Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

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

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 2 juni 2014 en het nader rapport d.d. 16 december 2015, aangeboden aan de Koning door de Staatssecretaris van Veiligheid en Justitie. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Bij Kabinetsmissive van 3 maart 2014, no. 2014000432, heeft Uwe Majesteit, op voordracht van de Minister van Veiligheid en Justitie, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), met memorie van toelichting.

Doel van het wetsvoorstel is versterking van het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit[2] en aanpassing daarvan aan de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. Daarnaast wordt aanpassing beoogd van het instrumentarium van politie en justitie ten behoeve van de opsporing en vervolging met behulp van een geautomatiseerd werk. Vanwege het voorgaande worden strafvorderlijke bevoegdheden uitgebreid en nieuwe strafbepalingen geïntroduceerd, waaronder de bevoegdheid om een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen. Daarbij kunnen onder meer gegevens worden overgenomen of ontoegankelijk gemaakt, kan observatie worden toegepast en kan communicatie worden afgetapt. Ook introduceert het wetsvoorstel de bevoegdheid tot het geven van een bevel aan een verdachte om versleutelde elektronische gegevens toegankelijk te maken (decryptiebevel). Het wetsvoorstel verruimt daarnaast de strafbaar-

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

[2] Computercriminaliteit betreft het plegen van strafbare feiten met behulp van dan wel gericht op een geautomatiseerd werk.

kst-34372-4
ISSN 0921 - 7371
's-Gravenhage 2015

stellingen van het corrumperen van minderjarigen en «grooming» (het ongewenst benaderen van minderjarigen op het internet met het oogmerk ontuchtige handelingen met hen te plegen). Voorgesteld wordt dat bij de bestrijding van grooming opsporingsambtenaren die zich als een minderjarige voordoen (zogeheten «lokpubers») kunnen worden ingezet. Ten slotte omvat het voorstel de strafbaarstelling van online handelsfraude, heling van computergegevens en het wederrechtelijk overnemen van niet-openbare gegevens. De voorgestelde regeling heeft een andere en veel bredere reikwijdte dan het geval was bij de Wet computercriminaliteit en Wet computercriminaliteit II, die in 1993 respectievelijk 2006 in werking traden.[3]

De Afdeling merkt op dat de voortschrijdende ontwikkeling van communicatietechnologie zowel de overheid als de samenleving voortdurend voor nieuwe vragen omtrent privacy en controle stelt. Volgens de toelichting schieten de bestaande opsporingsbevoegdheden tekort om aan bepaalde ontwikkelingen en knelpunten op het gebied van computercriminaliteit het hoofd te kunnen bieden. Het betreft met name de toenemende versleuteling van elektronische gegevens en het gebruik van draadloze netwerken en cloudcomputingdiensten, waarbij gegevens kunnen worden opgeslagen op een locatie die de gebruiker niet altijd bekend is. De Afdeling onderschrijft dat bij de bestrijding van ernstige misdrijven binnen de grenzen van het grondwettelijk en verdragsrechtelijk beschermde recht op eerbiediging van de persoonlijke levenssfeer ook van de nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt. Het voorstel is in zoverre noodzakelijk. De Afdeling acht echter de voorgestelde bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk onvoldoende gedifferentieerd naar de mate van de ingrijpendheid van die inbreuk op de persoonlijke levenssfeer. Daarmee staat de proportionaliteit van de voorgestelde bevoegdheid, zoals bedoeld in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), niet vast. Deze bevoegdheid behoeft naar het oordeel van de Afdeling derhalve differentiatie.
De voorgestelde bevoegdheid geeft de Afdeling tevens aanleiding voor een opmerking met een breder bereik dan het onderhavige voorstel. Zij adviseert te voorzien in structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd.

Ten aanzien van het decryptiebevel aan verdachten adviseert de Afdeling de noodzaak en vooral de effectiviteit ervan dragend te motiveren of anders dit onderdeel van het wetsvoorstel te schrappen. Voorts maakt de Afdeling opmerkingen met betrekking tot rechtvaardiging van de inbreuk die het bevel maakt op het nemo teneturbeginsel gelet op de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM). De voorgestelde bevoegdheid staat op gespannen voet met een tweetal uitspraken van het EHRM.[4]

De Afdeling is van oordeel dat het voorstel in verband met het bovenstaande nader dient te worden overwogen.

---

[3] Met de Wet computercriminaliteit (Stb. 1993, 33) is het Wetboek van Strafvordering uitgebreid met bevoegdheden betreffende onderzoek in geautomatiseerde werken en is de strafbaarstelling van computervredebreuk in het Wetboek van Strafrecht opgenomen. Met de Wet computercriminaliteit II (Stb. 2006, 300) is het Cybercrimeverdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2004, 290), geïmplementeerd.

[4] EHRM 21 december 2000, *Heaney en McGuinness t. Ierland*, nr. 34720/97. EHRM 21 december 2000, *Quinn t. Ierland*, nr. 36887/97.

Blijkens de mededeling van de Directeur van Uw kabinet van 3 maart 2014, nr. 2014000432, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 2 juni 2014, nr. W03.14.0055/II, bied ik U hierbij aan.

Het ontwerp geeft de Afdeling advisering aanleiding tot het maken van inhoudelijke opmerkingen. Deze opmerkingen worden hieronder besproken.

A. Heimelijk binnendringen in geautomatiseerd werk

Het voorstel omvat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk dat in gebruik is bij een verdachte. Daarbij wordt de vigerende definitie van «geautomatiseerd werk» aangepast, waardoor hieronder ieder apparaat valt dat op basis van een programma automatisch computergegevens verwerkt.[5] Hierbij kan worden gedacht aan in de toelichting genoemde voorbeelden als een computer, tablet of smartphone, de router waarmee een computer(netwerk) met het internet is verbonden of een USB-stick, maar ook aan een slimme meter, navigatiesysteem, geavanceerd sporthorloge of pacemaker.

De voorgestelde bevoegdheid is gebonden aan een aantal voorwaarden. Zij kan in de eerste plaats uitsluitend worden ingezet bij een verdenking van een misdrijf zoals omschreven in artikel 67, eerste lid, Sv dat een ernstige inbreuk op de rechtsorde oplevert.[6] Ten tweede is de bevoegdheid gekoppeld aan wettelijk omschreven strafvorderlijke doeleinden.[7] In de derde plaats kan de bevoegdheid uitsluitend worden ingezet op bevel van de officier van justitie en na schriftelijke machtiging door de rechter-commissaris. Deze machtiging geldt ten hoogste voor de duur van vier weken, en kan telkens voor maximaal vier weken worden verlengd.

De wijze waarop het technisch middel voor het heimelijk binnendringen wordt ingezet, is in het voorstel niet omschreven. De ingezette methode staat niet vast; deze is mede afhankelijk van de mogelijkheden van het binnen te dringen geautomatiseerd werk. Al naar gelang de machtiging van de rechter-commissaris en het bevel van de officier van justitie worden gps-gegevens uitgelezen, gegevens overgenomen, wordt meegekeken met handelingen op het apparaat of worden webcam en microfoon aangezet en communicatie of beelden opgenomen. De voorgestelde bevoegdheid vertoont daarmee – afhankelijk van de wijze van toepassing – overeenkomsten met reeds bestaande opsporingsbevoegdheden zoals doorzoeking ter vastlegging van gegevens, stelselmatige observatie en het opnemen van vertrouwelijke communicatie. Voor deze opsporingsbevoegdheden geldt dat met de inzet ervan een inbreuk wordt gemaakt op de persoonlijke levenssfeer zoals bedoeld in de Grondwet en het EVRM. Deze inbreuk betreft in het voorstel niet alleen de persoonlijke levenssfeer van de verdachte als gebruiker van het geautomatiseerd werk, maar tevens de persoonlijke levenssfeer van mogelijke andere gebruikers van het binnen te dringen geautomatiseerd werk alsmede van diegenen wier privacygevoelige gegevens behoren tot de gegevens die worden doorzocht en overgenomen.

---

[5] Voorgesteld artikel 80sexies Sr.

[6] Misdrijven waarop in de meeste gevallen een maximum gevangenisstraf van vier jaar is gesteld, en waarvoor voorlopige hechtenis mogelijk is.

[7] Genoemd in het voorgestelde artikel 125ja, eerste lid, Sv.

1. Differentiatie en verhouding tot het EVRM

a. Differentiatie

Het heimelijk binnendringen in een geautomatiseerd werk kan naar het oordeel van de Afdeling een grote inbreuk op de persoonlijke levenssfeer vormen, die vergelijkbaar is met het betreden van een woning met het oog op het opnemen van vertrouwelijke communicatie (artikel 126l, tweede lid, Sv): veelal immers behoort de smartphone of tablet in zekere zin tot een intieme sfeer waarin onderdelen van het persoonlijke en professionele leven samenkomen.[8] Het heimelijk op afstand, langdurig doorzoeken van een geautomatiseerd (net)werk, waarbij zowel historische, actuele als toekomstige gegevens kunnen worden overgenomen, is zeer ingrijpend. Op grond van het voorgestelde artikel 125ja, eerste lid, onderdeel b, Sv kunnen bijvoorbeeld fotobestanden en de financiële administratie worden doorzocht, kan opgeslagen emailverkeer worden overgenomen, kan het gebruik van het internet worden achterhaald en kunnen gegevens over andere vormen van communicatie worden overgenomen.

Het binnendringen in een geautomatiseerd werk kan ook minder ingrijpend zijn, bijvoorbeeld indien dat enkel geschiedt met het oog op het vaststellen van de identiteit van een geautomatiseerd werk of van de locatie van een gebruiker ervan door het aflezen van gps-gegevens (het voorgestelde artikel 125ja, eerste lid, onderdeel a, Sv). Deze bevoegdheid sluit wat betreft de ernst van de inbreuk op de persoonlijke levenssfeer enigszins aan op de bestaande bevoegdheid in artikel 126nb Sv tot het aanwenden van scanapparatuur met het doel om toepassing mogelijk te maken van de bevoegdheden tot het vorderen van verkeersgegevens (artikel 126n Sv) of tot het opnemen van communicatie (artikel 126m Sv).[9]

Een en ander betekent dat de inbreuk op de persoonlijke levenssfeer op basis van het voorgestelde artikel 125ja Sv kan verschillen. Het voorstel maakt echter geen enkel onderscheid naar de mate van de ingrijpendheid van die inbreuk op de persoonlijke levenssfeer. Op grond van het voorstel gelden in alle gevallen dezelfde voorwaarden: er moet in elk geval sprake zijn van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat een ernstige inbreuk op de rechtsorde vormt.

Naar het oordeel van de Afdeling sluit deze generieke benadering niet aan bij de verschillen in de mate van ingrijpendheid waarmee inbreuken op de persoonlijke levenssfeer gemaakt wordt en de daarmee samenhangende verschillen in te stellen voorwaarden aan de toepassing van opsporingsbevoegdheden op basis van het geldende strafvorderlijke stelsel.
Zoals reeds vermeld wordt bij de minder ingrijpende bevoegdheden, namelijk het vaststellen van de identiteit van een geautomatiseerd werk of van de locatie van een gebruiker ervan door het aflezen van gps-gegevens (het voorgestelde artikel 125ja, eerste lid, onderdeel a, Sv), aangesloten bij de bestaande bevoegdheid tot het aanwenden van scanapparatuur om

---

[8] Het EHRM hanteert de term «intiem» in het kader van inbreuken op het recht op bescherming van de persoonlijke levenssfeer als bedoeld in artikel 8 EVRM. Vgl. bijvoorbeeld EHRM 10-05-2011, 48009/08.

[9] Voor het aanwenden van scanapparatuur met het oog op het mogelijk maken van deze verschillende bevoegdheden, gelden verschillende voorwaarden: indien een IMSI-catcher wordt ingezet teneinde de bevoegdheid tot het vorderen van verkeersgegevens (artikel 126n Sv) mogelijk te maken, zal er sprake moeten zijn van een verdenking als omschreven in artikel 67, eerste lid, Sv. Indien zo'n scanner wordt ingezet om de bevoegdheid tot opnemen van (tele)communicatie mogelijk te maken (artikel 126m Sv), zal er bovendien sprake moeten zijn van een misdrijf dat gelet op de aard of samenhang met andere misdrijven een ernstige inbreuk op de rechtsorde maakt.

verkeersgegevens te vorderen of communicatie op te nemen. Naar het oordeel van de Afdeling kan bij deze bevoegdheden worden volstaan met de thans voorgestelde voorwaarden. Ook bij de bevoegdheden tot het aftappen van communicatie en de stelselmatige observatie (artikel 125ja, eerste lid, onderdelen d en e, Sv) kan worden aangesloten bij de bestaande voorwaarden en waarborgen, zoals voorgesteld.[10]
Betreft het echter het heimelijk op afstand doorzoeken van een geautomatiseerd werk en/of het overnemen van gegevens, dan is naar het oordeel van de Afdeling sprake van een beduidend zwaarder ingrijpen in de persoonlijke levenssfeer, dat vergelijkbaar is met de toepassing van de bestaande opsporingsbevoegdheid wanneer daarbij heimelijk wordt binnengetreden in een woning met het oog op het opnemen van vertrouwelijke communicatie. Aanwending van deze opsporingsbevoegdheid is beperkt tot gevallen waarbij een verdenking bestaat van misdrijven waarop gevangenisstraf van 8 jaar of meer is gesteld.[11] De Afdeling acht het passend dat eenzelfde drempel zou komen te gelden voor de meest ingrijpende vormen van de voorgestelde bevoegdheid tot heimelijk binnendringen in een geautomatiseerd werk. Daarbij zijn met het oog op de mate van ingrijpendheid drie aspecten van belang. Op de eerste plaats betreft het voorgestelde artikel 125ja, eerste lid, onderdeel b, Sv -anders dan het bestaande artikel 125i Sv dat de doorzoeking van een geautomatiseerd werk regelt- het heimelijk en op afstand binnendringen van een geautomatiseerd werk. Op de tweede plaats kan gedurende langere tijd niet alleen communicatie worden opgenomen[12], maar bovendien kunnen (versleutelde) bestanden, andere communicatie en internetgebruik door of op het geautomatiseerd werk worden onderzocht, vastgelegd en opgenomen. Op de derde plaats ziet het voorstel ook op toekomstige gegevens, die na de afgifte van het bevel worden «verwerkt».[13]

b. Verhouding tot het EVRM

Met betrekking tot het aanwenden van heimelijke opsporingsbevoegdheden heeft het EHRM vastgesteld aan welke criteria deze moet voldoen. Daarbij stelt het EHRM voorop dat de (regeling van de) toepassing van dergelijke heimelijke opsporingsbevoegdheden een inbreuk maakt op de persoonlijke levenssfeer in de zin van artikel 8 EVRM.[14] Inbreuken zijn mogelijk, voor zover zij zijn voorzien bij de wet en in een democratische samenleving noodzakelijk zijn in het belang van onder meer het voorkomen van strafbare feiten.[15] Gewaarborgd dient te zijn dat een gemaakte inbreuk op het recht op bescherming van de privésfeer proportioneel is ten opzichte van het doel van de inbreuk en dat er geen minder ingrijpende middelen voorhanden zijn waarmee hetzelfde doel kan worden bereikt.

