel strafbaar wordt gesteld met een gevangenisstraf van ten hoogste drie jaar of geldboete van de vierde categorie.

Een dergelijke strafbedreiging is in lijn met de strafmaxima in de andere landen. Zo is in Frankrijk gekozen voor drie jaar gevangenisstraf (met de mogelijkheid van strafverhoging tot vijf jaar als de overhandiging of toepassing van de sleutel het mogelijk gemaakt zou hebben het plegen van een misdrijf of overtreding te voorkomen of de effecten ervan te verkleinen), in het Verenigd Koninkrijk voor vijf jaar gevangenisstraf voor kinderporno en terrorismezaken, en Australië voor twee jaar gevangenisstraf. In het TILT-rapport wordt opgemerkt dat een bandbreedte van twee tot drie jaar gevangenisstraf – met eventuele hogere straffen voor bijzondere categorieën – kennelijk als een goede middenweg wordt gezien tussen enerzijds een te lage, niet effectieve straf en anderzijds een te hoge disproportionele straf (blz. 93/94).

4.5 De regeling in andere landen

In het TILT-rapport worden de wettelijke regelingen in enkele andere landen, zoals Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten, uitgebreid beschreven. Een korte weergave daarvan is opgenomen in de eerdergenoemde brief van 27 november 2012.

In de Franse Code pénal is, met de Wet op de dagelijkse veiligheid, een afzonderlijke bepaling opgenomen op grond waarvan degene, die kennis heeft van een geheime decryptiesleutel van een cryptologisch middel dat gebruikt kan zijn om een misdrijf of overtreding voor te bereiden, te faciliteren of te plegen en die weigert de sleutel op vordering van de autoriteiten te overhandigen, gestraft kan worden met een gevangenisstraf van drie jaar en een boete van 45.000 euro (artikel 434-15-2). Als de weigering is geschied terwijl de overhandiging of toepassing van de sleutel het mogelijk gemaakt zou hebben een misdrijf te voorkomen of de effecten hiervan te verminderen, dan kan de straf worden verhoogd naar vijf jaar gevangenisstraf en een boete van 75.000 euro. Daarnaast vormt het gebruik van encryptie een grond voor verhoging van de maximumgevangenisstraf met één categorie. Het bevel kan ook aan de verdachte worden gegeven. Tot nu toe is geen jurisprudentie bekend over de toepassing van de decryptieverplichting of de verhouding met het in artikel 6 van het EVRM vastgelegde beginsel van nemo tenetur.

In het Verenigd Koninkrijk is, met de Regulation of Investigative Powers Act 2000 (RIPA), een omvangrijke en complexe regeling van het ontsleutelbevel ingevoerd. Een ambtenaar van de douane, de politie of de veiligheidsdienst kan een persoon die redelijkerwijs geacht kan worden de sleutel te hebben, een schriftelijk bevel geven om de beschermde informatie vrij te geven in het belang van - onder meer - de voorkoming of ontdekking van strafbare feiten (s. 49 RIPA). De strafbedreiging is een gevangenisstraf van twee jaar, met een maximum van vijf jaar in terroristische zaken en kinderpornografie. Voor een ontsleutelbevel is rechterlijke toestemming nodig als de gegevens zijn verkregen op basis van een bevoegdheid die een rechterlijke machtiging vereist. In de andere gevallen is een opsporingsambtenaar zelf bevoegd een ontsleutelbevel te

geven, wanneer zijn functie een bepaald niveau vertegenwoordigt ('superintendent') of met toestemming van een opsporingsambtenaar van dat niveau. Vooraf dient het National Technical Assistance Centre (NTAC) te worden geconsulteerd over de uitoefening van de bevoegdheid. De aanvragen worden door het NTAC geregistreerd. Daarnaast oefenen de Chief Surveillance Commissioner en de Interception of Communications Commissioner onafhankelijk toezicht uit op de toepassing van de bevoegdheid. Door de toezichthoudende autoriteiten wordt ieder jaar een openbare rapportage opgesteld. Inmiddels heeft het Engelse Court of Appeal geoordeeld dat het ontsleutelbevel niet in strijd is met het in artikel 6 van het EVRM vastgelegde recht op een eerlijk proces. Daarbij is getoetst of de procedure in zijn geheel eerlijk is geweest. Indien het ontsleutelde materiaal inderdaad belastend blijkt te zijn, kan de rechter alsnog besluiten om dit materiaal uit te sluiten van het bewijs indien hij in een concreet geval oordeelt dat het nemo-teneturbeginsel is geschonden.

Naast het Verenigd Koninkrijk en Frankrijk kent ook Ierland de mogelijkheid van een ontsleutelbevel. Dit is echter beperkt tot fraude met digitale handtekeningen (Electronic Commerce Act 2000). Het niet meewerken aan het bevel is strafbaar met een gevangenisstraf van één jaar.

Wat betreft de landen buiten de EU kennen verschillende landen een verplichting voor de verdachte tot het ontsleutelen van versleutelde gegevens. In de VS is het beginsel van nemo tenetur vastgelegd in het vijfde amendement ("No person (...) shall be compelled in any criminal case to be a witness against himself"). De zaken die in de VS hebben gespeeld hadden alle betrekking op een vordering van een zogenaamde Grand Jury, vergelijkbaar met een vordering van een rechter-commissaris in een Nederlands opsporingsonderzoek. Het niet-meewerken aan de vordering is strafbaar op grond van 'contempt of court'. De Amerikaanse rechter heeft geoordeeld dat een vordering tot het overhandigen van bestanden van een computer of het zelf invoeren van een wachtwoord niet in strijd is met het Vijfde Amendement, indien de overheid met voldoende precisie kan aantonen dat zij weet dat de documenten bestaan en waar ze te vinden zijn. Aldus is vereist dat justitie over voldoende onafhankelijk bewijs beschikt van het bestaan van het belastende materiaal en van de beschikkingsmacht van de verdachte daarover. In Australië is een ontsleutelplicht ingevoerd met de Cybercrime Act 2001. Met die wet is s. 3LA ingevoegd in de Crimes Act 1914. De ontsleutelplicht geldt voor alle strafbare feiten van de Crimes Act 1914, en geldt ook jegens een verdachte. Het niet meewerken aan de verplichting is strafbaar gesteld met een gevangenisstraf van twee jaar.

4.6. De bescherming van grondrechten

4.6.1 Het beginsel van nemo tenetur

Volgens de vaste jurisprudentie van het EHRM wordt het nemo tenetur-beginsel beschermd door artikel 6 EVRM (recht op een eerlijk proces). De precieze reikwijdte van het beginsel is in de jurisprudentie nog niet volledig uitgekristalliseerd. De jurisprudentie lijkt in sterke mate te zijn bepaald door de casuïstiek. De ratio achter het nemo tenetur-beginsel is volgens het EHRM dat verklaringen die onder dwang zijn afgelegd, beïnvloedbaar zijn en onjuistheden kunnen bevatten

waardoor het bewijs onbetrouwbaar wordt. Het beginsel ziet primair op de verklaringsvrijheid van de verdachte; het zwijgrecht. Indachtig die strekking heeft het EHRM in een aantal arresten overwogen dat materiaal dat met gebruik van dwangmiddelen is verkregen maar dat onafhankelijk van de wil van de verdachte bestaat, buiten de reikwijdte van het nemo-teneturbeginsel valt. Dergelijk materiaal – in de jurisprudentie worden genoemd: documenten, adem, bloed- en urinemonsters, het lichaamsmateriaal ten behoeve van DNA-onderzoek, opnamen van stemgeluid – is niet door het uitoefenen van druk te beïnvloeden. Daarmee is ook in het geval van gedwongen medewerking de integriteit van het strafproces niet in het geding. Bij de beoordeling van nemo tenetur maakt het EVRM onderscheid in materiaal dat al dan niet onafhankelijk bestaat van de wil van de verdachte. Is het eerste het geval (de boekhouding, het bloed), is er meer ruimte voor een verplichting tot actieve medewerking van de verdachte. Is het laatste het geval, dan ligt dit anders.