Uit het gestelde onder a volgt naar het oordeel van de Afdeling dat in de voorgestelde bepaling onvoldoende wordt gedifferentieerd tussen de uiteenlopende aard van de inbreuken op de persoonlijke levenssfeer.

---

[10] De ontoegankelijkmaking van gegevens (voorgestelde artikel 125ja, onderdeel c, Sv) is in deze adviesopmerking niet genoemd, maar wordt afzonderlijk besproken in punt 6, onder b, van dit advies.
[11] Vgl. artikel 126l, tweede lid, Sv.
[12] Vergelijk het geldende artikel 126l Sv. Op grond daarvan is het bijvoorbeeld mogelijk om een woning te betreden om een «bug» in een computer te plaatsen voor het registeren van toetsaanslagen en muisklikken.
[13] Memorie van toelichting, paragraaf 2.2, De reikwijdte van de voorgestelde bevoegdheid en de plaatsing in het Wetboek van Strafvordering, derde alinea.
[14] EHRM 6 september 1978, *Klass t. Duitsland*, nr. 5029/71 § 41, EHRM 2 augustus 1984, *Malone t. VK*, nr. 8691/79, § 64, EHRM 2 september 2010, *Uzun t. Duitsland*, nr. 35623/05, §52.
[15] Artikel 8, tweede lid, EVRM.

Zoals hiervoor aangeduid, ligt het in de rede om in de wet zwaardere voorwaarden te stellen aan de toepassing van een bevoegdheid naarmate de bevoegdheid een zwaardere inbreuk maakt op de persoonlijke levenssfeer in de zin van artikel 8 EVRM. Nu deze differentiatie in het voorstel zoals het thans voorligt, ontbreekt, staat in het bijzonder de proportionaliteit zoals bedoeld in het EVRM gelet op de jurisprudentie van het EHRM niet vast. Hierbij merkt de Afdeling op dat voor zover sprake is van uitvoering van Unierecht, het Handvest van de grondrechten van de Europese Unie van toepassing is dat eveneens eisen stelt ten aanzien van de proportionaliteit.[16]

c. Conclusie

De Afdeling stelt vast dat de voorwaarden om van de voorgestelde bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk gebruik te maken niet differentiëren naar de mate waarin een inbreuk wordt gemaakt op de persoonlijke levenssfeer. In zoverre sluiten de voorwaarden niet goed aan bij het bestaande stelsel van strafvorderlijke bevoegdheden. Ingeval sprake is van bijvoorbeeld het bepalen van de identiteit of van de locatie van het geautomatiseerd werk of de gebruiker, zijn de voorgestelde waarborgen naar het oordeel van de Afdeling passend. Bij het binnendringen met het oog op het aftappen van communicatie of stelselmatige observatie, kan eveneens worden volstaan met de voorwaarden zoals voorgesteld. Voor het binnendringen dat het meest ingrijpend is, zoals het doorzoeken van alle gegevens in het geautomatiseerd werk en het overnemen daarvan, acht de Afdeling evenwel aansluiting bij de voorwaarden voor de toepassing van de bijzondere opsporingsbevoegdheid tot opnemen van vertrouwelijke communicatie waarbij een woning wordt binnengedrongen, aangewezen.

Omdat de voorgestelde bevoegdheid onvoldoende differentieert naar de mate van de ingrijpendheid van die inbreuk op de persoonlijke levenssfeer, staat in het bijzonder de proportionaliteit zoals bedoeld in het EVRM niet vast.

De Afdeling adviseert gelet op het voorgaande het voorgestelde artikel 125ja, eerste lid, Sv aan te passen.

2. Systeemtoezicht

a. Het voorliggende voorstel

De Afdeling overweegt dat de ontwikkelingen in de communicatietechnologie het aan de ene kant eenvoudiger maken voor criminelen om hun daden te onttrekken aan het zicht van de overheid en zo de opsporing en vervolging van strafbare feiten te bemoeilijken. Aan de andere kant bieden deze ontwikkelingen grote mogelijkheden voor binnenlandse en buitenlandse inlichtingen- en opsporingsdiensten om strafbare feiten op te sporen en in het kader daarvan (gedragingen van) burgers die niet of nog niet als verdachte kunnen worden aangemerkt te controleren. Het huidige voorstel past wat dat betreft in een reeks ontwikkelingen zoals het toenemend gebruik van de telefoon- en internettap,[17] *de opslag van verkeersgegevens omtrent internet- en telefoongebruik,*[18] *de registratie en*

---

[16] Zie artikel 52, eerste lid, van het Handvest van de grondrechten van de Europese Unie en het arrest van het Hof van Justitie van 8 april 2014, Digital Rights Ireland (C-293/12 en C-594/12).

[17] G. Odinot e.a., *Het gebruik van de telefoon- en internettap in de opsporing*, WODC 2012, blz. 82.

[18] Ingevolge Richtlijn 2006/24/EG (Richtlijn betreffende gegevensbewaring), zie tevens HvJ EU 8 april 2014, C-293/12 en C-594/12.

opslag van kentekengegevens van burgers[19] en de toepassing van gezichts- en gedragsherkenningssoftware bij het cameratoezicht. De toepassing en reikwijdte van deze bevoegdheden en met name de omvang van de gegevensverwerking kan daarbij van invloed zijn op het vertrouwen van burgers in de overheid.[20] Dit vertrouwen is naar het oordeel van de Afdeling mede afhankelijk van het toezicht dat wordt gehouden op de toepassing van deze bevoegdheden.

De Afdeling wijst erop dat het EHRM in verschillende uitspraken over heimelijke opsporingsbevoegdheden het belang heeft onderstreept van de aanwezigheid van «adequate and effective guarantees against abuse».[21] Het EHRM maakt een onderscheid tussen de verschillende fasen van het onderzoek; de fase voorafgaand, tijdens en na de toepassing van bevoegdheden.
In het Wetboek van Strafvordering is in de fase voorafgaand aan de toepassing van opsporingsbevoegdheden een voorname rol weggelegd voor de rechter-commissaris. Met de inwerkingtreding van de Wet versterking positie rechter-commissaris[22] is de nadruk gelegd op diens toezichthoudende taak, te weten controle op de rechtmatigheid van de inzet van de opsporingsbevoegdheden.[23] In het voorstel is de controletaak van de rechter-commissaris echter beperkt tot de voorafgaande machtiging.[24] De rechter-commissaris toetst dus niet achteraf de aanwending van de opsporingsbevoegdheden. Tijdens de opsporing is de officier van justitie belast met het toezicht op de toepassing van de opsporingsbevoegdheid.

Indien het opsporingsonderzoek leidt tot een onderzoek ter terechtzitting, is het toezicht op de toepassing van bevoegdheden belegd bij de strafrechter, die de rechtmatigheid van de bewijsgaring in het vooronderzoek beoordeelt. Hij zal daarbij wat betreft het voorgestelde binnendringen in een geautomatiseerd werk met name zijn aangewezen op de bij de inzet van die bevoegdheid gegenereerde logbestanden.[25] De toelichting vermeldt een aantal waarborgen tegen oneigenlijk gebruik van de opsporingsbevoegdheden. «Doordat alle technische handelingen die door de opsporingsambtenaren van het technische team worden verricht, worden gelogd en deze handelingen bovendien hun weerslag vinden in een proces-verbaal, is achteraf altijd controle mogelijk op de integriteit van de werking van het technische hulpmiddel en van de informatie die met behulp daarvan is vergaard, zonder dat gevoelige informatie over de methode zelf wordt prijs gegeven. Op deze manier is het mogelijk om de ter terechtzitting gevoerde verweren over de integriteit van het verzamelde bewijsmateriaal te toetsen», aldus de toelichting.[26]

---

[19] Kamerstukken II, 33 542.
[20] Rapport WRR, *iOverheid*, blz. 204–205 en 230–231.
[21] EHRM 29 juni 2006, *Weber en Saravia t. Duitsland*, nr. 54943/00, §117, EHRM 10 februari 2009, *Iordachi t. Moldavië*, nr. 25198/02, §47 e.v., EHRM 28 juni 2007, *Association for European integration and human rights en Ekimdzhiev t.* Bulgarije, nr. 62540/00, §85.
[22] Stb. 2011, 600.
[23] Artikel 170, tweede lid, Sv: «De rechter-commissaris is in het bijzonder belast met de uitoefening van toezichthoudende bevoegdheden met betrekking tot het opsporingsonderzoek, ambtshalve in door de wet bepaalde gevallen en voorts op vordering van de officier van justitie of op verzoek van de verdachte of diens raadsman.»
[24] Betrokkenheid van de rechter-commissaris bij het verloop van het opsporingsonderzoek werd door de wetgever niet aangewezen geacht. Kamerstukken II 2009/10, 32 177, nr. 3, paragraaf 4.1.
[25] Memorie van toelichting, paragraaf 2.5. «De inzet van de bevoegdheid, III De afsluiting van het onderzoek in een geautomatiseerd werk.»
[26] Memorie van toelichting, paragraaf 2.5. «De inzet van de bevoegdheid, III De afsluiting van het onderzoek in een geautomatiseerd werk.»

De Afdeling merkt op dat de gegenereerde logbestanden slechts toegankelijk zijn voor specialisten. In de regel zullen de strafrechter, noch de officier van justitie en de advocaat deze zelfstandig, dat wil zeggen zonder hulp van een technisch deskundige, kunnen beoordelen. Daarbij zal voor een goed inzicht in de volledigheid van de logbestanden tevens inzicht nodig zijn in de methode waarmee is geïnfiltreerd.[27] Dit roept de vraag op of de bij de gerechtelijke procedure betrokkenen voldoende controle zullen kunnen uitoefenen op de daadwerkelijke aanwending van de opsporingsbevoegdheden. De toegankelijkheid en controleerbaarheid van deze loggegevens voor de verdachte en de verdediging spreken dan ook niet voor zich. Voorts kan een beoordeling van de logbestanden door de verdediging daardoor mogelijk achterwege blijven, nu met de ontcijfering daarvan substantiële kosten kunnen zijn gemoeid.

De Afdeling merkt voorts op dat de rechterlijke controle achteraf enkel waarborgen biedt in gevallen waarin de resultaten van een opsporingsonderzoek leiden tot een onderzoek ter terechtzitting. Bij een substantieel deel van de gevallen wordt niet tot vervolging overgegaan en blijft de toetsing achteraf beperkt tot een mededeling dat in het geautomatiseerd werk is binnengedrongen. Deze notificatieverplichting[28] speelt in de jurisprudentie van het EHRM een belangrijke rol.[29] De notificatieplicht wordt echter reeds lange tijd slechts op beperkte schaal nageleefd.[30] Evenmin bestaat een instantie waartoe men zich kan wenden met klachten omtrent de inzet van de desbetreffende opsporingsbevoegdheid.[31] Voorts merkt de Afdeling op dat in het voorstel de notificatieverplichting slechts deels geregeld is. Leidt de opsporingsbevoegdheid immers niet tot vastlegging of ontoegankelijkmaking van gegevens, dan blijft notificatie achterwege.[32] Hierdoor zal voor een substantieel deel van de gevallen waarin de opsporingsbevoegdheid is toegepast niet of nauwelijks controle achteraf bestaan. Het ontbreken van deze controle klemt te meer vanwege het ingrijpende karakter van de voorgestelde bevoegdheid. Voor toezicht op de wijze waarop de voorgestelde bevoegdheid is uitgevoerd, schiet slechts een – niet in alle gevallen toepasselijke – notificatieverplichting met een beroep op de civiele rechter als restrechter derhalve tekort.

De Afdeling adviseert in het licht van het voorgaande in de toelichting in te gaan op de controle achteraf op de toepassing van de voorgestelde bevoegdheden in gevallen die aan het toezicht door de rechter zijn onttrokken.

---

[27] De toelichting stelt hierover: «De voorgeschreven logging heeft geen betrekking op de gebruikte methode voor het binnendringen in een geautomatiseerd werk dan wel voor de toepassing van bepaalde bijzondere opsporingsbevoegdheden. Alsdan zou gevoelige opsporingsinformatie prijs gegeven worden, met als gevolg dat een methode onbruikbaar wordt. De logging van de gegevens maakt het mogelijk achteraf controle uit te oefenen op de integriteit van de werking van het technische hulpmiddel en van de informatie die met behulp daarvan is vastgelegd, zodat verweren over de integriteit van het verzamelde bewijsmateriaal kunnen worden getoetst.» memorie van toelichting, artikelsgewijze toelichting op artikel 125ja Sv.

[28] Vergelijk artikel 125m Sv voor de notificatie na een doorzoeking die leidt tot het vastleggen of ontoegankelijk maken van gegevens en artikel 126bb Sv voor de notificatie na de uitoefening van bijzondere opsporingsbevoegdheden.

[29] EHRM 28 juni 2007, *Association for European integration and human rights en Ekimdzhiev t.* Bulgarije, nr. 62540/00.

[30] Spapens, Siesling & de Feijter, *Brandstof voor de opsporing evaluatie, Wet bevoegdheden vorderen gegevens*, BJU 2011, blz. 99. Eerder in dezelfde zin Beijer e.a., *De Wet bijzondere opsporingsbevoegdheden, Eindevaluatie*, BJU 2004, blz. 145.

[31] Zaken die niet voor de strafrechter komen, zouden voorgelegd kunnen worden aan de civiele rechter als restrechter. De Afdeling veronderstelt echter dat dit niet vaak gebeurt, mede omdat de notificatieplicht onvoldoende wordt nageleefd. Spapens, Siesling & de Feijter, *Brandstof voor de opsporing evaluatie, Wet bevoegdheden vorderen gegevens*, BJU 2011, blz. 99.

[32] Zie artikel 125m Sv.

b. Structureel systeemtoezicht

Bij de inzet van opsporingsbevoegdheden waarbij gegevens worden verwerkt, zoals het opnemen van communicatie, wordt op de gegevensverwerking toezicht gehouden door het College bescherming persoonsgegevens (Cbp).[33] Daarmee wordt evenwel in veel gevallen nog geen toezicht gehouden op de rechtmatigheid en proportionaliteit van aanwending van de opsporingsbevoegdheid als zodanig. Het Cbp, dat notificatie ook een slechts geringe waarborg acht, heeft geadviseerd te voorzien in een controle-instrument waarmee direct en effectief toezicht wordt uitgeoefend op de wijze van uitvoering van de voorgestelde bevoegdheid, onder meer door middel van een verplichting tot regelmatig beschikbaar stellen van statistieken en overzichten. In reactie daarop vermeldt de toelichting dat zal worden onderzocht of structureel informatie kan worden verzameld over de toepassing van het onderzoek in een geautomatiseerd werk. Deze informatie zal dan openbaar kunnen worden gemaakt in de vorm van een statistische rapportage, naar het model van de jaarlijkse verstrekking van gegevens over het aftappen van telecommunicatie, aldus de toelichting.[34]

Gegeven de reeks ontwikkelingen op het gebied van wetgeving, zoals in het begin van deze paragraaf geduid, waarbij het voorliggende voorstel wederom voorziet in nieuwe (en in dit geval vergaande) bevoegdheden vanwege de voortschrijdende informatie- en communicatietechnologie kan niet om de vraag worden heengegaan naar de wenselijkheid van aanvullend toezicht op de toepassing van opsporingsbevoegdheden door politie en justitie in zaken waarbij van deze technologie gebruik is gemaakt en die niet hebben geleid tot een procedure voor de strafrechter.[35] Dit geldt temeer, daar de technologie zich verder zal blijven ontwikkelen en het van belang is dat het juridisch instrumentarium daarmee gelijke tred houdt. Juist om politie en justitie te kunnen blijven voorzien van adequate opsporings- en vervolgingsbevoegdheden, dienen – ook vanwege het vertrouwen van burgers in de overheid – de waarborgen navenant te zijn. Daarbij zij herhaald dat het in dezen niet alleen gegevens van en informatie over verdachten betreft maar ook van en over onschuldige burgers.
De Afdeling is van oordeel dat systeemtoezicht wenselijk is waarbij structureel wordt toegezien op de rechtmatige uitoefening van opsporingsbevoegdheden, waarbij door middel van informatie- en communicatietechnologie naar gegevens wordt gezocht en/of deze worden verkregen. Om systeemtoezicht uit te kunnen voeren, moet de toezichthoudende instantie naar het oordeel van de Afdeling toegang hebben tot individuele dossiers, ook al zal geen oordeel worden uitgesproken over individuele zaken. Het toezicht zal zich in het bijzonder kunnen richten op de noodzakelijkheid, proportionaliteit en subsidiariteit van de toepassing van de betreffende bevoegdheden. Een jaarlijkse openbare rapportage is daarbij aangewezen, waarbij bepaalde bij opsporingsbevoegdheden toegepaste methoden geheim zouden kunnen blijven. De toezichthoudende instantie zou naar aanleiding van dit structurele toezicht op systeemniveau aanbevelingen voor verbetering kunnen doen.
Voor zaken die niet zijn voorgelegd aan de rechter zou een dergelijke instantie klachten in individuele zaken kunnen onderzoeken.

Wat betreft de taken en bevoegdheden van de toezichthouder zou gekeken kunnen worden naar de regeling ten aanzien van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) die als

---

[33] Artikel 35 van de Wet politiegegevens.
[34] Memorie van toelichting, paragraaf 9. Adviezen over het wetsvoorstel.
[35] Zie ook Y. Buruma, *Toezicht op geheim onderzoek*, NJB 2007, 2005.

toezichthouder fungeert en tevens als klachtinstantie.[36] Ook buitenlandse toezichthoudende organen zouden mede als voorbeeld kunnen dienen.[37] Met betrekking tot de positionering kan eraan worden gedacht de toezichthoudende instantie onder te brengen bij het Openbaar Ministerie, waar de Centrale Toetsingscommissie al een rol in dezen vervult[38], maar daarbij externe elementen aan te brengen door middel van bijvoorbeeld een externe onafhankelijke voorzitter en (deels) bemensing met externe terzake deskundigen. Ter illustratie wijst de Afdeling op de voormalige Commissie Evaluatie Afgesloten Strafzaken.[39]

De Afdeling adviseert in de toelichting op het voorgaande in te gaan en geeft in overweging te voorzien in structureel systeemtoezicht op de rechtmatige uitoefening van de opsporingsbevoegdheden waarbij gebruik wordt gemaakt van informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd. De daartoe aangewezen instantie zou voor zaken die niet zijn voorgelegd aan de rechter tevens klachten in individuele zaken kunnen onderzoeken.

3. Plaatsing in titel IV van het Eerste Boek Sv

De essentie van de voorgestelde bevoegdheid is dat op afstand heimelijk een geautomatiseerd werk wordt onderzocht, dus zonder dat de verdachte daar kennis van krijgt. De Afdeling merkt op dat de voorgestelde bevoegdheid daarom in de kern samenhang vertoont met de bijzondere opsporingsbevoegdheden die zijn vervat in Titel IVA van het Eerste Boek Sv zoals stelselmatige observatie, inkijkoperaties, opnemen van vertrouwelijke communicatie (direct afluisteren) of onderzoek van communicatie door middel van geautomatiseerde werken (aftappen). De voorgestelde bevoegdheid past derhalve minder goed bij de regeling van de bijzondere dwangmiddelen, die (fysieke) doorzoeking van een computer ter vastlegging van gegevens betreffen (Titel IV van het Eerste Boek Sv). In de

---

[36] De CTIVD oefent toezicht achteraf uit op de rechtmatige uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002 alsmede de Wet veiligheidsonderzoeken. Ook heeft zij tot taak de betrokken Ministers te adviseren over de afhandeling van klachten over de AIVD en de MIVD. Het toezicht ziet in beginsel op alle activiteiten en maatregelen in de drie door het EHRM onderscheiden fasen met betrekking tot de taakuitvoering van inlichtingen- en veiligheidsdiensten. De Afdeling wijst er op dat de CTIVD toezicht houdt op bevoegdheden die niet onder rechterlijke controle staan. In zoverre is dat niet vergelijkbaar met de bevoegdheden in het voorliggende wetsvoorstel aangezien elke inzet daarvan kan leiden tot een gerechtelijke procedure met een rechterlijk oordeel. In dezen is dus wel van rechterlijke controle sprake.

[37] In het Verenigd Koninkrijk zijn specifieke toezichthoudende organen belast met het toezicht achteraf op de toepassing van bijzondere opsporingsbevoegdheden zoals aftappen en het decryptiebevel, namelijk de Interception of Communications Commissioner en de Chief Surveillance Commissioner. Het betreft brede toezichthoudende bevoegdheden. De Afdeling tekent daarbij wel aan dat de rechtspleging in het VK wezenlijk verschilt van die in Nederland en dat de positie van deze toezichthouders ook in de lokale context bezien moet worden.

[38] De toelichting vermeldt dat de officier van justitie, wil deze machtiging verkrijgen van de rechter-commissaris voor aanwending van de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk, eerst toestemming daartoe moet verkrijgen van de Centrale toetsingscommissie (CTC). Memorie van toelichting, paragraaf 2.6. Dit interne adviesorgaan, samengesteld uit leden van het OM en de politie, adviseert het College van procureurs-generaal over de voorgenomen inzet van een aantal bijzondere opsporingsbevoegdheden en -methodieken. Het College van procureurs-generaal brengt aan de Minister verslag uit over het aantal ter toetsing en registratie aangeboden (bijzondere) opsporingsbevoegdheden.

[39] De Commissie Evaluatie Afgesloten Strafzaken (CEAS), ook bekend als de Commissie Posthumus II of de Commissie Buruma, had ten doel na te gaan of zich in de opsporing van strafbare feiten en/of in de behandeling van daaruit voortgekomen strafzaken ernstige manco's hadden voorgedaan die een evenwichtige beoordeling van de feiten door de rechter in de weg stonden. De commissie bestond uit drie leden: een onafhankelijke voorzitter, een lid van buiten het OM en een lid van binnen het OM. De commissie werd ondersteund vanuit het OM (parket-generaal).

toelichting wordt ingegaan op de keuze voor opneming in Titel IV.[40] De Afdeling acht die argumentatie evenwel niet overtuigend. Bij de toepassing van bijzondere opsporingsbevoegdheden op grond van Titel IVA zijn meer rechtswaarborgen van toepassing dan bij Titel IV het geval is. De Afdeling wijst op de ruimere notificatieplicht – notificatie geschiedt volgens Titel IV slechts indien de bevoegdheid leidt tot vastlegging of ontoegankelijkmaking van gegevens, terwijl mededeling van de uitoefening van de bijzondere opsporingsbevoegdheden op grond van Titel IVA wordt gedaan zodra het belang van het onderzoek het toelaat –, de voeging van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen die verschoningsgerechtigden raken.[41]

Indien niet dragend gemotiveerd kan worden waarom de voorgestelde bevoegdheid tot binnendringen op afstand opgenomen dient te worden in Titel IV van het Eerste Boek Sv, adviseert de Afdeling deze bevoegdheid op te nemen in de regeling van bijzondere opsporingsbevoegdheden (Titel IVA van het Eerste Boek Sv).

4. Identiteit van een geautomatiseerd werk

De voorgestelde bevoegdheid tot binnendringen is niet zonder risico. Binnendringen in een geautomatiseerd werk levert per definitie risico's op ten aanzien van de stabiliteit van het geïnfiltreerde systeem. De toelichting onderkent dat risico's zijn verbonden aan het binnendringen, maar stelt dat bij de toepassing van de opsporingsbevoegdheid een afweging zal moeten worden gemaakt waarbij onder andere deze risico's een rol zullen spelen.[42]

De Afdeling merkt op dat de opsporingsbevoegdheid tevens zal kunnen worden toegepast om de identiteit van het geautomatiseerd werk vast te kunnen stellen.[43] Meer in het algemeen is niet vereist dat voorafgaand daaraan de identiteit van het geautomatiseerd werk vaststaat. Het door een verdachte gebruikte geautomatiseerd werk zou echter een vitale functie kunnen vervullen binnen bijvoorbeeld een ziekenhuis, bank of cruciaal beveiligingssysteem. Zou deze functie bekend zijn, dan zou dit waarschijnlijk tot de conclusie leiden dat de risico's van infiltratie in dat betreffende geautomatiseerd werk onaanvaardbaar groot zijn, en infiltratie dus achterwege moet blijven. Niet valt in te zien waarom eenzelfde conclusie dan niet zou moeten worden verbonden aan het onbekend zijn van de identiteit van het geautomatiseerd werk.

Gelet op het voorgaande komt het de Afdeling voor dat het vaststaan van de identiteit van het geautomatiseerd werk een wettelijk vereiste zou dienen te zijn voor toepassing van de bevoegdheid tot heimelijk binnendringen. Dit zou slechts dan anders moeten zijn, indien dit wettelijk vereiste onevenredig grote gevolgen zou hebben voor de uitvoerings-

---

[40] «Voor opneming van de voorgestelde bevoegdheid in Titel IV van het Wetboek van Strafvordering is gekozen vanwege de nauwe samenhang tussen deze bevoegdheid en de regels voor de doorzoeking ter vastlegging van gegevens, die zijn opgenomen in de zevende afdeling van die titel. In die afdeling zijn reeds de nodige waarborgen opgenomen (...)» memorie van toelichting, paragraaf 9. Adviezen over het wetsvoorstel.

[41] Zo bestaat er een verschil in de notificatieverplichting tussen de artikelen 125m en 126bb Sv. Artikel 125l Sv sluit het onderzoek in een geautomatiseerd werk uit, indien daarin gegevens zijn ingevoerd door of vanwege personen met bevoegdheid tot verschoning. Artikel 126aa Sv regelt de vernietiging van processen-verbaal of andere voorwerpen die mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 Sv zou kunnen verschonen.

[42] Memorie van toelichting, paragraaf 2.5. De inzet van de bevoegdheid, I De verkennende fase.

[43] Voorgesteld artikel 125ja, eerste lid, onder a, Sv.

praktijk. De toelichting geeft hierover echter geen informatie en geeft evenmin een afweging. Indien zou blijken dat met een wettelijk vereiste, dat de identiteit van het binnen te dringen geautomatiseerd werk vast moet staan, de bevoegdheid niet bijdraagt aan de effectiviteit van opsporing of vervolging, dan zou het voorstel op dit punt geen wijziging behoeven. In dat geval echter zou bij de rechter-commissaris in ieder geval uitdrukkelijk gemotiveerd moeten worden, waarom de risico's van heimelijk binnendringen in een geautomatiseerd werk waarvan de identiteit niet vaststaat in dat specifieke geval niet opwegen tegen het belang van het onderzoek bij toepassing van de bevoegdheid tot binnendringen in dat werk.

De Afdeling adviseert de mogelijkheid tot het binnendringen in geautomatiseerde werken waarvan de identiteit niet vaststaat in het licht van het voorgaande dragend te motiveren en het wetsvoorstel zo nodig aan te passen. Blijft het voorstel ongewijzigd, dan adviseert de Afdeling in het voorstel het vereiste op te nemen dat bij de rechter-commissaris uitdrukkelijk gemotiveerd moeten worden, waarom de risico's van heimelijk binnendringen in een geautomatiseerd werk waarvan de identiteit niet vaststaat in dat specifieke geval niet opwegen tegen het belang van het onderzoek bij toepassing van de bevoegdheid tot binnendringen in dat werk.

5. Rechtsmacht

In de toelichting wordt ingegaan op het vraagstuk van de rechtsmacht in geval van de opsporing van grensoverschrijdende ernstige strafbare feiten, waarbij gebruik wordt gemaakt van geautomatiseerde werken. Uitgangspunt bij het heimelijk binnendringen van een geautomatiseerd werk in het buitenland zal moeten zijn dat dit enkel geschiedt met toestemming van het land waar het geautomatiseerd werk zich bevindt. De toelichting legt de nadruk op situaties waarbij de feitelijke locatie van elektronische gegevens niet valt te achterhalen. In die gevallen kan niet worden vastgesteld dat deze zich in het buitenland bevinden, en zou Nederland moeten kunnen optreden, aldus de toelichting. Als dit anders zou zijn, dan zou dit betekenen dat het internet een ongereguleerde rechtssfeer is en aldus een vrijplaats voor de criminaliteit. Dat is niet aanvaardbaar, aldus de toelichting.[44]

De Afdeling onderkent dat het gelet op de huidige stand van de techniek eenvoudig is om de locatie van een geautomatiseerd werk of opgeslagen gegevens te verhullen. Daarbij is bij de opslag in de cloud in veel gevallen niet langer sprake van één duidelijk identificeerbare locatie, en als gevolg daarvan onder omstandigheden evenmin één aanwijsbaar land waarbinnen de opslag plaatsvindt.[45] Het beperken van de opsporingsbevoegdheid tot enkel die gevallen waarin men zeker weet dat het geautomatiseerd werk zich in Nederland bevindt, is gelet daarop niet goed mogelijk. Ook in die gevallen moet optreden mogelijk zijn. Tegelijkertijd roept dit een situatie in het leven waarbij het aanmerkelijke risico wordt genomen dat opsporingshandelingen worden verricht buiten het territorium van Nederland, zonder dat hiervoor een grondslag in het volkenrecht bestaat. De opmerking in de toelichting dat voorzichtigheid past bij het zelfstandig optreden ter handhaving,[46] zou naar het oordeel van de Afdeling dan ook tot uitdrukking moeten komen in de regelgeving.