In het Nederlandse stelsel van Strafvordering zijn inmiddels uitzonderingen op het beginsel van nemo tenetur aanvaard. Dit betreft bijvoorbeeld de bevoegdheid van de officier van justitie te bevelen dat van een verdachte celmateriaal (wangslimvlies, bloed of haarwortels) wordt afgenomen ten behoeve van een DNA-onderzoek (artikel 151b, eerste lid, Sv). Een ander voorbeeld betreft de verplichting van een bestuurder van een voertuig tot het verlenen van medewerking aan een ademtest of een bloedonderzoek (artikel 163, tweede en zesde lid, WVV). In beide gevallen gaat het om materiaal dat bestaat onafhankelijk van de wil van de verdachte. Overigens vormt het beginsel van nemo tenetur een essentiële waarborg in het Nederlandse stelsel van strafvordering. Daarvoor kan worden gewezen op de artikelen 96a, tweede lid (de uitlevering van een voor inbeslagneming vatbaar voorwerp), 105, derde lid (het bevel tot uitlevering van een voor inbeslagneming vatbaar voorwerp), 125k, derde lid (een bevel tot het verschaffen van toegang tot een geautomatiseerd werk), 126a, tweede lid (opgave van gegevens of vermogensbestanddelen in het kader van een strafrechtelijk financieel onderzoek), 126nc, derde lid, 126uc, tweede lid en 126zk, tweede lid (vordering verstrekking identificerende gegevens), 126nd, 126ud en 126zl, tweede lid (vordering verstrekking gegevens), 126ne, 126ue en 126zm, eerste lid, (vordering verstrekking toekomstige gegevens) en 126nf, 126uf en 126zn, tweede lid (vordering verstrekking gevoelige gegevens) van het Wetboek van Strafvordering. In deze artikelen wordt de verdachte uitgesloten van de daarin opgenomen verplichtingen tot het verlenen van medewerking aan de opsporing van strafbare feiten.

Juist bij een elektronische sleutel of wachtwoord is discussie mogelijk over de vraag of dit materiaal onafhankelijk van de wil van de verdachte bestaat. Gesteld kan worden dat een (complexe) encryptiesleutel, die op een gegevensdrager is opgeslagen, onafhankelijk van de wil van de verdachte bestaat, zodat deze informatie buiten de reikwijdte van het nemo-teneturbeginsel valt. Maar als de verdachte de encryptiesleutel uit het hoofd zou leren, kan de vraag worden opgeworpen of het wachtwoord dat de gegevens toegankelijk maakt onder de reikwijdte van het nemo-teneturbeginsel valt. Het recht van de verdachte om geen medewerking te verlenen aan het verkrijgen van voor hem mogelijk belastend bewijsmateriaal is in elk geval – ook volgens het EHRM – geen absoluut recht.

In het TILT-rapport wordt opgemerkt dat de rechtsontwikkeling een verfijning van het Saunders-criterium laat zien. Sedertdien wordt door het EHRM onderscheid gemaakt tussen materiaal dat onafhankelijk van de wil van de verdachte bestaat en materiaal dat onafhankelijk van de wil van de verdachte kan worden verkregen. Als een wachtwoord ergens is opgeschreven is er alleen sprake van een vordering tot uitlevering van fysiek bewijs. Gaat het echter om een wachtwoord dat alleen in het hoofd van de verdachte is opgeslagen dan is een intellectuele inspanning van de verdachte nodig. In de praktijk zal justitie niet (zeker) weten of het wachtwoord ergens is opgeschreven, en aangenomen moet worden dat het wachtwoord feitelijk alleen in het hoofd van de verdachte bestaat. Het gaat dan om materiaal dat onafhankelijk van de wil van de verdachte bestaat maar niet onafhankelijk van zijn wil kan worden verkregen. Voor het vorderen van het wachtwoord betekent dit dat het alleen aanvaardbaar zou kunnen zijn als justitie voldoende overtuigend kan aantonen dat de verdachte het wachtwoord (nog) kent. In het rapport wordt opgemerkt dat wanneer het gaat om materiaal dat niet door de normale lichaamsfuncties wordt geproduceerd, de verdachte zich meer moet inspannen om materiaal dat onafhankelijk van zijn wil bestaat, te produceren. Wanneer de overheid onder dwang materiaal probeert te verkrijgen waarbij de verdachte moet meewerken op een manier die de passieve of beperkt (fysiek) actieve medewerking te boven gaat, legt het Hof meer de nadruk op het feit dat het materiaal wordt 'obtained in defiance of the will of the accused' en minder nadruk op het feit dat het materiaal onafhankelijk van de wil van de verdachte bestaat (blz. 85). Het vorderen van een wachtwoord zou alleen aanvaardbaar kunnen zijn als justitie voldoende overtuigend kan aantonen dat de verdachte het wachtwoord (nog) kent. Bij de beoordeling van de toelaatbaarheid van een inbreuk op het nemo-teneturbeginsel zijn vier factoren in gezamenlijkheid van belang:

1. de aard en mate van de dwang;
2. het gewicht van het publieke belang;
3. de aanwezigheid van relevante waarborgen in de procedure; en
4. de manier waarop het afgedwongen materiaal wordt gebruikt.

Er zijn verschillende modaliteiten en gradaties mogelijk die de inbreuk op nemo tenetur aanvaardbaar kunnen maken. Bij een ontsleutelplicht voor verdachten gaat het om een afgewogen geheel. Hierbij fungeren de factoren 1 en 4 enerzijds en de factoren 2 en 3 anderzijds als communicerende vaten. Naarmate de dwang om mee te werken groter is, en naarmate het afgedwongen materiaal een zwaardere rol heeft bij het bewijs, zal het publieke belang van afgedwongen medewerking des te groter moeten zijn en zullen er meer waarborgen moeten zijn voor rechtsbescherming. Bij een lagere mate van dwang of een ondergeschikte rol van afgedwongen bewijsmateriaal zal een ontsleutelplicht eerder de toets van artikel 6 van het EVRM kunnen doorstaan (blz. 103).

Wat betreft de aard van de dwang zal een strafbedreiging van twee tot drie jaar volgens het TILT-rapport een ernstige vorm van dwang opleveren. Een dergelijke dwang zal door het EHRM vermoedelijk alleen worden geaccepteerd als er andere criteria zijn die deze hoge mate van dwang compenseren. De dwang zal ook kleiner zijn als de verdachte bij een decryptiebevel met zijn advocaat kan overleggen om weloverwogen zijn procespositie te kunnen bepalen. Daarnaast kan

ook het gewicht dat bij de bewijsconstructie aan het niet-meewerken wordt toegekend, van belang zijn (blz. 94).

Het publieke belang dient voldoende zwaarwegend te zijn. Dit betekent dat een decryptiebevel aan de verdachte alleen ingevoerd zou moeten worden ten aanzien van delicten die voldoende ernstig zijn, bijvoorbeeld waar gevangenisstraf van ten minste vier jaar op staat, en dat een bevel alleen toegepast zou moeten worden in gevallen die ook in concreto voldoende ernstig zijn. Ook een subsidiariteitseis zal helpen om het publieke belang gewicht te geven. Ten tweede zullen er aanzienlijke relevante waarborgen in de procedure moeten zijn opgenomen. In dit licht verdient de Britse wetgeving volgens het TILT-rapport de aandacht, omdat daarin is voorzien in onafhankelijk toezicht op de uitoefening van het ontsleutelbevel. De Chief Surveillance Commissioner heeft de taak toe te zien op de uitoefening door niet-rechterlijke instanties van de bevoegdheden en plichten uit Deel III RIPA (s. 62 RIPA). Ten derde is relevant op welke manier het ontsleutelbevel en het daaruit voortkomende bewijsmateriaal wordt gebruikt. Een onder dwang opgelegd decryptiebevel aan de verdachte zal sneller aanvaardbaar zijn als het specifiek is geënt op een concreet maatschappelijk probleem in een bepaalde sector. Zo zou de problematiek van de bewijsbaarheid van kinderpornobezit een sterk argument van publiek belang kunnen zijn om de inbreuk op het nemo-teneturbeginsel bij de strafbaarstelling van weigering te rechtvaardigen (blz. 99).