---

[44] Ibidem.

[45] Koops e.a., *Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing*, Centrum voor Recht, Technologie en Samenleving (TILT), oktober 2012, blz. 36.

[46] Memorie van toelichting, paragraaf 2.8.4. Conclusie.

In het voorstel wordt niet vereist dat de machtiging of het bevel vermeldt waar het geautomatiseerd werk zich bevindt. Noch vermeldt de toelichting dat en hoeveel moeite mag worden verwacht van de opsporingsdiensten om de locatie van een geautomatiseerd werk of gegevensdrager te achterhalen. Daarmee staat ook niet vast dat de rechter-commissaris en de officier van justitie een expliciete afweging zullen maken ten aanzien van de mogelijk internationale toepassing van de opsporings-bevoegdheid. Anders dan de toelichting suggereert, beperkt de regeling de toepassing van de opsporingsbevoegdheid evenmin tot die gevallen waarin de noodzaak tot onverwijld grensoverschrijdend optreden vaststaat.[47] Ten slotte ontbreekt in de toelichting aandacht voor de situatie waarbij de locatie van het geautomatiseerd werk aanvankelijk onbekend was, maar na het binnendringen duidelijk wordt dat het geautomatiseerd werk zich buiten Nederland bevindt.[48] Van belang is dat toepassing van de bevoegdheid onmiddellijk wordt beëindigd dan wel op de kortst mogelijke termijn alsnog toestemming wordt gevraagd van het desbetreffende land.[49] In het voorstel dient geregeld te zijn wat dient te geschieden met hetgeen reeds aan informatie is verkregen.

De Afdeling adviseert in het licht van het voorgaande in de toelichting nader in te gaan op de toepassing van opsporingsbevoegdheden waarbij niet vast staat dat het geautomatiseerd werk zich in Nederland bevindt en het voorstel zo nodig aan te passen.

6. Overige opmerkingen heimelijk binnendringen

a. Aanzetten webcams in woningen

De voorgestelde bevoegdheid tot heimelijk binnendringen in een geautomatiseerd werk lijkt mee te brengen dat in voorkomende gevallen op afstand een webcam kan worden aangezet. Indien dit een woning betreft, zou ook (op afstand) kunnen worden meegekeken in een woning. De voorgestelde wettekst sluit dat althans niet uitdrukkelijk uit.
Uit de wetsgeschiedenis van de Wet bijzondere opsporingsbevoegdheden blijkt echter dat het – in het kader van stelselmatige observatie – (van buitenaf) permanent waarnemen door middel van een camera van wat er zich in een woning afspeelt, als even ingrijpend moet worden beschouwd als het betreden van een woning, en uitdrukkelijk is verboden.[50] Het verbod tot het betreden – ter uitvoering van een bevel tot observatie – van een woning zonder toestemming van de rechthebbende is vervat in artikel 126g, tweede lid, Sv.[51]

Gelet hierop adviseert de Afdeling in de toelichting in te gaan op de voorgestelde bevoegdheid tot binnendringen van een geautomatiseerd werk met het oog op een bevel tot observatie (het voorgestelde artikel 125ja, eerste lid, onderdeel e, Sv) in het geval dat het geautomatiseerd werk zich in een woning bevindt. Zij adviseert met name in te gaan op de verhouding tot het bestaande artikel 126g, tweede lid, Sv dat het betreden van woningen met het oog op observatie uitdrukkelijk verbiedt en het wetsvoorstel zo nodig aan te passen.

---

47 Idem.
48 Vergelijk de regeling in artikel 126ma, tweede lid, Sv.
49 Zie ook artikel 32 van het Cybercrimeverdrag.
50 Kamerstukken II 1996/97, 25 304, nr. 3, blz. 71.
51 De redenen daarvoor zijn dat woningen worden gezien als plaatsen waar men bij uitstek onbevangen zichzelf kan zijn en dat het huisrecht zowel krachtens de Grondwet als internationale mensenrechtenverdragen speciale bescherming geniet. Kamerstukken II 1996/97, 25 403, nr. 3, blz. 43.

b. Ontoegankelijkmaking

i. In het voorgestelde artikel 125ja Sv wordt een bevoegdheid opgenomen om een geautomatiseerd werk binnen te dringen, onder meer met het oog op het ontoegankelijk maken van gegevens.[52] De bevoegdheid tot ontoegankelijkmaking van gegevens die bij een doorzoeking in een geautomatiseerd werk worden aangetroffen is thans geregeld in artikel 125o Sv. De Afdeling begrijpt uit de toelichting dat indien in het kader van het heimelijk binnendringen gegevens worden aangetroffen, niet langer de bestaande bevoegdheid behoeft te worden toegepast, maar dat het ontoegankelijk maken kan plaatsvinden op basis van het bevel tot onderzoek in een geautomatiseerd werk.[53]

In de toelichting wordt niet ingegaan op de noodzaak van de voorgestelde bevoegdheid tot ontoegankelijkmaking in het licht van de bestaande bevoegdheid in artikel 125o Sv. Het bevel tot ontoegankelijkmaking betreft een verstrekkende bevoegdheid die inbreuk kan maken op de vrijheid van meningsuiting. Zo'n inbreuk kan noodzakelijk zijn in het belang van onder meer het voorkomen van wanordelijkheden en strafbare feiten.

In het licht hiervan adviseert de Afdeling de noodzaak voor de voorgestelde bevoegdheid tot ontoegankelijkmaking in het kader van het heimelijk binnendringen van een geautomatiseerd werk, mede in het licht van de bestaande bevoegdheid tot ontoegankelijk maken, nader toe te lichten.

ii. De Afdeling wijst voorts op een aantal verschillen tussen de voorgestelde bevoegdheid tot ontoegankelijkmaking in het kader van het binnendringen van een geautomatiseerd werk en de bestaande bevoegdheid tot ontoegankelijkmaking. De toelichting stelt dat de voorgestelde bevoegdheid slechts kan worden ingezet voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Dit criterium blijkt evenwel niet uit de voorgestelde bepaling; het is wel opgenomen in het bestaande artikel 125o Sv. Ook blijkt uit de voorgestelde bepaling niet dat het gaat om gegevens «met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd», zoals dat wel geldt voor het bestaande artikel 125o Sv. Voorts is in het voorgestelde artikel 125ja Sv [54]niet geregeld dat, zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de ontoegankelijkmaking, bepaald dient te worden dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerd werk worden gesteld.[55] Evenmin is geregeld dat de rechter bij zijn uitspraak een beslissing neemt over de ontoegankelijkmaking op grond van artikel 125ja Sv,[56] of dat belanghebbenden beklag kunnen indienen op het moment dat voor hen duidelijk is dat gegevens ontoegankelijk zijn gemaakt op grond van artikel 125ja Sv.[57]

De Afdeling adviseert de voorgestelde bevoegdheid tot ontoegankelijkmaking in het kader van het binnendringen in een geautomatiseerd werk (artikel 125ja, eerste lid, onderdeel b, Sv) vorm te geven naar analogie van artikel 125o Sv en nodige afwijkingen te motiveren.

---

[52] Daarnaast wordt in artikel 125p Sv voorgesteld om een aanbieder van een telecommunicatiedienst te bevelen dat gegevens ontoegankelijk worden gemaakt. Deze bevoegdheid is thans opgenomen in artikel 54a Sr. Uit een oogpunt van wetssystematiek is overplaatsing naar het Wetboek van Strafvordering wenselijk, aldus de toelichting, par. 3.1, tweede alinea.

[53] Vergelijk de artikelsgewijze toelichting op artikel 125ja, eerste lid, Sv.

[54] Alsmede het voorgestelde artikel 125p Sv.

[55] Vergelijk 125o, derde lid, Sv.

[56] In de zin van artikel 354 Sv. Vergelijk artikel II, onderdeel O van het voorstel.

[57] Artikel 552a Sv. Vergelijk artikel II, onderdeel P van het voorstel.

iii. De ontoegankelijkmaking is blijkens de toelichting mede gericht op botnets, netwerken van geïnfecteerde computers waarvan de eigenaar niet weet dat deze wordt misbruikt voor bijvoorbeeld het versturen van spam of het uitvoeren van een DDOS-aanval, pogingen om een computer of dienst onbruikbaar te maken.

Er bestaan twee soorten botnets: netwerken met een centrale aansturing (command and control- server) en netwerken zonder centrale aansturing (peer-to-peer). Ziet de Afdeling het goed dan zijn de eerste netwerken in de toekomst op basis van het voorgestelde artikel 125p Sv aan te pakken.[58] De laatste netwerken zijn niet uit te schakelen door middel van een centrale server, maar zouden in iedere afzonderlijke computer moeten worden uitgeschakeld. Hiervoor zou de bevoegdheid tot binnendringen kunnen dienen.

Met name het binnendringen ter afsluiting van de laatste soort botnets vergt een zodanige inspanning dat die naar het oordeel van de Afdeling al snel disproportioneel zal kunnen zijn ten opzichte van de last die een botnet veroorzaakt. Gelet op het grote aantal computers verbonden in een botnet zal het risico op het binnendringen van computers met een vitale functie daarbij toenemen. Daarbij verdient tevens de aandacht dat blijkens de praktijk het verwijderen van een botnet slechts tijdelijk effect heeft. Deze netwerken verspreiden zichzelf, en kunnen binnen korte tijd opnieuw of in hernieuwde vorm actief zijn. Een opsporingsbevoegdheid ten behoeve van grootschalige opruimacties is gelet hierop dan ook weinig effectief. Daarbij bestaat het gevaar dat men zal belanden in een wedloop waaraan substantiële kosten zullen zijn verbonden.

De Afdeling adviseert de bevoegdheid tot binnendringen en ontoegankelijkmaking in relatie tot de bestrijding van botnets nader te motiveren.

c. Heimelijk binnendringen in een telefoon

De toelichting onderkent dat een softwareapplicatie als een technisch hulpmiddel in de zin van het Wetboek van Strafvordering kan worden aangemerkt. De toelichting merkt daarbij op dat bij de observatiebevoegdheid in de artikelen 126g en 126o, derde lid, Sv is bepaald dat een technisch hulpmiddel niet op een persoon wordt bevestigd tenzij met diens toestemming. Vervolgens stelt de toelichting dat in de jurisprudentie is geoordeeld dat een telefoon geen heimelijk op het lichaam geplaatst hulpmiddel is in de zin van de wet. «Een telefoon wordt niet op de persoon bevestigd onder gezag of in opdracht van het openbaar ministerie en/of de politie. Er wordt namelijk gebruik gemaakt van een voorwerp dat een verdachte reeds voor een ander doel bij zich draagt.», aldus de uitspraak waarnaar wordt verwezen, waarbij de telefoon van een verdachte werd gepeild door middel van zogenaamde stealth-sms-en.[59] De toelichting stelt dat aangenomen kan worden dat dit eveneens zal gelden voor de toepassing van een softwareapplicatie op een telefoon.

Waarop deze aanname berust is daarmee evenwel niet duidelijk gemaakt. De softwareapplicatie wordt immers zelfstandig als technisch hulpmiddel gezien. Nu deze heimelijk, onder gezag van het openbaar ministerie, op de telefoon van een verdachte kan worden geplaatst is evenzeer aannemelijk dat de toepassing van dit middel stuit op het verbod van artikel 126g en 126o, derde lid, Sv. Deze situatie lijkt immers aan te sluiten op de omschrijving die door de wetgever is gegeven van «Bevestiging op een persoon» bij de totstandkoming van artikel 126g, derde lid, Sv: «Beves-

[58] Zie artikel II, onderdeel G, van het voorstel.
[59] Rechtbank 's-Hertogenbosch, 14 juni 2012, LJN BW 8619 en BW 8633.

tiging op een persoon houdt in: op of aan het lichaam of de kleding. Daaronder valt ook plaatsbepalingsapparatuur die wordt aangebracht in een aansteker of pen die in of op de kleding wordt gedragen.»[60] Met deze uitzondering werd aangesloten bij de aanbevelingen in het eindrapport van de Parlementaire enquêtecommissie opsporingsmethoden.[61] Waarom thans tot een andere beoordeling wordt gekomen ten aanzien van de proportionaliteit van een locatiebepalingsmiddel op een persoon behoeft dan ook een dragende motivering, die thans in de toelichting ontbreekt.

De Afdeling adviseert in het licht van het bovenstaande in de toelichting nader in te gaan op de verhouding van de voorgestelde bevoegdheid tot het verbod om een technisch hulpmiddel op de persoon te bevestigen zoals bedoeld in artikel 126g en 126o, derde lid, Sv en het voorstel zo nodig aan te passen.

d. Systeemzwakte door binnendringen

De toelichting gaat slechts beperkt in op het aan het binnendringen verbonden risico dat derden gebruik zullen maken van de aldus gecreëerde systeemzwakte. De toelichting erkent dat het openen van een toegangspoort tot een computer ertoe kan leiden dat derden van diezelfde opening gebruik maken. Wanneer de toegangspoort voorheen niet was geopend, zal het in de praktijk niet snel voorkomen dat een derde daarvan gebruik maakt, omdat de gebruikte software dit doorgaans zal tegengaan. Als dit toch het geval zou zijn dan is dit voor de politie zichtbaar, ook in de logging van de gegevens, en zullen maatregelen worden getroffen om de gegevensstroom via de poort onder controle te houden en het gebruik door de derde te beëindigen, aldus de toelichting.[62] Daarmee gaat de toelichting niet in op ervaringen in Duitsland met de FinFisher-spyware, zoals opgemerkt in het advies van Bits of Freedom in de internetconsultatie.[63] Zowel in Duitsland als in Frankrijk zou zijn afgezien van het gebruik van spyware omdat oneigenlijk gebruik door derden en de politie niet viel uit te sluiten.

Gelet op het bovenstaande adviseert de Afdeling in de toelichting nader in te gaan op het risico van systeemzwaktes veroorzaakt door de gebruikte software, en de mogelijkheden van oneigenlijk gebruik van die software door derden, waaronder de leveranciers van de software. Daarbij zou tevens moeten worden ingegaan op de mogelijkheden om dit oneigenlijk gebruik te voorkomen, en de wijze waarop de politie voorafgaand aan de inzet van een technisch middel de daaraan verbonden risico's kan beheersen.

e. Nadere regels omtrent technische eisen

Het voorgestelde artikel 125ja Sv biedt de grondslag om regels te stellen omtrent de technische eisen waaraan de software (het technische hulpmiddel) moet voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde gegevens. Daarmee worden nog geen eisen gesteld met betrekking tot mogelijk oneigenlijk gebruik van het technische hulpmiddel. Ook op het gebied van de onschendbaarheid van de vastgelegde gegevens worden in de grondslag geen eisen gesteld. Er wordt enkel voorzien in een grondslag voor nadere regels. Naar het oordeel van de Afdeling maken de hoofdlijnen van de eisen die aan de te

---

[60] Kamerstukken II 1996/97, 25 403, nr. 3, blz. 71.
[61] Kamerstukken II 1995/96, 24 072, nr. 10–11, blz. 175–176 en 458.
[62] Memorie van toelichting, § 2.5. De inzet van de bevoegdheid, III De afsluiting van het onderzoek in een geautomatiseerd werk.
[63] Bits of Freedom, Reactie op consultatie Wetsvoorstel Computercriminaliteit III, blz. 16.

gebruiken technische hulpmiddelen worden gesteld, zoals de onschendbaarheid van de gegevens, en voorkoming of beperking van mogelijk oneigenlijk gebruik onderdeel uit van de hoofdlijnen van de voorgestelde regeling. Gelet daarop zouden deze eisen dan ook zelfstandig moeten worden opgenomen in het voorgestelde artikel 125ja Sv, waarbij een nadere uitwerking van de technische eisen bij of krachtens algemene maatregel van bestuur mogelijk wordt gemaakt.

De Afdeling adviseert in de toelichting op het voorgaande in te gaan en het voorstel zo nodig aan te passen.

f. Verwijdering software

De toelichting stelt dat het niet altijd mogelijk zal zijn om software die is gebruikt om binnen te dringen in een geautomatiseerd werk (een zogenaamd trojan horse) te verwijderen, aangezien hieraan risico's kunnen zijn verbonden voor de stabiliteit van het systeem.[64] Wanneer de software aanwezig blijft in het geautomatiseerd werk, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerd werk, aldus de toelichting.
Dit roept echter de vraag op welke waarborgen zijn verbonden aan dit stopzetten van het dataverkeer. Dit zou immers impliceren dat zonder al te veel moeite het dataverkeer ook weer kan worden hervat. Ook bestaat het risico dat derden van de niet verwijderde software gebruik kunnen maken.

De Afdeling adviseert in de toelichting in te gaan op de waarborgen van stopzetting van het dataverkeer door de politie alsmede op het risico dat derden van de niet verwijderde software gebruik kunnen maken, en het voorstel zo nodig aan te passen. Tevens adviseert de Afdeling in het voorstel een verplichting op te nemen tot het verstrekken van technische gegevens aan de hand waarvan het voor de beheerder van het geautomatiseerd werk mogelijk wordt om de in het kader van het onderzoek geïnstalleerde software te verwijderen.

A. Heimelijk binnendringen in geautomatiseerd werk

1. Differentiatie en verhouding tot het EVRM

a. Differentiatie

De Afdeling advisering (hierna ook: de Afdeling) wijst erop dat de inbreuk op de persoonlijke levenssfeer op basis van de voorgestelde bevoegdheid kan verschillen, afhankelijk van de handeling, maatregel of bevoegdheid die wordt toegepast. De generieke benadering van het wetsvoorstel, waarbij in alle gevallen dezelfde voorwaarden gelden, sluit hier naar het oordeel van de Afdeling niet bij aan. Ingeval sprake is van bijvoorbeeld het bepalen van de identiteit of van de locatie van het geautomatiseerde werk of de gebruiker, zijn de voorgestelde waarborgen naar het oordeel van de Afdeling passend. Bij het binnendringen met het oog op het aftappen van communicatie of stelselmatige observatie, kan eveneens worden volstaan met de voorgestelde voorwaarden. Bij het heimelijk op afstand doorzoeken van een geautomatiseerd werk en/of het overnemen van gegevens is sprake van een beduidend zwaarder ingrijpen in de persoonlijke levenssfeer, vergelijkbaar met het heimelijk binnendringen in een woning met het oog op het opnemen van vertrouwelijke communicatie. De Afdeling acht het passend dat eenzelfde drempel als voor de

[64] Memorie van toelichting, paragraaf 2.5. De inzet van de bevoegdheid, III De afsluiting van het onderzoek in een geautomatiseerd werk.

aanwending van die opsporingsbevoegdheid, namelijk een verdenking van misdrijven waarop gevangenisstraf van acht jaar of meer is gesteld, zou komen te gelden voor de meest ingrijpende vormen van de voorgestelde bevoegdheid tot heimelijk binnendringen in een geautomatiseerd werk.

b. Verhouding tot het EVRM

De Afdeling wijst op de vereisten die uit artikel 8 van het EVRM voortvloeien, zoals de vereisten van proportionaliteit en subsidiariteit. Het ligt in de rede om in de wet zwaardere voorwaarden te stellen aan de toepassing van een bevoegdheid naarmate de bevoegdheid een zwaardere inbreuk maakt op de persoonlijke levenssfeer in de zin van artikel 8 EVRM. Nu deze differentiatie ontbreekt, staat in het bijzonder de proportionaliteit van de inbreuk niet vast.

c. Conclusie

Hieruit volgt naar het oordeel van de Afdeling dat in de voorgestelde bepaling onvoldoende wordt gedifferentieerd tussen de uiteenlopende aard van de inbreuken op de persoonlijke levenssfeer. Voor het binnendringen dat het meest ingrijpend is, zoals het doorzoeken van alle gegevens in het geautomatiseerde werk en het overnemen daarvan, acht de Afdeling aansluiting bij de voorwaarden voor de toepassing van de bijzondere opsporingsbevoegdheid tot het opnemen van vertrouwelijke communicatie waarbij een woning wordt binnengedrongen, aangewezen. De Afdeling adviseert het voorgestelde artikel 125ja Sv aan te passen.

Het advies van de Afdeling strekt ertoe dat differentiatie wordt aangebracht in de voorwaarden voor de toepassing van de voorgestelde bevoegdheid, zodat het doorzoeken van alle gegevens en het overnemen daarvan uitsluitend mogelijk is in geval van verdenking van een misdrijf waarop een vrijheidsstraf van acht jaar of meer is gesteld. Aan dit advies is deels gevolg gegeven. Met de Afdeling advisering kan worden geoordeeld dat het op afstand binnendringen in een geautomatiseerd werk, gevolgd door het doorzoeken van alle gegevens die in dat werk zijn opgeslagen, een meer vergaande inbreuk op de privacy van de betrokkene oplevert dan wanneer het binnendringen wordt gevolgd door het aftappen van communicatie of de stelselmatige observatie. Beperking van de toepassing tot zeer ernstige misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld, is echter te beperkend. Er zijn bepaalde ernstige strafbare feiten waarop een vrijheidsstraf van minder dan acht jaar is gesteld maar die naar hun aard worden gepleegd met behulp van een geautomatiseerd werk – het gebruik van een geautomatiseerd werk is dan instrumenteel voor het plegen van het delict – waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders, en de inzet van andere opsporingsbevoegdheden onvoldoende zicht op resultaat biedt. Dit kan bijvoorbeeld aan de orde zijn bij het ontoegankelijk maken van kinderpornografisch materiaal dat op internet wordt gepubliceerd. Voor het beëindigen van een dergelijke situatie is het van essentieel belang dat op afstand kan worden binnengedrongen in een server om dit materiaal ontoegankelijk te maken. Ook bij de bestrijding van een botnet kan het onvermijdelijk zijn om een server binnen te dringen om de gegevens ontoegankelijk te maken, bijvoorbeeld in de gevallen waarin banken worden belaagd door een zogenaamde DDOS-aanval. Een botnet kan zoveel overlast voor het maatschappelijk verkeer veroorzaken dat de toepassing van de voorgestelde bevoegdheid van het binnendringen van een server of een ander geautomatiseerd werk met het oog op de ontoegankelijkmaking van gegevens aangewezen is, zeker in het licht van de betrekkelijk lichte

inbreuk op de bescherming van de persoonlijke levenssfeer die daarbij aan de orde is. Dit ligt anders bij misdrijven die raakvlakken hebben met de vrijheid van meningsuiting, zoals de belediging (art. 137c Sr), het aanzetten tot haat (art. 137d Sr), of de openbaarmaking van beledigende uitlatingen (art. 137e Sr). Bij deze misdrijven kan het binnendringen van een server eveneens dienstig zijn om een einde te maken aan een strafbare uiting, maar valt de afweging tussen de betrokken belangen – het belang van de opsporing, de bescherming van de persoonlijke levenssfeer en de vrijheid van meningsuiting – anders uit; deze misdrijven zullen niet bij algemene maatregel van bestuur worden aangewezen.

Naar aanleiding van het advies van de Afdeling advisering is de voorwaarde voor de inzet van deze bevoegdheid aangescherpt voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens. Daarbij kunnen gegevens worden doorzocht die in het geautomatiseerde werk worden verwerkt. Voor het verrichten van deze onderzoekshandelingen is een misdrijf vereist dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of een misdrijf dat bij algemene maatregel van bestuur is aangewezen. De bij algemene maatregel van bestuur aan te wijzen misdrijven betreffen bepaalde misdrijven waarop weliswaar geen gevangenisstraf van acht jaar is gesteld maar die naar hun aard worden gepleegd met behulp van een geautomatiseerd werk. Het doorzoeken van de gegevens in het geautomatiseerde werk, teneinde deze vast te leggen of ontoegankelijk te maken, is essentieel voor het opsporen van dergelijke delicten. Dit betreft misdrijven als het gebruik van een botnet (artikel 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) de «grooming» (artikel 248e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.

In het licht van het bovenstaande zijn de voorgestelde artikelen 125nba en 125uba, eerste lid, aangepast. Daarbij wordt onderscheid gemaakt in de wettelijke voorwaarden die gelden voor het verrichten van de verschillende onderzoekshandelingen. Voor onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op de bepaling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker of met het oog op de uitvoering van een bevel tot het aftappen van telecommunicatie, het direct afluisteren of stelselmatige observatie, is een misdrijf vereist waarvoor voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert. Voor onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens is een misdrijf vereist waarop een gevangenisstraf van tenminste acht jaar is gesteld of dat bij algemene maatregel van bestuur is aangewezen en dat een ernstige inbreuk op de rechtsorde oplevert.

2. Systeemtoezicht

a. Het voorliggende wetsvoorstel

De Afdeling heeft geadviseerd in de toelichting in te gaan op de controle achteraf op de toepassing van de voorgestelde bevoegdheden in gevallen die aan het toezicht door de rechter zijn onttrokken,

Naar aanleiding van het advies van de Afdeling is hierop in de toelichting nader ingegaan. Voorgesteld wordt de bevoegdheid tot het onderzoek in een geautomatiseerd werk onder te brengen in de regeling voor de bijzondere opsporingsbevoegdheden van het Wetboek van Strafvordering. Dit komt hieronder nader aan de orde (punt 3). Hieruit vloeit voort dat de notificatieplicht van toepassing is op de inzet van de voorgestelde bevoegdheid tot het onderzoek in een geautomatiseerd werk. Hierdoor wordt de betrokkene in staat gesteld om de rechtmatigheid van die inzet te laten toetsen, bijvoorbeeld door middel van een klacht bij de Nationale ombudsman. Tevens zal, conform de werkwijze bij het aftappen van communicatie, jaarlijks aan de Kamer worden gerapporteerd over de inzet van deze bevoegdheid. Dit betreft het aantal malen dat de bevoegdheid is ingezet, het aantal personen jegens wie de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid.

b. Structureel systeemtoezicht

Aan het advies van de Afdeling om te voorzien in structureel systeemtoezicht op de rechtmatige uitoefening van opsporingsbevoegdheden waarbij gebruikt wordt gemaakt van informatie en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd is geen gevolg gegeven. Op dit moment voorziet de regeling rond de inzet van bijzondere opsporingsbevoegdheden in uitgebreide waarborgen voor de inzet van die bevoegdheden. In sommige gevallen, waarbij dit vanwege de inbreuk van de bevoegdheid op de persoonlijke levenssfeer van de betrokkene aan de orde is, is rechterlijke tussenkomst vereist voordat de bevoegdheid kan worden ingezet. Aanvullend zal voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk komen te gelden dat de Centrale Toetsingscommissie van het Openbaar Ministerie de voorgenomen inzet toetst. Deze waarborgen acht ik voldoende om een rechtmatige en zorgvuldige toepassing van de bevoegdheden te kunnen garanderen.

3. Plaatsing in titel IV van het Eerste Boek Sv

De Afdeling acht de argumentatie voor opneming van de voorgestelde bevoegdheid in Titel IV van het Eerste Boek van het Wetboek van Strafvordering niet overtuigend en adviseert om, als die keuze niet dragend gemotiveerd kan worden, deze bevoegdheid op te nemen in de regeling van bijzondere opsporingsbevoegdheden (Titel VIA van het Eerste Boek Sv).

Naar aanleiding van het advies van de Afdeling is het wetsvoorstel aangepast. De bevoegdheid tot het onderzoek in een geautomatiseerd werk is ondergebracht in de regeling van de bijzondere opsporingsbevoegdheden (Titel IVA) van het Eerste Boek van het Wetboek van Strafvordering. Het is wenselijk dat deze bevoegdheid tevens kan worden ingezet bij het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband (Titel V) en bij de opsporing van terroristische misdrijven (Titel VB). Bij de aanpassing van het wetsvoorstel is hierin voorzien. In de toelichting is hierop nader ingegaan.

4. Identiteit van een geautomatiseerd werk

De Afdeling wijst op de risico's van het binnendringen in een geautomatiseerd werk, bijvoorbeeld als dit een vitale functie vervult binnen een bank of ziekenhuis, en adviseert de mogelijkheid tot het binnendringen in

geautomatiseerde werken waarvan de identiteit niet vaststaat dragend te motiveren en het wetsvoorstel zo nodig aan te passen.

Naar aanleiding van het advies is het wetsvoorstel aangepast. Voor de voorgestelde bevoegdheid tot het heimelijk binnendringen is als voorwaarde opgenomen dat in het bevel gegevens dienen te worden opgenomen met het oog op de identificeerbaarheid van het geautomatiseerde werk. Tevens is de toelichting aangevuld. Daarbij is aangegeven dat de identificeerbaarheid van het geautomatiseerde werk van belang is voor de afgrenzing van de voorgestelde bevoegdheid en daarmee voor de toetsing door de rechter-commissaris.
Naar aanleiding van dit advies kan nog worden opgemerkt dat de technische risico's die aan het op afstand heimelijk binnentreden van een geautomatiseerd werk zijn verbonden, doorgaans alleen bekend zijn bij de beheerder van het betreffende werk. De officier van justitie en de rechter-commissaris kunnen deze risico's minder goed beoordelen. De technische risico's kunnen worden beheerst dan wel beperkt door middel van de deskundigheid van de opsporingsambtenaren die zijn belast met het plaatsen van het technische hulpmiddel en de software met behulp waarvan het onderzoek in een geautomatiseerd werk kan worden verricht. Dit is in de toelichting verhelderd.

5. Rechtsmacht

De Afdeling wijst op het aanmerkelijke risico dat opsporingshandelingen worden verricht buiten het territorium van Nederland zonder dat hiervoor een grondslag in het volkenrecht bestaat. De voorzichtigheid die past bij het zelfstandig optreden ter handhaving zou tot uitdrukking moeten komen in de regelgeving.