In het TILT-rapport wordt geconcludeerd dat een decryptiebevel aan verdachten met strafbaarstelling van weigering een inbreuk maakt op het beginsel van nemo tenetur. In het rapport wordt niettemin enige ruimte binnen de grenzen van het nemo-teneturbeginsel gezien om een onder strafbedreiging afgedwongen ontsleutelplicht voor verdachten in te voeren. Een dergelijke inbreuk zal alleen aanvaardbaar zijn in het licht van artikel 6 van het EVRM als de wettelijke regeling en uitvoering met voldoende waarborgen worden omkleed. Een zorgvuldige regeling met veel checks and balances, zoals in de Britse regeling, is dan vereist. Daarbij dient ook aandacht te worden geschonken aan de wijze waarop het afgedwongen materiaal wordt gebruikt, een discretionaire bevoegdheid van de rechter om belastend materiaal alsnog uit te sluiten van bewijs speelt daarbij een belangrijke rol. Hierbij wordt ook gewezen op de jurisprudentie in het VK, de VS, Australië en Frankrijk, waaruit blijkt dat wetgevers en rechters een strafrechtelijk gesanctioneerde ontsleutelplicht voor verdachten onder bepaalde voorwaarden aanvaardbaar achten. Hoewel de rechtspraak in deze landen nog in ontwikkeling is, wordt in het rapport opgemerkt dat geconcludeerd kan worden dat de vraag naar de verenigbaarheid met het nemo-teneturbeginsel in deze landen niet a priori negatief wordt beantwoord, maar in de rechtspraak casuïstisch wordt beantwoord, waarbij het afdwingen van medewerking soms wel en soms niet aanvaardbaar zal worden geacht (blz. 104/105). Dit noopt tot een zorgvuldige afweging van de voorwaarden voor toepassing van de bevoegdheid.

Met dit wetsvoorstel wordt de verplichting voor de verdachte om gegevens te ontsleutelen strafbaar gesteld met een gevangenisstraf van te hoogste drie jaar. Deze strafbedreiging is aanzienlijk hoger dan de strafbedreiging voor de wederspanning die, zoals hierboven reeds is gemeld, strafbaar is gesteld met een gevangenisstraf van ten hoogste drie maanden (artikel 184

Sr). De voorgestelde strafbedreiging van drie jaar gevangenisstraf betekent dat de dwang om mee te werken aanzienlijk is, een dergelijke mate van dwang zal alleen dan de toets van artikel 6 EVRM kunnen doorstaan als het publieke belang van afgedwongen medewerking groter is en er meer waarborgen voor rechtsbescherming zijn. In het licht van deze vereisten wordt het decryptiebevel beperkt tot het maken van een beroep of gewoonte van het bezit, de vervaardiging en verspreiding van kinderpornografie en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens. Daarbij zullen zeer strikte waarborgen gelden voor de uitoefening en toepassing van deze bevoegdheid. Een bevel kan uitsluitend worden gegeven als het belang van het opsporingsonderzoek dat dringend vordert. Het bevel zal uitsluitend gegeven kunnen worden door de officier van justitie, na schriftelijke machtiging van de rechter-commissaris. Daardoor is rechterlijke controle gewaarborgd voordat de bevoegdheid wordt ingezet.

In het Verenigd Koninkrijk is een toezichthoudend orgaan belast met het toezicht op de toepassing van de bevoegdheid in de praktijk. Het toezicht door de rechter-commissaris op de toepassing van de bevoegdheid in Nederland past in ons systeem van strafvordering waarbij de toepassing van ingrijpende opsporingsbevoegdheden, zoals het aftappen van communicatie en het direct af luisteren, afhankelijk is van een voorafgaande schriftelijke machtiging van de rechter-commissaris. Er zijn echter meer verschillen met de Britse regeling. In de eerste plaats zal de bevoegdheid tot het geven van een decryptiebevel aan de verdachte worden beperkt tot bepaald aangewezen, zeer ernstige misdrijven. In de Britse wetgeving geldt deze beperking niet; voldoende is dat het bevel noodzakelijk is voor bepaalde doeleinden, waaronder de voorkoming of bestrijding van criminaliteit (artikel 49, derde lid, RIPA). In de tweede plaats zal de bevoegdheid uitsluitend uitgeoefend kunnen worden op basis van een bevel van de officier van justitie, met een machtiging van de rechter-commissaris. De opsporingsambtenaar is daartoe niet zelfstandig bevoegd. In de Britse wetgeving kan een decryptiebevel ook worden gegeven door een ambtenaar van de douane, de politie of de veiligheidsdienst, die een bepaald niveau vertegenwoordigt. Een (afzonderlijke) rechterlijke machtiging is vereist als de bevoegdheid op basis waarvan de gegevens zijn verkregen een rechterlijke machtiging vereist of wanneer de gegevens zijn verkregen zonder uitoefening van een wettelijke bevoegdheid.

Gelet op deze overwegingen meen ik dat de voorgestelde wettelijke regeling voor het decryptiebevel de toets van artikel 6 EVRM kan doorstaan.

4.6.2 Het recht op bescherming van de persoonlijke levenssfeer

Het decryptiebevel aan een verdachte kan ertoe leiden dat de overheid de beschikking verkrijgt over of kennis neemt van gegevens die een min of meer volledig beeld geven van bepaalde aspecten van iemands leven. De toepassing van een decryptiebevel aan een verdachte kan daarom leiden tot een inbreuk op eerbiediging van de persoonlijke levenssfeer, bedoeld in artikel 10 van de Grondwet en in artikel 8 van het EVRM. De voorgestelde regeling voor het decryptiebevel dient daarom de toets aan de voorwaarden die uit de Grondwet en het EVRM voortvloeien, te doorstaan. Ingevolge artikel 10 van de Grondwet heeft eenieder recht op eerbiediging van de persoonlijke levenssfeer, behoudens bij of krachtens de wet te stellen beperkingen. Het recht op de bescherming van de persoonlijke levenssfeer is dus geen absoluut recht, maar op basis van een

wettelijke regeling zijn beperkingen mogelijk. Met dit wetsvoorstel wordt voorzien in een regeling van het decryptiebevel aan de verdachte in het Wetboek van Strafvordering. Ingevolge artikel 8 van het EVRM is inmenging van enig openbaar gezag in de uitoefening van het recht op eerbiediging van de persoonlijke levenssfeer alleen toegestaan voor zover daarin 'bij de wet is voorzien' en dit 'in een democratische samenleving noodzakelijk is' in het belang van enkele met name genoemde doelen, waaronder het voorkomen van strafbare feiten. Zoals in de paragrafen 2.9.1 en 3.4.1 reeds aan de orde is gekomen, wordt de noodzaak tot de inzet van een bevoegdheid waarmee dit recht wordt 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 in welke gevallen en onder welke omstandigheden de bevoegdheid kan worden toegepast. De regeling moet bovendien voldoende waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid.

De voorgestelde bevoegdheid van het decryptiebevel aan de verdachte voldoet aan deze eisen. Aan de eis dat de inmenging 'bij de wet is voorzien', wordt met de voorgestelde wettelijke regeling tegemoet gekomen. De voorgestelde wettelijke regeling omschrijft de gevallen waarin de bevoegdheid kan worden toegepast. De toepassing is beperkt tot enkele bepaald aangewezen, zeer ernstige misdrijven. Verder is vereist dat het opsporingsonderzoek het decryptiebevel dringend vordert. Het bevel kan uitsluitend worden gegeven met het oog op de opheldering van het desbetreffende strafbare feit. De uitoefening van de bevoegdheid is voorbehouden aan de officier van justitie, zodat een zorgvuldige afweging plaatsvindt van het belang van eerbiediging van de persoonlijke levenssfeer en het belang van de opsporing. Daarbij is voorzien in een rechterlijke toetsing. Vanwege de ingrijpendheid van de bevoegdheid is voorzien in een rechterlijke toetsing voordat het bevel kan worden gegeven. In het bevel van de officier van justitie moeten bepaalde gegevens zijn opgenomen, zodat de verdachte kan begrijpen wat er van hem wordt verwacht en de rechter-commissaris de rechtmatigheid van het bevel kan toetsen. Verder is in de wet nauwkeurig omschreven op welke wijze de verdachte uitvoering moet geven aan het decryptiebevel. Op grond hiervan kan worden geconcludeerd dat de voorgestelde wettelijke regeling voldoet aan de eisen op het gebied van de kenbaarheid en de voorzienbaarheid.

Bij de eis dat de inmenging noodzakelijk moet zijn in een democratische samenleving geldt een eigen beoordelingsruimte voor de nationale overheid. De eis van noodzakelijkheid houdt in dat de voorgestelde bevoegdheid nodig is voor de strafrechtelijke handhaving. In een concreet geval van toepassing moet tevens een afweging plaatsvinden van het belang van eerbiediging van de persoonlijke levenssfeer en het belang van de opsporing. Daarbij gaat het om een toetsing aan de eisen van proportionaliteit en subsidiariteit. Hierboven is, in paragraaf 4.1, de noodzaak van een decryptiebevel aan de verdachte aan de orde gekomen. De ontwikkelingen op het gebied van de encryptie maken het eenvoudig om gegevens af te schermen voor de politie. Het is gebleken dat in kringen van personen die zijn betrokken bij de productie en distributie van kinderpornografie veelvuldig gebruik wordt gemaakt van de versleuteling van gegevens, zodat de gegevens niet toegankelijk zijn voor de politie. Weliswaar wordt in dit wetsvoorstel ook voorgesteld te komen tot een wettelijke regeling van onderzoek in een geautomatiseerd werk, maar dit onderzoek biedt geen garantie dat met de inzet van die bevoegdheid daadwerkelijk de elektronische sleutels worden

verkregen waarmee de versleuteling van de gegevens ongedaan kan worden gemaakt. De mogelijkheid van een decryptiebevel aan de verdachte is onmisbaar voor de gevallen waarin de gegevens zijn versleuteld, de toegang tot de versleutelde gegevens van essentieel belang is voor de opsporing van het desbetreffende strafbare feit en er geen andere, minder ingrijpende mogelijkheid is om toegang te verkrijgen tot de gegevens.

5. *De heling van gegevens*

5.1 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 139f 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 die 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 "heling" 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 overgenomen, al dan niet na in een geautomatiseerd werk te zijn binnengedrongen (de computervredereuk, 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.

5.2 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) ontzutselen 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 computervrederebreuk 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 computervrederebreuk (artikel 138ab Sr). Inmiddels hebben ook andere gevallen in de media de nodige aandacht gekregen, zoals de publicatie op het internet van door computervrederebreuk 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). Dit onderdeel van het voorliggende wetsvoorstel vormt het resultaat daarvan.

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 computervrederebreuk – 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 verschafft. 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 computervrederebreuk (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 "vernietigen" 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 computervredesbreuk te zijn verkregen. De voorgestelde strafbepaling is, in aanvulling op de strafbaarstelling van computervredesbreuk, 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. In het voorgestelde artikel 139f 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 computervredbreuk. Zo worden personen strafbaar die gegevens, die uit de computer van anderen zijn onttreemd, bekend maken aan een ander, verkopen of op internet plaatsen. Hiermee zal ook degene die zich erop beroept deze gegevens niet zelf te hebben onttreemd 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. Zie hierover de artikelsgewijze toelichting op artikel 139f 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 139f 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 computervredbreuk. 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).

Met betrekking tot de voorgestelde strafbaarstelling van het wederrechtelijk overnemen van gegevens is tijdens de consultatie van het eerdere conceptwetsvoorstel 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.

5.3 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.

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 139f 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 26-03-2013, 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.

6. Financiële paragraaf

Uitvoering van de bevoegdheden in dit wetsvoorstel hebben financiële gevolgen voor de politie en voor de rechterlijke macht, zowel voor de staande als de zittende magistratuur. Niet alleen door 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 door 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 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. De recente vorming van de Nationale Politie en het reorganisatieproces dat nu loopt, en de budgetbesprekingen bij het openbaar ministerie geven thans onvoldoende houvast om de financiële consequenties van het wetsvoorstel en het vermogen om die te dragen geheel te overzien. Uitgangspunt is dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in geautomatiseerd werk dekken binnen het reguliere budget. Tijdens de consultatie wordt het gesprek met de politie en de rechterlijke macht voortgezet.

II ARTIKELSGEWIJS

Artikel I, onderdeel A

Zoals in paragraaf 3 van het algemeen deel van de toelichting is opgemerkt, wordt de bevoegdheid om te bevelen dat gegevens ontoegankelijk worden gemaakt, als zelfstandige bevoegdheid naar het Wetboek van Strafvordering overgeheveld (zie nader artikel II, onderdeel F). 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).

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" omvatten 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, 26671, nr. 3, blz. 44). 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 is gebleken dat de cumulatie van voorwaarden problemen oplevert in het licht van de ontwikkeling van de informatie- en communicatietechnologie. Dit heeft specifiek betrekking op de strafbaarstelling van het hacken van een router. Een router kan worden omschreven als een apparaat dat twee of meer verschillende computernetwerken aan elkaar verbindt, bijvoorbeeld internet en een bedrijfsnetwerk, en pakketten data van het ene naar het andere netwerk verzendt (<http://nl.wikipedia.org/wiki/Router>). In de jurisprudentie is de bovenbedoelde cumulatie van de functies bevestigd. Daarbij is bepaald dat uit de wetsgeschiedenis ook volgt dat het begrip geautomatiseerd werk niet beperkt is tot apparaten die zelfstandig aan deze drievoudige eis kunnen voldoen. Ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen heeft de wetgever onder het begrip geautomatiseerd werk willen brengen (HR 26 maart 2013, LJN BY9718).