Naar aanleiding van het advies is het wetsvoorstel aangepast. Voor de voorgestelde bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk is als voorwaarde opgenomen dat als de gegevens niet in Nederland zijn opgeslagen, dit in het bevel dient te worden vermeld. Tevens is de toelichting aangevuld. Daarbij is aangegeven dat de rechter-commissaris een machtiging tot het op afstand heimelijk binnendringen van een geautomatiseerd werk kan afgeven, ook in het geval dat de gegevens niet in Nederland zijn opgeslagen, waarbij de rechter-commissaris ervan uit mag gaan dat de officier van justitie zich houdt aan de regels op het gebied van de internationale samenwerking. Tevens is ingegaan op de situatie waarbij de locatie van het geautomatiseerd werk aanvankelijk onbekend was, maar na het binnendringen duidelijk wordt dat het geautomatiseerd werk zich buiten Nederland bevindt.

6. Overige opmerkingen heimelijk binnendringen

a. Aanzetten webcams in woningen

De Afdeling adviseert in te gaan op de verhouding tussen de voorgestelde bevoegdheid en het verbod in artikel 126g, tweede lid, Sv dat het betreden van een woning met het oog op observatie verbiedt.

Naar aanleiding van het advies is in de toelichting ingegaan op de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk en de uitvoering van de bevoegdheid tot stelselmatige observatie. Uit de verwijzing naar de bestaande bepalingen over de stelselmatige observatie in het wetsvoorstel vloeit voort dat het verbod op de stelselmatige observatie in een woning (artikelen 126g, tweede lid en 126o, tweede lid, Sv) onverminderd blijft gelden. Het permanent waarnemen wat zich in

een woning afspeelt via het op afstand aanzetten van een webcam van bijvoorbeeld een smartphone of een laptop, moet als even ingrijpend worden aangemerkt als het betreden van een woning; dit is niet toegestaan (vergelijk Kamerstukken II 1996/97, 25 403, nr. 3, blz. 71 wat betreft het plaatsen van een camera in een woning).

b. Ontoegankelijkmaking

i. De Afdeling adviseert de voorgestelde bevoegdheid tot ontoegankelijkmaking vorm te geven naar analogie van de bestaande bevoegdheid tot ontoegankelijkmaking.

i. en ii. Naar aanleiding van het advies is de voorgestelde bepaling over de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk aangepast. In die bepaling is verhelderd dat de voorgestelde bevoegdheid kan worden ingezet met het oog op de toepassing van de bevoegdheid tot ontoegankelijkmaking, bedoeld in artikel 125o Sv. Hiermee wordt, in lijn met het advies van de Afdeling, wettelijk vastgelegd dat de regeling van artikel 125o Sv bij het ontoegankelijk maken van gegevens van toepassing is.

iii. De Afdeling adviseert de voorgestelde bevoegdheid tot ontoegankelijkmaking in relatie tot de bestrijding van botnets nader te motiveren.

Naar aanleiding van het advies van de Afdeling is de bevoegdheid tot het binnendringen en de ontoegankelijkmaking van gegevens in relatie tot de bestrijding van botnets nader gemotiveerd.

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

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

c. Heimelijk binnendringen in een telefoon

De Afdeling adviseert nader in te gaan op de verhouding van de voorgestelde bevoegdheid tot het verbod om een technisch hulpmiddel op een persoon te bevestigen.

Naar aanleiding van het advies is in de toelichting nader ingegaan op de verhouding tussen de voorgestelde bevoegdheid en het verbod om een technisch hulpmiddel op een persoon te bevestigen. Dit heeft tevens geleid tot een aanpassing van de voorgestelde bepaling inzake het

binnendringen van een geautomatiseerd werk en de artikelen 126g, derde lid, en 126o, derde lid, Sv (stelselmatige observatie).

De huidige techniek maakt het mogelijk om op afstand software te plaatsen op een geautomatiseerd werk dat de verdachte meevoert, zoals een mobiele telefoon, en hiermee de gps-functie aan te zetten. Op deze wijze kunnen signalen worden opgevangen over de locatie waar het toestel en mogelijk de bezitter zich bevinden. Plaatsbepaling op basis van GPS-gegevens is nuttig in die gevallen waarin andere observatiemogelijkheden niet of niet voldoende resultaat hebben of wanneer de verblijfplaats van de verdachte onbekend is.
De ontwikkeling van de techniek leidt ertoe dat de reikwijdte van het verbod om een technisch hulpmiddel op een persoon te bevestigen minder strikt dient te worden uitgelegd dan voorheen. Voorgesteld wordt om de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel tot binnendringen van een geautomatiseerd werk melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt. Op deze wijze kan de rechter-commissaris hiermee rekening houden bij de beoordeling van de rechtmatigheid van het bevel.

d. Systeemzwakte door binnendringen

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

Naar aanleiding van het advies is in de toelichting nader ingegaan op het risico van systeemzwaktes veroorzaakt door de gebruikte software. Bij het binnendringen van een geautomatiseerd werk wordt gebruik gemaakt van een bestaande zwakte in het systeem. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd. Door het binnendringen met behulp van software wordt het systeem niet per definitie zwakker.

Als de politie gebruik maakt van bestaande zwakheden in het systeem is het in theorie mogelijk dat derden deze kwetsbaarheden eveneens gebruiken om binnen te dringen. Niet is uit te sluiten dat derden van diezelfde opening gebruik maken. Wanneer de politie van een dergelijke opening gebruik maakt, zal de politie waar mogelijk proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken. Het open laten van de mogelijkheid tot binnendringen in het systeem door derden tijdens de uitoefening van de bevoegdheid is niet het belang van het onderzoek, omdat dit afbreuk kan doen aan de betrouwbaarheid van het bewijs. De politie neemt voorts bij de inzet van de bevoegdheid technische maatregelen om de gegevensstroom onder controle te houden en de integriteit van de bewijsmiddelen te kunnen garanderen. Dit gebeurt bijvoorbeeld door geautomatiseerde vastlegging van de gegevens ter uitvoering van het bevel (logging), waardoor misbruik door derden kan worden onderkend en maatregelen kunnen worden getroffen om dit misbruik te beëindigen. Indien gebruik gemaakt wordt van een technisch hulpmiddel wordt moet het onder meer een functie bevatten die het

functioneren van het technische hulpmiddel tijdens de inzet ervan technisch vastlegt.

Met de voorafgaande keuring van het technische hulpmiddel kan worden voorkomen dat softwareapplicaties worden ingezet die niet voldoen aan de daaraan te stellen eisen. De ervaringen met bepaalde softwareapplicaties in andere landen onderstrepen het belang van een zorgvuldige keuringcertificering. De keuringseisen worden uitgewerkt in het Besluit technische hulpmiddelen strafvordering.

e. Nadere regels omtrent technische eisen

De Afdeling adviseert de eisen die aan de te gebruiken technische hulpmiddelen worden gesteld, zoals de onschendbaarheid van de gegevens en het voorkomen van oneigenlijk gebruik, in het Wetboek van Strafvordering op te nemen, waarbij een nadere uitwerking bij algemene maatregel van bestuur mogelijk wordt gemaakt.

Aan het advies is gevolg gegeven. In verband met de verplaatsing van de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk naar de regeling van de bijzondere opsporingsbevoegdheden (Titel IVA) van het Eerste Boek van het Wetboek van Strafvordering, wordt de grondslag voor het stellen van eisen aan technische hulpmiddelen die worden gebruikt bij het onderzoek doen in een geautomatiseerd werk geregeld in artikel 126ee Sv. Hiermee wordt aangesloten bij de wettelijke systematiek van de regeling omtrent de bijzondere opsporingsmiddelen, waarbij de algemene regels betreffende bevoegdheden in de titels IVA tot en VC zijn neergelegd in titel VD. Artikel 126ee Sv bevat een grondslag om technische eisen te stellen waaraan de hulpmiddelen dienen te voldoen, onder met het oog op de onschendbaarheid van de vastgelegde waarnemingen. Hieraan voegt het wetsvoorstel de vastgelegde gegevens – in het kader van een onderzoek in een geautomatiseerd werk – toe. Voorts wordt toegevoegd dat eisen kunnen worden gesteld met het oog op misbruik van het technische hulpmiddel door derden. Uitwerking van de technische eisen vindt plaats in het Besluit technische hulpmiddelen strafvordering.

f. Verwijdering software

De Afdeling adviseert om in te gaan op de waarborgen van stopzetting van het dataverkeer door de politie en het risico dat derden van niet verwijderde software gebruik maken.

Naar aanleiding van het advies van de Afdeling is in de toelichting ingegaan op de waarborgen van stopzetting van het dataverkeer door de politie indien de software aanwezig blijft in het geautomatiseerde werk. Voorts is ingegaan op het risico dat derden van de niet verwijderde software gebruik kunnen maken. Naar aanleiding van het advies wordt in artikel 126ee Sv een grondslag opgenomen om bij algemene maatregel van bestuur eisen te stellen aan een technisch hulpmiddel met het oog op voorkoming van misbruik door derden. Hierbij kan gedacht worden aan eisen omtrent de beveiliging van het gebruik van de software.

De Afdeling adviseert tevens om in het wetsvoorstel een verplichting op te nemen tot het verstrekken van technische gegevens aan de beheerder van een geautomatiseerd werk, zodat verwijdering van de geïnstalleerde software mogelijk wordt.

Naar aanleiding van het advies is in het voorgestelde artikel 126nba, zesde lid, Sv, een verplichting opgenomen tot het (zoveel mogelijk) ongedaan maken van de wijzigingen aan het geautomatiseerde werk nadat de

uitvoering van het bevel tot het onderzoek van een geautomatiseerd werk is beëindigd. Indien dit niet mogelijk is en dit risico's oplevert voor het functioneren van het geautomatiseerde werk dienen de nodige technische gegevens aan de beheerder van het geautomatiseerde werk te worden verstrekt. De verstrekking kan worden uitgesteld zolang het belang van het onderzoek zich tegen mededeling verzet.

B. Decryptiebevel aan de verdachte

Het wetsvoorstel beoogt een wettelijke grondslag te creëren voor het bevel aan de verdachte tot het toegankelijk maken van versleutelde elektronische gegevens.[65] De verdachte dient aan het bevel te voldoen door toegang te verschaffen tot het geautomatiseerd werk of delen daarvan, tot de gegevensdrager of tot versleutelde gegevens dan wel door kennis omtrent de beveiliging ter beschikking te stellen.[66] Op het niet meewerken aan het bevel wordt een gevangenisstraf gesteld van ten hoogste 3 jaren.[67]

De officier van justitie geeft, na een voorafgaande machtiging van de rechter-commissaris, het decryptiebevel aan de verdachte indien het onderzoek dit dringend vordert. De gevallen waarin het bevel kan worden gegeven betreffen verdenking van een terroristisch misdrijf, waarop een gevangenisstraf van acht jaar of meer is gesteld, dan wel het maken van een beroep of gewoonte van de vervaardiging, verspreiding en het bezit van kinderpornografie.[68] De verdachte wordt door de rechter-commissaris gehoord en is bevoegd zich tijdens het verhoor door een raadsman te doen bijstaan.

7. Noodzaak en effectiviteit decryptiebevel

a. Noodzaak

De toelichting vermeldt dat het van groot belang is dat politie en justitie toegang kunnen krijgen tot versleutelde gegevens 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. Vanwege het ingrijpende karakter van de bevoegdheid tot decryptiebevel aan verdachten 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 en het plegen van terroristische misdrijven, waarbij gebruik is gemaakt van versleutelde elektronische gegevens.

De Afdeling stelt voorop het streven van de regering om kinderpornografie en terrorisme te bestrijden te onderschrijven. Daarmee acht de Afdeling de aanpak van belemmeringen bij de opsporing en vervolging door gebruik van encryptie van belang. De Afdeling maakt echter de volgende kanttekeningen bij het voorgestelde decryptiebevel aan verdachten.

Volgens de toelichting komt het gebruik van encryptie voornamelijk voor binnen bepaalde netwerken van kinderpornogebruikers en -verspreiders. Dit is in het kader van de Rotterdamse proeftuin kinderpornografie aan de

---

[65] Voorgestelde wijziging van artikel 125k Sv.
[66] Voorgesteld artikel 125k, vijfde lid, Sv.
[67] Voorgesteld artikel 184b Sr.
[68] Artikel 240b, tweede lid, Sr. Op dit strafbaar feit staat 8 jaar gevangenisstraf.

orde gekomen.[69] De toelichting vermeldt dat er gevallen zijn waarin de verdachte zijn wachtwoorden vrijwillig verstrekt, maar zet niet uiteen in hoeverre het ontbreken van het decryptiebevel aan verdachten in de praktijk tot problemen heeft geleid.
Of het probleem zodanige vormen aanneemt dat het een aanzienlijke inbreuk op grondrechten zou rechtvaardigen, valt volgens het rapport «Het decryptiebevel en het nemo-teneturbeginsel» niet te zeggen.[70] Daarmee is onduidelijk wat de omvang van het probleem is. In het bijzonder wat betreft het decryptiebevel aan verdachten van terroristische misdrijven ontbreekt in het geheel zicht op de omvang van het probleem. Voorts onderkent de Afdeling dat wil een decryptiebevel worden gegeven er sprake moet zijn van een ernstig misdrijf. De ernst van de misdrijven impliceert echter niet, gelet op de inbreuk op grondrechten – in het bijzonder het zwijgrecht en het nemo teneturbeginsel, die besloten liggen in het recht op eerlijk proces van artikel 6 EVRM, en het recht op eerbiediging van de persoonlijke levenssfeer – dat de omvang van het probleem irrelevant zou zijn.

In de tweede plaats wijst de Afdeling erop dat de voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen in een geautomatiseerd werk ertoe kan leiden dat de behoefte aan het decryptiebevel voor verdachten vermindert. Thans is immers de voorgestelde bevoegdheid tot binnendringen nog niet mogelijk. Waar deze bevoegdheid succesvol ingezet wordt voor het vaststellen van de aanwezigheid van gegevens en/of en voor het overnemen van gegevens als bewijsmateriaal, is een decryptiebevel overbodig.

b. Effectiviteit

De Afdeling merkt op dat bij de effectiviteit van het decryptiebevel aan verdachten de nodige vraagtekens te plaatsen zijn en wijst daarbij op het volgende.

De toelichting wijst op de ervaringen in het Verenigd Koninkrijk. Hoewel het decryptiebevel daar niet wordt gezien als een wondermiddel, vindt men het een nuttig en effectief instrument, aldus de toelichting.[71] De Afdeling plaatst hierbij de kanttekening dat er volgens het recente jaarverslag (2012–2013) van de autoriteit die in het Verenigd Koninkrijk toezicht houdt op de uitoefening van de bevoegdheid een decryptiebevel te geven, de Chief Surveillance Commissioner, 35 aanvragen tot decryptiebevel waren ingediend bij de NTAC (autoriteit die toestemming moet verlenen), waarvan in 26 gevallen een bevel volgde. Aan slechts 3 bevelen werd voldaan, aan 19 niet. In 3 gevallen volgde een veroordeling voor decryptieweigering.[72]

---

[69] Memorie van toelichting, paragraaf 4.1. De noodzaak en de reikwijdte van de voorgestelde bevoegdheid.