Vanuit het oogpunt van de rechtshandhaving is het niet aanvaardbaar dat personen binnen kunnen dringen in een router om vervolgens door middel van de beveiligde verbinding, die in gebruik is bij een ander, het internet op te gaan en berichten te verzenden waarbij de indruk wordt gewekt dat het bericht afkomstig is van de rechthebbende van de beveiligde verbinding. Weliswaar wordt hiermee geen toegang verkregen tot het geautomatiseerde werk dat met een router is verbonden, niettemin wordt met dergelijk gedrag gebruik gemaakt van de internetverbinding van een ander waardoor de capaciteit van die verbinding wordt verminderd. Daar komt bij dat de

opsporingsdiensten op afstand heimelijk een router moeten kunnen betreden, op grond van het voorgestelde artikel 125ja Sv, ten behoeve van de identificatie van het geautomatiseerde werk of de gebruiker. Ondanks de ruime uitleg van het begrip geautomatiseerd werk in de jurisprudentie is het dan ook wenselijk om ook de router onder de definitie van geautomatiseerd werk te brengen. Daarom wordt voorgesteld de definitie van geautomatiseerd werk aan te passen. Om nauw aan te sluiten bij de bestaande begripsomschrijving en in het licht van de bedoeling van de wetgever, zoals die ook tot uitdrukking komt in de toelichting op artikel 80sexies Sr, is gekozen voor een alternatieve formulering. Een eerste vereiste is dat een geautomatiseerd werk een inrichting is die bestemd is om langs elektronische weg gegevens te verwerken. Cumulatief is vereist dat de bestemming van die inrichting tevens is gericht op het opslaan of overdragen van gegevens. Hieronder vallen dus computers, smartphones, netwerken van aan elkaar verbonden computers, servers, en geautomatiseerde inrichtingen voor telecommunicatie. Hieronder vallen dus niet de inrichtingen die uitsluitend bestemd zijn voor de opslag van gegevens, zoals een usb-stick, of de overdracht van gegevens, zoals een (analoge) radio of een zend- of ontvanginrichting.

Artikel I, onderdeel C

In het voorgestelde artikel 138c Sr wordt 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 hoeft te zijn van het binnendringen van het desbetreffende geautomatiseerde werk door degene die de gegevens (vervolgens) wederrechtelijk overneemt. Voor een toelichting op dit onderdeel kan worden verwezen naar paragraaf 5.2 van deze toelichting, waarin uitvoering is ingegaan op de achtergronden van deze wijziging.

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, voor zover dit niet onder het “thuis kopiëestelsel” in artikel 16c e.v. van de Auteurswet valt, strafbaar op grond van de Auteurswet.

Artikel I, onderdeel D

Voorgesteld wordt de maximale gevangenisstraf, die is voorzien in het geldende artikel 139e Sr, te verhogen van zes maanden naar een jaar. De verhoging geldt ook voor zover het gaat om beeldmateriaal dat door misdrijf is verkregen. 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 schuldheiling is een maximale gevangenisstraf gesteld van een jaar (artikel 417bis Sr) en op opzetheling vier jaar (artikel 416 Sr). Daarbij kan worden aangetekend dat in geval de rechthebbende de beschikkingsmacht over de gegevens heeft verloren, volgens de in hoofdstuk 5 van het algemeen deel van de toelichting bedoelde uitspraken van enkele feitenrechters kan worden aangenomen dat van diefstal van een goed sprake is; in die lijn ligt dat de heilingbepalingen 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.

Artikel I, onderdeel E

Artikel 139f Sr

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 de hoogleraar B.J. Koops heeft gemaakt (zie "Tijd voor Computercriminaliteit III", *NJB* 2010, blz. 2465-2466) is de delictsommschrijving 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 downloadt. 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 kindporno en auteursrechtelijk beschermd materiaal dat niet onder het thuishoofdstelsel 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 uit het geldende artikel 139e Sr overgenomen. 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 de maximale gevangenisstraf die is voorzien in het geldende artikel 139e Sr verhoogd van zes maanden naar een jaar. De verhoging geldt ook voor zover het gaat om beeldmateriaal dat door misdrijf is verkregen. 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). 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 waarborg is besproken in paragraaf 5.3 van het algemeen deel van de toelichting.

Artikel I, onderdeel F

In het voorgestelde artikel 139f Sr is de strafbaarstelling opgenomen van het voorhanden hebben en bekend maken van door misdrijf verkregen gegevens. Omdat in het voorgestelde artikel onverschillig is uit welk misdrijf de gegevens zijn verkregen, kunnen de huidige artikelen 139f, onderdeel 2°, en 139g Sr 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. 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.

Artikel I, onderdeel G

In het algemeen deel van de toelichting is reeds ingegaan op de strafbedreiging voor het opzettelijk niet voldoen aan een decryptiebevel door de verdachte.

De verdachte die opzettelijk niet voldoet aan het bevel tot het ontsleutelen van gegevens pleegt een misdrijf. Het opzet heeft betrekking op alle bestanddelen van het delict. De verdachte is niet strafbaar als het bevel niet rechtmatig is gegeven. Dit is aan de orde als het bevel niet door een officier van justitie is gegeven of niet aan de andere wettelijke vereisten is voldaan. De verdachte kan zich erop beroepen niet in staat te zijn aan het bevel te voldoen omdat hij niet in staat is de sleutel te reproduceren. Zijn geheugen schiet te kort of het papier, waarop de elektronische sleutel is geschreven, is buiten zijn beschikkingsmacht geraakt. Dit kan worden aangemerkt als een beroep op overmacht, dat echter ook consequenties kan hebben voor het bewijs van het opzet. Het is dan aan de rechter om een dergelijk verweer te beoordelen. Afhankelijk van de feiten en omstandigheden in het concrete geval zal een rechter zich hieromtrent een oordeel moeten vormen. Het openbaar ministerie kan feiten en omstandigheden aanvoeren ter weerlegging van een dergelijk verweer. Daarvoor kan worden gedacht aan afgetapte informatie die inzicht geeft over het gebruik van de versleutelde bestanden door de verdachte. Een internettap biedt daarvoor mogelijkheden. Voorstelbaar is ook dat de verdachte betwist beschikkingsbevoegd te zijn ten aanzien van de gegevensdrager dan wel de versleutelde gegevens. In een dergelijk geval zullen verklaringen van getuigen of andere bewijsmiddelen ter weerlegging kunnen worden ingebracht.

Artikel I, onderdeel H

Dit betreft een wijziging van meer technische aard. In artikel 126la van het Wetboek van Strafvordering 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).

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 II, onderdeel A

Dit betreft een aanvulling van artikel 67 Sv, dat de gevallen bevat waarin een bevel tot voorlopige hechtenis kan worden gegeven. Dit betreft 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 139f Sr omschreven misdrijf. 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

Voorgesteld wordt het opschrift van de zevende afdeling van Titel IV van het Wetboek van Strafvordering te wijzigen in verband met het opnemen van de regeling van het onderzoek in een geautomatiseerd werk.

Artikel II, onderdeel C

Artikel 125ja

Eerste lid

Dit betreft het bevel tot onderzoek in een geautomatiseerd werk. Het bevel kan worden gegeven aan een opsporingsambtenaar, als bedoeld in artikel 141, onder b, Sv, of een buitengewone opsporingsambtenaar als bedoeld in artikel 142, eerste lid, onder b, Sv. Dit betreft in de eerste plaats de ambtenaren van politie, bedoeld in artikel 2, onder a, van de Politiewet 2012, en de ambtenaren van politie, bedoeld in artikel 2, onder c en d, van die wet, voor zover zij zijn aangesteld voor de uitvoering van de politietaak. Dit betreft in de tweede plaats de ambtenaren waarvan de opsporingsbevoegdheid zich uitstrekt tot de in de akte of aanwijzing aangeduide strafbare feiten. 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.

Het onderzoek dat met het oog op de in het voorgestelde artikel 125ja, eerste lid, Sv genoemde doelen wordt verricht, kan plaatsvinden in een geautomatiseerd werk of de daarmee in verbinding staande gegevensdrager. Voor de definitie van geautomatiseerd werk kan worden verwezen naar artikel 80sexies Sr. Voor een gegevensdrager kan worden gedacht aan een usb-stick of een externe harde schijf die aangesloten is op een computer. Vereist is dat het geautomatiseerde werk of de daarmee in verbinding staande gegevensdrager 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 of de gegevensdrager. 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. 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 omschrijving van onderzoek in een geautomatiseerd werk staat er niet aan in de weg dat ook onderzoek wordt verricht in een ander geautomatiseerd werk dat bij de verdachte in gebruik is, en dat vanuit het geautomatiseerde werk dat bij hem in gebruik is kan worden benaderd. Binnen de voorgestelde bevoegdheid kan als het ware worden 'doorgestapt' naar een ander geautomatiseerd werk. Hierbij kan ook worden verwezen naar de wetsgeschiedenis, waaruit volgt dat het begrip geautomatiseerd werk niet is beperkt tot apparaten die zelfstandig voldoen aan de vereisten van opslag, verwerking en overdracht van gegevens. Ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen zijn onder het begrip geautomatiseerd werk gebracht.

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, het overnemen van gegevens ook betrekking kan hebben op gegevens die na het tijdstip van afgifte van het bevel worden verwerkt. 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 overgenomen en 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 'overnemen' van gegevens wordt bedoeld op het kopiëren van gegevens, zonder dat deze uit de beschikkingmacht 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.

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.

Vanwege de plaatsing van deze bepaling in de zevende afdeling van Titel IV van het Wetboek van Strafvordering is artikel 125i Sv van toepassing. Deze bepaling staat in de weg aan onderzoek naar gegevens die zijn ingevoerd door of vanwege personen die zich kunnen beroepen op een wettelijk verschoningsrecht, behoudens met hun instemming, voor zover hun plicht tot geheimhouding zich uitstrekt (artikel 218 Sv). Naar gegevens waartoe hun plicht tot geheimhouding zich uitstrekt vindt geen onderzoek plaats noch worden zodanige gegevens vastgelegd. Geen toestemming is vereist als sprake is van 'zeer uitzonderlijke omstandigheden die met zich meebrengen dat het belang van de waarheidsvinding moet prevaleren boven het belang dat door het verschoningsrecht wordt gediend' (HR 10 maart 2009, LJN BG9494). De toestemming zal door de verschoningsgerechtigde persoonlijk of door een persoon die verklaart daartoe te zijn gemachtigd (HR 25 november 1986, NJ 1987, 513) en uitdrukkelijk per geval moeten worden gegeven.

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 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 dor 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 derde 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 (het opnemen van geluid, het maken van screenshots, het vastleggen van toetsaanslagen e.d.). In de vierde 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. Tenslotte dient te worden vermeld voor welk deel van het geautomatiseerd werk of de daarmee in verbinding staande gegevensdrager 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 (gegevens van een e-mailbox of van een harde schijf, msn-berichten, Skype communicatie e.d.).

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, 126m, 126l, 126o, 126s, 126t, 126zd, 126zf en 126zg Sv. 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 artikelen 126l, 126s dan wel 126zf of het bevel tot het aftappen van communicatie, bedoeld in de artikelen 126m, 126t dan wel 126zg Sv, betreft dit de gegevens, bedoeld in de artikelen 126l, 126s, 126zf, derde lid, respectievelijk de artikelen 126m, 126t, 126zg, tweede lid, Sv. Bij het bevel tot stelselmatige observatie, bedoeld in de artikelen 126g, 126o en 126zd, eerste lid, onderdeel a, Sv, betreft dit de gegevens, bedoeld in artikel 126g, vijfde lid, respectievelijk 126o, vierde 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.

Niet is vereist dat in het bevel de methode(n) wordt vermeld, op grond waarvan in een geautomatiseerd werk of de daarmee in verbinding staande gegevensdrager wordt binnengedrongen. Dit zou de opsporingsdiensten nodeloos beperken in de wijze waarop uitvoering wordt gegeven aan het bevel tot het doorzoeken van een geautomatiseerd werk en overigens kunnen leiden tot extra werklust 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.

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 als het overnemen en vastleggen van gegevens of de maatregel van de ontoegankelijkmaking van gegevens. Hiermee wordt tevens aangesloten bij de duur van een bevel tot het opnemen van vertrouwelijke communicatie of het aftappen van communicatie (artikelen 126l, 126m, 126s en 126t, vijfde lid, 126zf, vierde lid, en 126zg, vijfde lid, 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 en 126o, vijfde 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 heeft 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, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van andere bijzondere opsporingsbevoegdheden met betrekking tot de gegevens in het geautomatiseerde werk, 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 dient op grond van dit lid aan de rechter-commissaris te worden voorgelegd, met het oog op de 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 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 mondelinge 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 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 van een geautomatiseerd werk beperkt tot de aanpassing van een reeds gegeven schriftelijk bevel.

Zesde lid

Onderzoek in een geautomatiseerd werk vindt plaats met behulp van een technisch hulpmiddel. Omdat het onderzoek doorgaans via het internet wordt verricht, bestaat het technische hulpmiddel uit een softwareapplicatie door middel waarvan het onderzoek wordt verricht. Het is van groot belang dat de software voldoet aan eisen op het gebied van controleerbaarheid en integriteit, zodat de uitvoering van het onderzoek in een geautomatiseerd werk en de vastlegging van de gegevens te allen tijde kan worden getoetst.

De regels over de opslag, plaatsing en verstrekking van het technische hulpmiddel zullen worden opgenomen in het Besluit technische hulpmiddelen strafvordering. Deze algemene maatregel van bestuur 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 direct afluisteren van communicatie (artikelen 126l, 126s en 126zf Sv) en het aftappen van communicatie zonder medewerking van de aanbieder (artikelen 126m, 126t en 126zg Sv). Het Besluit bevat regels over de opslag, verstrekking, plaatsing en verwijdering van camera's en richtmicrofoons. Daarnaast bevat het Besluit technische eisen voor deze hulpmiddelen. Aanvullend op de normen voor de camera en de richtmicrofoon zullen regels worden vastgelegd voor de opslag, plaatsing en verstrekking van de softwareapplicatie en de technische eisen voor de softwareapplicatie die kan worden gebruikt voor onderzoek in een geautomatiseerd werk. Daarbij zullen de volgende uitgangspunten worden gehanteerd:

De opslag, verstrekking en plaatsing van de software vindt uitsluitend plaats door de door de korpschef aangewezen opsporingsambtenaren. De softwareapplicatie dient te zijn gecertificeerd. De eisen voor de certificatie worden neergelegd in het Besluit technische hulpmiddelen strafvordering. Dit brengt met zich mee dat de mogelijkheid bestaat om technische hulpmiddelen van verschillende leveranciers te betrekken, op voorwaarde dat deze middelen aan de wettelijke eisen voldoen.

Van belang is 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. 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. De softwareapplicatie dient te worden toegepast binnen de grenzen van de bevoegdheid; andere functionaliteiten worden niet ingeschakeld en geïnstalleerd in het geautomatiseerde werk waarin het onderzoek plaatsvindt.

De werking van de software wordt gelogd. Dit houdt in dat gegevens worden vastgelegd over het verrichten van bepaalde onderzoekshandelingen, het toepassen van de maatregel van de ontoegankelijkmaking van gegevens of het inzetten van bepaalde afzonderlijke bijzondere opsporingsbevoegdheden met betrekking tot de gegevens van het geautomatiseerde werk.

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 op dit moment worden gedacht aan een versleuteling met een cryptografische sterkte van tenminste 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 van 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 Nationale 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 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 betreffende 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.

Artikel II, onderdeel D

Artikel 125k

Eerste lid

In het thans geldende artikel 125k Sv is de bevoegdheid opgenomen tot het richten van een bevel aan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de beveiliging van een geautomatiseerd werk, tot het verschaffen van toegang tot het geautomatiseerde werk of delen daarvan. Omdat dit artikel is opgenomen in de zevende afdeling van Titel IV van het Wetboek van Strafvordering ('Doorzoeking ter vastlegging van gegevens') is een decryptiebevel mogelijk in het geval van een doorzoeking ter vastlegging van gegevens of een netwerkzoeking. Met dit wetsvoorstel wordt voorgesteld om een bevoegdheid tot onderzoek in een geautomatiseerd werk op te nemen in het Wetboek van Strafvordering. Ook bij de toepassing van een dergelijke bevoegdheid kan het noodzakelijk zijn dat aan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de beveiliging van het geautomatiseerde werk, een decryptiebevel kan worden gericht. Daarvoor kan worden gedacht aan de afzender van een versleuteld bericht, de netwerkbeheerder, de aanbieder van een communicatiedienst waarbij de communicatie wordt versleuteld of een aanbieder die op het internet diensten aanbiedt op het gebied van de versleuteling van (opgeslagen) gegevens. Met de voorgestelde aanpassing van het eerste lid van artikel 125k wordt in deze mogelijkheid voorzien.