[70] «Rond de Amsterdamse zedenzaak is de opsporing gestuit op beveiligde computers en versleutelde bestanden, maar dat heeft niet tot grote problemen bij de vervolging geleid. Robert M. gaf vrijwillig zijn wachtwoorden, de crypto van Flovin O. bleek door het NFI te kraken, en de weigering van Matthijs van der M. werd door de rechter gebruikt bij de verwerping van bepaalde verweren, bij de beslissing over onttrekking aan het verkeer en als strafverzwarende omstandigheid. Men kan dus niet zeggen dat het toenemend gebruik van cryptografie een onneembaar obstakel is met het huidige arsenaal aan juridische middelen.» «Het decryptiebevel en het nemo-teneturbeginsel», blz. 81.

[71] Memorie van toelichting, paragraaf 4.1. «De noodzaak en de reikwijdte van de voorgestelde bevoegdheid».

[72] Annual report of the Chief Surveillance Commissioner for 2012–2013, blz. 12–13.

Onder andere het College van Procureurs-Generaal en de Nederlandse Vereniging voor Rechtspraak, plaatsen kritische kanttekeningen bij de effectiviteit van het decryptiebevel aan verdachten.[73] Zij wijzen op de moeilijke bewijslevering ten aanzien van het opzet waardoor met de strafbepaling moeilijk zal kunnen worden gewerkt. Genoemd College stelt dat in «verreweg de meeste gevallen het bewijs van het opzet niet zal zijn te leveren». De verdachte hoeft bijvoorbeeld immers maar te stellen dat hij zich de sleutel niet kan herinneren.[74] De toelichting geeft wel aan dat de strafrechter in voorkomende gevallen een dergelijk beroep op overmacht kan verwerpen, maar kan daarmee niet weerleggen dat de bewijslevering ter zake moeilijk is.

Voorts wordt door genoemde adviserende instanties terecht gewezen op «calculerend gedrag» door de verdachte: deze kan immers de keuze maken voor een veroordeling voor decryptieweigering van maximaal 3 jaar teneinde een mogelijk zwaardere veroordeling voor het gronddelict (8 jaar of meer) te ontlopen.
De toelichting gaat echter niet in op het gestelde ten aanzien van het mogelijke calculerende gedrag van de verdachte in relatie tot de effectiviteit van het voorgestelde decryptiebevel.[75]

Een volgend aspect betreft het risico dat verdachten het wachtwoord verstrekken tot een bepaald deel van het geheugen van het geautomatiseerd werk, waarin alleen «onschuldige» bestanden zitten (het «non-hidden volume») en daarmee voldoen aan het decryptiebevel. De incriminerende bestanden kunnen worden opgeslagen in het «hidden volume» van het geautomatiseerd werk, waarvan de autoriteiten het bestaan niet kunnen bewijzen.[76]
In reactie daarop vermeldt de toelichting dat programma's beschikbaar zijn die versleutelde volumes kunnen zoeken en dat de grootte van de opslagcapaciteit aanwijzing kan zijn voor het bestaan van die bestanden.[77] De toelichting erkent echter dat niet uitgesloten is dat opsporingsautoriteiten worden misleid.

De toelichting vermeldt nog dat de misdrijven waarbij een decryptiebevel kan worden gegeven doorgaans door doorgewinterde criminelen worden gepleegd die bereid zijn vergaande maatregelen te treffen om ontdekking van het strafbare feit te voorkomen.[78] In het rapport «Het decryptiebevel

---

[73] Advies College van Procureurs-Generaal, blz. 7; advies Nederlandse Vereniging voor Rechtspraak, paragraaf 2.5.; Bits of Freedom, Reactie op consultatie Wetsvoorstel Computercriminaliteit III, paragraaf 3.3. «Het decryptiebevel is niet effectief».

[74] Advies College van Procureurs-Generaal, blz. 7. Ook uit het rapport «Het decryptiebevel en het nemo teneturbeginsel» (blz. 88 en 96) blijkt dat vertegenwoordigers van politie en het Openbaar Ministerie justitie sceptisch zijn over de effectiviteit en meerwaarde van een strafrechtelijk gesanctioneerd decryptiebevel voor verdachten.

[75] De toelichting vermeldt wel dat een ontsleutel*verzoek* (dus niet een bevel) waarschijnlijk niet zal werken bij berekenende criminelen die geen medewerking willen verlenen. Memorie van toelichting, paragraaf 4.1. De noodzaak en de reikwijdte van de voorgestelde bevoegdheid.

[76] Bits of Freedom, Reactie op consultatie Wetsvoorstel Computercriminaliteit III, blz. 22.

[77] Memorie van toelichting, paragraaf 9. Adviezen over het wetsvoorstel.

[78] Memorie van toelichting, paragraaf 4.4. «De strafbedreiging voor het opzettelijk niet voldoen aan een decryptiebevel».

en het nemo teneturbeginsel» wordt gesteld dat een ontsleutelplicht juist bij zware (zeden)delinquenten weinig effectief zal zijn.[79]

Gelet op het voorgaande is de Afdeling niet van de noodzaak en vooral niet van de effectiviteit van het voorgestelde decryptiebevel aan verdachten overtuigd. Zij adviseert op bovenstaande aspecten in de toelichting in te gaan, de noodzaak en met name de effectiviteit van het voorgestelde decryptiebevel aan verdachten dragend te motiveren of anders dit onderdeel van het wetsvoorstel te schrappen.

8. Verenigbaarheid decryptiebevel met het nemo teneturbeginsel

a. Het nemo teneturbeginsel

Het nemo teneturbeginsel houdt in dat een verdachte niet aan zijn eigen veroordeling behoeft mee te werken en verschoond dient te blijven van dwang tot zelfbeschuldiging. Volgens het EHRM ligt in het recht op het eerlijk proces van artikel 6 EVRM het recht «to remain silent» en «not to incriminate oneself» besloten.[80] *Het recht van de verdachte om zichzelf niet te belasten is «primarily concerned with respecting the will of an accused person to remain silent».*[81]
De ratio van genoemde rechten ligt volgens het EHRM in het beschermen tegen ontoelaatbare dwang door de autoriteiten tegen de wil van de verdachte. Artikel 6 EVRM verzet zich echter niet tegen het gebruik voor het bewijs in een strafzaak van onder dwang door de verdachte afgegeven materiaal dat onafhankelijk van de wil van de verdachte bestaat.[82] *Volgens de Hoge Raad is voor de vraag of het nemo teneturbeginsel is geschonden beslissend of het gebruik tot het bewijs van een (al dan niet in een document vervatte) verklaring van de verdachte in een strafzaak zijn recht om te zwijgen en daarmee zijn recht om zichzelf niet te belasten van zijn betekenis zou ontdoen.*[83]

De Nederlandse wetgever heeft mede op grond van het nemo teneturbeginsel tot nu toe afgezien van de invoering van een decryptiebevel voor verdachten. Met de Wet computercriminaliteit[84] *is in 1993 de mogelijkheid ingevoerd een decryptiebevel te geven aan degene (een derde, niet verdachte) die kennis draagt van de beveiliging (versleuteling) van een geautomatiseerd werk.*[85] *In de wet is bepaald dat het bevel niet mag worden gegeven aan verdachten.*[86] *Zowel bij de Wet computercriminaliteit als de Wet computercriminaliteit II*[87] *(2006) is afgezien van het*

---

[79] Rapport «Het decryptiebevel en het nemo-teneturbeginsel», blz. 88 (interview politie): «Een ontsleutelplicht zou misschien een stukje oplossing kunnen bieden, maar alleen bij bepaalde soorten verdachten; vooral de verzamelaars en/of de categorie «sufferds». Maar die werken nu ook al meestal gewoon mee; ze zijn soms blij dat hun dubbelleven ontdekt is. De hele grote jongens laten zich echt niet afschrikken. Die gebruiken de beste encryptie, [de anonimiseringstechnieken] Tor en proxies, en hebben hun beveiliging 15 lagen hoog opgestapeld; die kun je niet tappen laat staan materiaal in beslag nemen. Die zullen nooit onder strafbedreiging meewerken. Met een ontsleutelplicht zou je dan alleen de middengroep bereiken die tussen de verzamelaars en de grote jongens in zit. Maar dat zijn vaak verdachten die plussen en minnen en dan vaak liever zullen kiezen voor een veroordeling voor niet-meewerken dan het materiaal te ontsluiten en dan het risico te lopen van een hogere straf of TBS.»

[80] EHRM 25 februari 1993, *Funke t. Frankrijk,* nr. 82/1991/334/407; EHRM 17 december 1996, *Saunders* t. VK, nr. 43/1994/490/572, NJ 1997, 699.

[81] EHRM 29 juni 2007, *O'Halloran and Francis t. VK,* nrs. 15809/02 en 25624/02.

[82] EHRM 25 februari 1993, *Funke t. Frankrijk,* nr. 82/1991/334/407; EHRM 17 december 1996, *Saunders* t. VK, nr. 43/1994/490/572, NJ 1997, 699.

[83] HR 21 december 2010, LJN BL0666.

[84] Stb. 1993, 33.

[85] Artikel 125k Sv.

[86] Zo bepaalt artikel 125k, derde lid, Sv. De verschoningsgerechtigden hoeven het bevel niet na te komen.

[87] Stb. 2006, 300.

decryptiebevel aan verdachten.[88] Bij de totstandkoming van de Wet computercriminaliteit II was de regering van oordeel dat de medewerking van verdachten aan ontsleuteling «een stap te ver ging», omdat met het verplicht vertellen van een slechts in het geheugen van de verdachte opgeslagen code of wachtwoord de verklaringsvrijheid en het zwijgrecht van de verdachte in het geding is.[89]
Volgens de toelichting zijn er redenen om te komen tot een andere afweging van het decryptiebevel aan verdachten.[90] Verwezen wordt naar het – in opdracht van het WODC uitgevoerd – rapport «Het decryptiebevel en het nemo teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?» (hierna: rapport).[91] In het rapport wordt geconcludeerd dat het decryptiebevel aan verdachten inbreuk maakt op het nemo teneturbeginsel, maar dat het onder bepaalde – strenge – voorwaarden met dat beginsel verenigbaar is.[92]

b. Toetsingsfactoren EHRM inbreuk nemo teneturbeginsel

In de Europese Unie[93] kennen uitsluitend het Verenigd Koninkrijk en Frankrijk een verplichting voor de verdachte om gegevens te ontsleutelen. Die wettelijke regelingen zijn tot nog toe niet aan het EHRM voorgelegd, zodat het EHRM zich nog niet heeft kunnen uitspreken over de verenigbaarheid van de ontsleutelplicht aan verdachten met het nemo teneturbeginsel. Op basis van de Straatsburgse rechtspraak over artikel 6 EVRM kan echter worden geconcludeerd dat het EHRM beoordeelt of de procedure de kern van het recht om zichzelf niet te belasten van zijn betekenis heeft ontdaan («whether a procedure has extinguished the very essence of the privilege against self-incrimination»).[94] Daarbij slaat het EHRM acht op de volgende factoren:

---

[88] Kamerstukken II 1989/90, 21 551, nr. 3, blz. 28: «Het eerste lid geeft uitwerking aan het beginsel dat de verdachte niet ware te verplichten mee te werken aan zijn eigen veroordeling. Weliswaar bestaan op dit beginsel uitzonderingen, doch deze hebben slechts zin indien er een verhouding valt aan te brengen tussen de straf die kan worden opgelegd wegens niet-nakoming van het bevel en wegens het delict dat voorwerp is van het onderzoek. Deze relatie is bij computercriminaliteit in de regel niet aanwezig, omdat het daarbij kan gaan om zeer ernstige delicten. Een dergelijke verplichting lijkt dan weinig zinvol omdat de naleving ervan in veel gevallen illusoir en niet handhaafbaar zal zijn.»

[89] Kamerstukken II 1998/99, 26 671, nr. 3, blz. 26.

[90] Memorie van toelichting, paragraaf 4.1. De noodzaak en de reikwijdte van de voorgestelde bevoegdheid.

[91] Universiteit van Tilburg, Centrum voor Recht, Technologie en Samenleving (TILT), in opdracht van het WODC, september 2012. In 2000 heeft het Centrum voor Recht, Technologie en Veiligheid van de Universiteit van Tilburg een studie gepubliceerd over het decryptiebevel aan de verdachte. In die studie werd geconcludeerd dat, in het licht van de Nederlandse wetgeving, een ontsleutelplicht voor verdachten in het commune strafrecht een unieke bevoegdheid zou zijn en dat de wetgever daarom zeer zwaarwichtige redenen zou moeten hebben om een dergelijke bevoegdheid in te voeren.

[92] Rapport «Het decryptiebevel en het nemo-teneturbeginsel», blz. 107. Decryptiebevel met strafbaarstelling zal volgens het rapport alleen aanvaardbaar zijn in het licht van artikel 6 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, aldus het rapport.

[93] Australië heeft een decryptiebevel dat zich tot verdachten richt. In de VS bestaat een ontsleutelplicht voor verdachten die zich uitkristalliseert in de rechtspraak. Andere landen die een ontsleutelplicht kennen, zijn Antigua & Barbuda, Ierland, India, Maleisië, Singapore, Thailand, Trinidad & Tobago en Zuid-Afrika. Rapport «Het decryptiebevel en het nemo-teneturbeginsel», blz. 77.

[94] EHRM 5 november 2002, *Allan t. VK*, NJ 2004, 262.