Derde lid

In dit lid is vastgelegd dat een decryptiebevel in beginsel niet aan de verdachte kan worden gericht. In het algemeen deel van deze toelichting is de wenselijkheid van een decryptiebevel aan de verdachte aan de orde gekomen. Een dergelijk bevel is mogelijk in het geval van verdenking van het maken van een beroep of gewoonte van het bezit, de vervaardiging of de verspreiding van kinderpornografie en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens. Met de voorgestelde wijziging van dit lid wordt in die mogelijkheid voorzien.

In dit lid is tevens geregeld dat artikel 96a Sv van overeenkomstige toepassing is. Dit betreft de bevoegdheid van een persoon die bevoegd is tot verschoning, niet aan een decryptiebevel te voldoen. De uitzondering voor een verschoningsgerechtigde blijft onverkort gelden.

Vierde lid

In dit lid wordt voorgesteld dat, ingeval van verdenking van bepaald aangewezen ernstige strafbare feiten de officier van justitie aan de verdachte een decryptiebevel kan richten. Voor de toelichting op het decryptiebevel kan worden verwezen naar het algemeen deel van deze toelichting. De officier van justitie geeft het bevel niet dan nadat de verdachte in de gelegenheid is gesteld te worden gehoord. In het kader van het verhoor zal de verdachte in de gelegenheid kunnen worden gesteld medewerking te verlenen aan het verlenen van toegang tot het geautomatiseerde werk of het ontsleutelen van de desbetreffende gegevens. De verdachte is bevoegd zich bij het horen door een raadsman te doen bijstaan. De verdachte moet op deze bevoegdheid worden gewezen.

Vijfde lid

In dit lid is geregeld welke gegevens in het decryptiebevel aan de verdachte moeten zijn opgenomen. Het decryptiebevel is schriftelijk en dient de nodige informatie te bevatten zodat de verdachte kan begrijpen wat er precies van hem wordt verwacht en de rechter-commissaris in staat wordt gesteld te komen tot een zorgvuldige beoordeling van de vordering van de officier van justitie van een machtiging. Dit betreft in de eerste plaats het misdrijf en de naam van de verdachte (onderdeel a). Dit spreekt voor zichzelf. Dit betreft in de tweede plaats de feiten en omstandigheden waaruit blijkt dat de wettelijke voorwaarden voor een decryptiebevel zijn vervuld (onderdeel b). Dit behelst de aard van de verdenking, de ernst van de desbetreffende strafbare feiten en het onderzoeksbelang dat dringend vordert dat een decryptiebevel wordt gegeven aan de verdachte. Dit betreft in de derde plaats een zo nauwkeurig mogelijke aanduiding van de het geautomatiseerde werk, de gegevensdrager of de te ontsleutelen gegevens en de termijn waarbinnen, alsmede de wijze waarop de toegang dient te worden verschaft (onderdeel c). Voor de inhoud van de onderdelen b en c kan worden verwezen naar het algemeen deel van deze toelichting (paragraaf 4.3).

De officier van justitie geeft het bevel niet dan nadat de degene tot wie de vordering is gericht in de gelegenheid is gesteld te worden gehoord. Degene tot wie de vordering is gericht is bevoegd zich bij het horen te doen bijstaan door een raadsman. Degene tot wie de vordering is gericht moet op deze bevoegdheid worden gewezen.

Zesde en zevende lid

De officier van justitie heeft voor een decryptiebevel aan de verdachte een schriftelijke machtiging van de rechter-commissaris. In het zevende lid is omschreven op welke wijze de verdachte uitvoering dient te geven aan een decryptiebevel. De medewerking van de verdachte kan bestaan uit het ter beschikking stellen van de benodigde kennis omtrent de beveiliging of het daadwerkelijk verschaffen van toegang tot de versleutelde gegevens door de verdachte. Hiervoor kan worden verwezen naar het algemeen deel van deze toelichting.

Artikel II, onderdeel E

Dit onderdeel betreft de wijziging van de artikelen 125m, 125n en 125o Sv in verband met het onderzoek in een geautomatiseerd werk.

In artikel 125m Sv is geregeld dat indien een doorzoeking leidt tot vastlegging of ontoegankelijkmaking van gegevens, zo spoedig mogelijk aan de betrokkene schriftelijk mededeling wordt gedaan van de vastlegging of ontoegankelijkmaking en van de aard van de vastgelegde of ontoegankelijk gemaakte gegevens. Dit betreft de zogenaamde notificatieplicht, die voor de bijzondere opsporingsbevoegdheden is geregeld in artikel 126bb Sv.

Met de voorgestelde wijziging van het eerste lid wordt geregeld dat de betrokkene wordt geïnformeerd over het onderzoek in een geautomatiseerd werk. Dit is doorgaans de verdachte. Niet

uitgesloten is dat een geautomatiseerd werk bij meerdere personen in gebruik is, de mededelingsplicht bestaat ten opzichte van de burger op wiens rechten inbreuk wordt gemaakt. 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. Met de voorgestelde wijziging van het tweede lid wordt deze mogelijkheid ook geboden 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.

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 onderzoek in een geautomatiseerd werk. Dit vereist aanpassing van artikel 125n Sv. Op grond van de regeling worden de vastgelegde gegevens vernietigd zodra blijkt dat zij van geen betekenis zijn voor het strafvorderlijk onderzoek dat tot vastlegging heeft geleid. De officier van justitie kan bepalen dat de vastgelegde gegevens 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 (artikel 125n, derde lid, Sv.). Dit laatste betreft de gegevensverwerking door een criminele inlichtingen eenheid van de politie of een bijzondere opsporingsdienst.

Tenslotte wordt voorgesteld de redactie van artikel 125o Sv aan te passen, zodat de regeling van de ontoegankelijkmaking van gegevens van toepassing op de gegevens die zijn vastgelegd tijdens een onderzoek in een geautomatiseerd werk. 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

Artikel II, onderdeel F

In dit onderdeel wordt voorgesteld artikel 125p aan het Wetboek van Strafvordering toe te voegen. Dit artikel wordt – in aanvulling op paragraaf 3 van het algemeen deel van de toelichting – hieronder nader toegelicht.

Eerste lid

In dit lid is vastgelegd dat de officier van justitie, in geval van verdenking van een strafbaar feit, 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 strafbaar 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 als zij inmiddels zijn verspreid, daarvan volledig te verwijderen. 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.

Het bevel zal, als direct optreden jegens degene die de beschikking heeft over het geautomatiseerde werk met gebruikmaking 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 gevraagde gegevens in Nederland worden gehost zal dit in de eerste plaats de hosting provider zijn. In geval het materiaal in het buitenland wordt gehost en ontoegankelijkmaking noodzakelijk is, kan het bevel tot de access provider worden gericht. De kosten en inspanningen die ontoegankelijkmaking in het algemeen met zich brengen aan de kant van de aanbieder is een factor die bij het bevel mede betrokken moet worden: hem kan op grond

van het eerste lid immers alleen worden bevolen dat hij alle redelijkerwijs van hem te vergen maatregelen treft om gegevens ontoegankelijk te maken.

De officier van justitie geeft het bevel niet dan nadat de degene tot wie de vordering is gericht in de gelegenheid is gesteld te worden gehoord. Degene tot wie de vordering is gericht is bevoegd zich bij het horen te doen bijstaan door een raadsman. Degene tot wie de vordering is gericht moet op deze bevoegdheid worden gewezen.

Tweede lid

Het bevel moet voldoen aan een aantal eisen die in dit lid zijn opgenomen. Allereerst zal het bevel duidelijk maken welk strafbaar feit het betreft en zo mogelijk de naam van de verdachte. Gelet op de mogelijkheden die het internet biedt om de werkelijke identiteit te verhullen, zal het niet altijd mogelijk zijn om de (identiteit van de) verdachte te achterhalen. In dat geval kan worden volstaan met een zo nauwkeurige mogelijke aanduiding (onderdeel a).

Het bevel zal ook duidelijkheid moeten verschaffen over de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens nodig is om het strafbaar 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 lid, Sv van overeenkomstige toepassing verklaard. Op grond van het derde lid 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 ontoegankelijk worden gemaakt door middel van verwijdering van de gegevens, 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.

Vierde lid

De officier van justitie heeft 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 rechtshandhaving, de belangen van degene die de gegevens op het internet heeft gepubliceerd, alsmede de belangen van de aanbieder indien het bevel tot hem is gericht. Ten behoeve van een zorgvuldige beoordeling van het bevel van de officier van justitie door de rechter-commissaris is het geraden dat de betrokken partijen worden gehoord voordat de officier van justitie een machtiging vordert. Hiervoor gelden geen termijnen, de officier van justitie zal hierbij rekening kunnen houden met de omstandigheden van het betreffende geval. 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 G

De artikelen 126n en 126u Sv betreffende de bevoegdheid tot het vorderen van gegevens over een gebruiker van een communicatiedienst en het communicatieverkeer met betrekking tot die gebruiker. Deze gegevens worden ook aangeduid als verkeersgegevens. Met de Wet vorderen gegevens zijn specifieke bevoegdheden voor het vorderen van gegevens opgenomen in de zevende en achtste afdeling van Titel IVA van het Wetboek van Strafvordering. In deze gevallen wordt de mogelijkheid geboden van een mondelinge vordering. In het geval van een mondelinge vordering stelt de opsporingsambtenaar of de officier van justitie de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht (artikelen 126nc, vijfde lid, 126nd, vierde lid, 126ne, eerste lid, 126nf, vierde lid, 126ng, vijfde lid, 126uc, tweede lid, 126ud, tweede lid, 126ue, tweede lid, 126uf, tweede lid, 126ug, vijfde lid, Sv).

Op basis van de geldende wettelijke regels is de situatie ontstaan dat een vordering aan een aanbieder van een communicatiedienst tot het verstrekken van andere gegevens dan verkeersgegevens, op grond van de artikelen 126n en 126u Sv, mondeling kan worden gedaan. Voor een vordering tot het verstrekken van verkeersgegevens is dit echter niet mogelijk. Dit is in de praktijk niet goed werkbaar. Daarom wordt voorgesteld om voor de bevoegdheid van het vorderen van verkeersgegevens door de officier van justitie expliciet de mogelijkheid te bieden van een mondelinge vordering van verkeersgegevens. In het geval van een mondelinge vordering stelt de officier van justitie de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.

Artikel II, onderdeel H

De artikelen 126na en 126ua Sv betreffende de bevoegdheid tot het vorderen van gegevens ter zake van naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker van een communicatiedienst. Deze gegevens worden ook aangeduid als gebruikersgegevens. Ook voor de vordering van gebruikersgegevens geldt dat de wettelijke bevoegdheid niet voorziet in de mogelijkheid van een mondelinge vordering van deze gegevens. Hiermee wordt afgeweken van het stelsel van het vorderen van gegevens, in de zevende en achtste afdeling van Titel IVA van het Wetboek van Strafvordering, waarin wel in een dergelijke vordering wordt voorzien. Hiervoor kan

ook worden verwezen naar de toelichting op artikel II, onderdeel G. In het geval van een mondelinge vordering stelt de opsporingsambtenaar de vordering achteraf op schrift en verstrekt deze binnen drie dagen nadat de vordering is gedaan aan degene tot wie de vordering is gericht.

Artikel II, onderdeel I

In Titel VB van het Eerste Boek van het Wetboek van Strafvordering zijn bijzondere bevoegdheden tot opsporing van terroristische misdrijven opgenomen. In artikel 126zh, tweede lid, Sv is de bevoegdheid van de officier van justitie opgenomen om, in geval van aanwijzingen van een terroristisch misdrijf, een vordering te doen tot het verstrekken van verkeersgegevens. Met de voorgestelde wijziging van dit artikel wordt de mogelijkheid geboden van een mondelinge vordering van dergelijke gegevens. Hiervoor kan worden verwezen naar de toelichting op artikelen 126n en 126u Sv (artikel II, onderdeel G).

Artikel II, onderdeel J

Dit betreft de vordering van gebruikersgegevens ingeval van aanwijzingen van een terroristisch misdrijf. In artikel 126zi Sv is de bevoegdheid van de opsporingsambtenaar opgenomen om, ingeval van aanwijzingen van een terroristisch misdrijf, een vordering te doen tot het verstrekken van identificerende gegevens. Voor de toelichting op dit artikel kan worden verwezen naar de toelichting op de artikelen 126na en 126ua Sv (artikel II, onderdeel G) en artikel 126zh, tweede lid, Sv (artikel II, onderdeel I).

Artikel II, onderdeel K

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 L

In artikel 354, derde lid, Sv wordt geregeld dat in het geval dat de rechtbank een veroordeling, vrijspraak of ontslag van alle rechtsvervolgning uitspreekt, tevens een beslissing wordt genomen over het bevel tot het ontoegankelijk maken 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 M

Eerste lid, onderdeel a

Dit lid betreft de mogelijkheid voor belanghebbenden om zich te beklagen over een decryptiebevel aan de verdachte. Op grond van de huidige wettelijke regeling kunnen belanghebbenden zich beklagen over de vordering tot het ontsleutelen van gegevens, op grond van de artikelen 125k, tweede lid, en 126nh en 126uh, eerste lid, Sv. De ratio daarvan is dat het gebruik van gegevens in een geautomatiseerd werk dikwijls privacygevoelige of anderszins vertrouwelijke informatie betreft. Daarom zal naast een ieder die recht op teruggave van gegevens(bestanden) heeft ook degene die door het publiek worden van gegevens in zijn belangen wordt geschaad als belanghebbende kunnen worden aangemerkt. Het ligt in rede om de mogelijkheid voor belanghebbenden om zich te beklagen over het ontsleutelen van gegevens, ook te laten gelden voor het decryptiebevel aan een verdachte. Als naar het oordeel van het gerecht terecht wordt geklaagd over de kennisneming of het gebruik van gegevens dan zal het gerecht last geven het gewraakte gebruik of de gewraakte kennisneming te stoppen. Vanwege het spoedeisende karakter van de beslissing is in dit onderdeel vastgelegd dat het gerecht zo spoedig mogelijk op het beklag beslist.

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.

Dit lid bevat tevens het herstel van enkele omissies. In de eerste plaats wordt artikel 552a Sv 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 opnemings 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). Zoals hierboven is opgemerkt, is daarbij 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 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 het ontoegankelijk maken van gegevens, op grond van het voorgestelde artikel 125p Sv. Met het nieuwe derde 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.

Vierde lid

Dit betreft een aanvulling van dit lid met het decryptiebevel en 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.

Achtste lid

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

Artikel II, onderdeel N

Dit onderdeel betreft reparatie van artikel 592, tweede lid, Sv. 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.

De Minister van Veiligheid en Justitie,