– *de aard en de intensiteit van de dwang («the nature and degree of the compulsion»)*[95]
– *de relevante procedurele waarborgen («the existence of any relevant safeguards in the procedures»)*
– *het gebruik van het materiaal («the use to which any material so obtained is put»)*
– *Het gewicht van het publieke belang bij het opsporen en bestraffen van het concrete strafbare feit («the weight of the public interest in the investigation and punishment of the offence at issue»).*[96]

c. Verenigbaarheid voorgesteld decryptiebevel met het nemo-tenetur beginsel

Voorgesteld wordt van verdachten van kinderpornografie en terrorisme te vorderen dat zij beveiligde gegevens (bewijsmateriaal) toegankelijk maken, waarbij de toegang vrijwel altijd zal bestaan uit een wachtwoord.[97] *Het gaat om een wachtwoord dat niet onafhankelijk van de wil van verdachte kan worden verkregen. Het voldoen door de verdachte aan het bevel kan leiden tot de verkrijging van voor hem belastend bewijsmateriaal door de autoriteiten.*
De Afdeling gaat met de toelichting en het rapport alsmede met de adviesorganen[98] *ervan uit dat het decryptiebevel aan verdachten inbreuk maakt op het nemo teneturbeginsel. Vervolgens moet beoordeeld worden of deze inbreuk gerechtvaardigd kan worden.*

De Afdeling wijst daartoe op het volgende. De strafdreiging met drie jaar gevangenisstraf bij het niet voldoen aan het decryptiebevel levert naar het oordeel van de Afdeling een aanzienlijke mate van dwang op. De toelichting erkent dat.[99] *De Afdeling wijst in dit verband op de jurisprudentie van het EHRM over de druk op terrorismeverdachten om informatie te verstrekken. Volgens het EHRM was de dreiging bij terrorismeverdachten met een gevangenisstraf van 6 maanden om informatie te verstrekken zodanig, dat het recht om zichzelf niet te belasten in de kern was aangetast.*[100] *De terrorismeverdachten werden op straffe van 6 maanden gevangenisstraf verplicht tijdens politieverhoor te verklaren waar zij zich op een bepaald tijdstip bevonden. Allen zijn veroordeeld tot gevangenisstraf van 6 maanden wegens de weigering deze verklaring af te leggen. Het EHRM oordeelde unaniem dat de mate van dwang in deze zaken het recht om zichzelf niet te belasten teniet heeft gedaan. Volgens het rapport*[101] *bestond in de meeste gevallen waarin het EHRM het aanvaardbaar heeft geacht om onder strafbedreiging medewerking af te*

---

[95] EHRM 21 december 2000, *Heaney en McGuinness t. Ierland*, nr. 34720/97. EHRM 21 december 2000, *Quinn t. Ierland,* nr. 36887/97. De zaken betroffen terrorismeverdachten, die op straffe van 6 maanden gevangenisstraf verplicht werden tijdens het politieverhoor te verklaren waar zij zich op een bepaald tijdstip bevonden. Allen zijn veroordeeld tot gevangenisstraf van 6 maanden wegens het weigeren te verklaren. Het EHRM oordeelt unaniem dat de mate van dwang in deze zaken het recht om zichzelf niet te belasten teniet heeft gedaan.

[96] Laatstgenoemd criterium introduceert het EHRM in de zaken *Jalloh* en *O'Halloran and Francis* bij de beoordeling of het recht om zichzelf te belasten is geschonden («whether the applicant's right not to incriminate himself has been violated), naast de reeds genoemde criteria. EHRM 11 juli 2006, *Jalloh t. Duitsland,* nr. 54810/00 en EHRM 29 juni 2007, *O'Halloran and Francis t. VK,* nrs. 15809/02 en 25624/02. Aan het criterium van het publiek belang toetst het EHRM voor het eerst in de uitspraak *Jalloh*; hieruit kunnen evenwel geen algemene uitgangspunten worden gedestilleerd. In *O'Halloran and Francis* is het criterium slechts aangehaald, maar niet nader geconcretiseerd. Het criterium komt nadien niet in de EHRM-jurisprudentie voor.

[97] De decryptiesleutel wordt door het encryptieprogramma opgeslagen op een gegevensdrager en beveiligd met wachtwoord.

[98] Memorie van toelichting, paragraaf 4.6.1. Het beginsel van nemo tenetur.

[99] Memorie van toelichting, paragraaf 4.6.1. Het beginsel van nemo tenetur.

[100] EHRM 21 december 2000, *Heaney en McGuinness t. Ierland*, nr. 34720/97. EHRM 21 december 2000, *Quinn t. Ierland,* nr. 36887/97.

[101] Raport «Het decryptiebevel en het nemo-teneturbeginsel», blz. 94.

dwingen, de dwang uit (niet al te hoge) boetes[102] of maximaal twee dagen gevangenisstraf.[103] Het herhaaldelijk opleggen van boetes is vaak al een ontoelaatbare vorm of mate van dwang.[104] De Afdeling ziet op dit punt spanning tussen het wetsvoorstel en de jurisprudentie van het EHRM. De toelichting gaat op deze jurisprudentie niet in.

Concluderend merkt de Afdeling op dat de toelichting onvoldoende motiveert dat het voorgestelde decryptiebevel «EHRM-proof» is. In de toelichting wordt geen aandacht besteed aan de uitspraken van het EHRM, waaruit blijkt dat een strafbedreiging van 6 maanden gevangenisstraf een zodanige mate van dwang oplevert, dat het recht om zichzelf niet te belasten in de kern is aangetast.

De regering hecht kennelijk veel waarde aan het criterium van het publieke belang. In de toelichting wordt in dat kader benadrukt dat het decryptiebevel is beperkt tot enkele zeer ernstige misdrijven, waarop een vrijheidsstraf van acht jaar of meer is gesteld. De Afdeling merkt op dat het onduidelijk is, welke betekenis in de jurisprudentie van het EHRM over artikel 6 EVRM aan de factor «publiek belang» dient te worden toegekend.[105] Het rapport vermeldt over dit criterium: «In de meeste gevallen lijkt het EHRM weinig gewicht toe te kennen aan het publiek belang, dat in elk geval nooit ingeroepen kan worden om een ernstige mate van dwang (zoals dreiging met geweld) of het gebruik van een afgedwongen verklaring als essentieel bewijselement te rechtvaardigen».[106] Uit de jurisprudentie van het EHRM volgt voorts dat het recht om zichzelf niet te belasten van toepassing is op alle (soorten) strafbare feiten zonder onderscheid, van de meest eenvoudige tot de meest complexe.[107] Voorts kunnen volgens het EHRM de belangen van veiligheid en openbare orde een maatregel, die de kern van het recht zichzelf niet te belasten teniet doet – hetgeen het geval was in genoemde zaken betreffende de terrorismeverdachten – niet rechtvaardigen.[108] Gelet op de jurisprudentie van het EHRM is vooralsnog onzeker of dit criterium voldoende compenserend vermogen heeft ten aanzien van de aanzienlijke mate van dwang; de vermelde uitspraken van het EHRM betroffen terrorismeverdachten. Ook op dit onderdeel schiet de toelichting tekort wat betreft de verenigbaarheid met het nemo teneturbeginsel.
De Afdeling trekt derhalve in twijfel dat de relatief grote waarde die de toelichting aan het criterium «publiek belang» hecht, gerechtvaardigd is gelet op de EHRM-rechtspraak.

De Afdeling adviseert gelet op het bovenstaande dragend te motiveren waarom de voorgestelde regeling van het decyptiebevel in overeenstemming is met de vereisten die op grond van het nemo teneturbeginsel

---

[102] EHRM 29 juni 2007, *O'Halloran and Francis t. VK,* nrs. 15809/02 en 25624/02.
[103] EHRM 10 januari 2008, *Lückhof und Spanner t. Oostenrijk,* nrs. 58452/00 en 61920/00.
[104] EHRM 25 februari 1993, *Funke t. Frankrijk*, nr. 82/1991/334/407; EHRM 3 mei 2001, *J.B. t. Zwitserland,* nr. 31827/96.
[105] De (toenmalige) EHRM-rechter Myjer vermeldt in de dissenting opinion bij de uitspraak *O'Halloran and Francis* het volgende over het «public interest-criterium»: «(...) the majority in fact also seem to play the «public interest» card in the form of a rather tricky new criterion which was first stated in (...) Jalloh v. Germany. (...) This is, moreover, a new criterion which is incompatible with the established case-law that the use of incriminating statements obtained from the accused under compulsion in such a way as to extinguish the very essence of the right to remain silent cannot in principle be justified by reference to the public interest served. EHRM 21 december 2000 zaak nr. 36887/97. Zie voorts D. van Toor, «Het decryptiebevel en het nemo teneturbeginsel», NJB 2013/385.
[106] Rapport «Het decryptiebevel en het nemo-teneturbeginsel», blz. 39.
[107] EHRM 17 december 1996, *Saunders* t. VK, nr. 43/1994/490/572.
[108] EHRM 21 december 2000, *Heaney en McGuinness t. Ierland*, nr. 34720/97. EHRM 21 december 2000, *Quinn t. Ierland*, nr. 36887/97.

voortvloeien uit artikel 6 EVRM of anders dit onderdeel van het wetsvoorstel te schrappen.

9. Overige opmerkingen decryptiebevel

a. Aanscherpen voorwaarden voor de toepassing van het decryptiebevel

Het vigerende artikel 125k Sv, dat ziet op het decryptiebevel aan een derde, bevat de voorwaarden dat redelijkerwijs kan worden vermoed dat de verdachte kennis draagt van de wijze van beveiliging van een geautomatiseerd werk en voorts dat het waarschijnlijk is dat de versleutelde gegevens verband houden met het strafbare feit. De Afdeling merkt op dat de voorgestelde regeling van het decryptiebevel aan de verdachte[109] deze voorwaarden niet bevat. Daarmee is de voorgestelde bepaling niet afdoende afgebakend.

De Afdeling adviseert de voorgestelde regeling van het decryptiebevel in vorenbedoelde zin aan te scherpen.

b. Voorlopige hechtenis bij decryptieweigering

Het wetsvoorstel voorziet in de opneming van decryptieweigering door de verdachte in de gevallen waarin voorlopige hechtenis mogelijk is.[110] Vanwege de ernst van de achterliggende strafbare feiten en het belang dat de verdachte aan een decryptiebevel gevolg geeft, is het wenselijk dat de verdachte voorlopig van zijn vrijheid kan worden beroofd, zolang hij geen gevolg geeft aan een dergelijk bevel, aldus de toelichting.[111] Hiermee wordt volgens de toelichting gevolg gegeven aan het advies van het College van Procureurs-Generaal.

De Afdeling ziet niet goed in waarom in geval van het niet voldoen (door de verdachte) aan het decryptiebevel voorlopige hechtenis zou moeten kunnen worden bevolen, aangezien de gronddelicten waarvoor het decryptiebevel kan worden toegepast (gekwalificeerde kinderpornografie en terrorisme) strafbare feiten zijn waarvoor reeds voorlopige hechtenis mogelijk is. Het komt de Afdeling voor dat een toevoeging als voorgesteld overbodig is. Voorts merkt de Afdeling op dat uit het advies van het College van Procureurs-Generaal niet blijkt, dat zij een aanvulling van artikel 67 Sv met decryptieweigering wenselijk heeft geacht. Ten slotte wijst de Afdeling erop dat «het belang dat de verdachte aan een decryptiebevel gevolg geeft» geen grond is voor voorlopige hechtenis in de zin van artikel 67a Sv. Voorlopige hechtenis mag niet worden toegepast als pressiemiddel. Dit blijkt uitdrukkelijk uit artikel 67a, tweede lid, Sv. Daarin is als grond genoemd dat voorlopige hechtenis «redelijkerwijze noodzakelijk is voor het, anders dan door verklaringen van de verdachte, aan de dag brengen van de waarheid.»

De Afdeling adviseert de voorgestelde aanvulling van artikel 67 Sv met de decryptieweigering te schrappen.

---

[109] Voorgesteld artikel 125k, vierde lid, Sv.

[110] Voorgestelde wijziging van artikel 67 Sv. Vanwege de voorgestelde strafbedreiging van drie jaar gevangenisstraf voor het opzettelijk niet voldoen aan het decryptiebevel, is voorlopige hechtenis op grond van artikel 67 Sv niet mogelijk.

[111] Memorie van toelichting, Artikelsgewijze toelichting op Artikel II, onderdeel A, van het wetsvoorstel.

B. Decryptiebevel aan de verdachte

7. Noodzaak en effectiviteit decryptiebevel

a. en b. Noodzaak en effectiviteit

De Afdeling onderschrijft het streven van de regering om kinderpornografie en terrorisme te bestrijden maar maakt kanttekeningen bij het voorgestelde decryptiebevel aan verdachten. In de eerste plaats is onduidelijk wat de omvang van het probleem is, dit geldt in het bijzonder voor verdachten van terroristische misdrijven. In de tweede plaats kan de voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen in een geautomatiseerd werk ertoe leiden dat de behoefte aan het decryptiebevel voor verdachten vermindert. Verder is de Afdeling niet overtuigd van de effectiviteit van het decryptiebevel aan de verdachte.

8. Verenigbaarheid decryptiebevel met het nemo teneturbeginsel

a. en b. Het nemo teneturbeginsel en toetsingsfactoren EHRM inbreuk nemo teneturbeginsel

De Afdeling merkt op dat de Nederlandse wetgever tot nu toe mede op grond van het nemo teneturbeginsel heeft afgezien van de invoering van een decryptiebevel voor verdachten. De Afdeling wijst er op dat in de Europese Unie alleen het Verenigd Koninkrijk en Frankrijk een verplichting voor de verdachte kennen om gegevens te ontsleutelen.

c. Verenigbaarheid voorgesteld decryptiebevel met het nemo-teneturbeginsel

De Afdeling gaat er met de toelichting en het rapport alsmede met de adviesorganen van uit dat het decryptiebevel aan verdachten inbreuk maakt op het nemo teneturbeginsel. Vervolgens moet beoordeeld worden of deze inbreuk gerechtvaardigd kan worden. Daarbij wijst de Afdeling op de spanning tussen de voorgestelde strafbedreiging van drie jaar en de jurisprudentie van het EHRM over de druk op terrorismeverdachten, op grond waarvan de dreiging met een gevangenisstraf van zes maanden om informatie te verstrekken zodanig was dat het recht om zichzelf niet te belasten in de kern was aangetast. Gelet op die jurisprudentie is onzeker of het criterium van het publieke belang voldoende compenserend vermogen heeft ten aanzien van de aanzienlijke mate van dwang.

Gelet hierop adviseert de Afdeling dragend te motiveren waarom de voorgestelde regeling van het decryptiebevel in overeenstemming is met de vereisten die op grond van het nemo teneturbeginsel voortvloeien uit artikel 6 EVRM of anders dit onderdeel van het wetsvoorstel te schrappen.

Naar aanleiding van het advies is het voorstel voor het decryptiebevel aan verdachten geschrapt. De door de Afdeling gemaakte kanttekeningen op het gebied van de effectiviteit van het decryptiebevel en de verhouding met het nemo teneturbeginsel hebben mij tot de overtuiging gebracht dat het de voorkeur verdient dit voorstel te schrappen. Het wetsvoorstel is dienovereenkomstig aangepast. De opvatting van de Afdeling, dat de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk ertoe kan leiden dat de behoefte aan het decryptiebevel aan verdachten vermindert, kan ik delen. In het geval van versleuteling van elektronische gegevens biedt de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk de mogelijkheid om de gegevens op afstand heimelijk over te nemen en vast te leggen, zodat de versleuteling ongedaan gemaakt kan worden. De inzet van deze bevoegdheid

biedt de meeste kans 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 en maatregelen kan treffen om het onderzoek te frustreren. Vanwege deze redenen geef ik de voorkeur aan de bevoegdheid van het onderzoek in een geautomatiseerd werk boven handhaving van het voorstel van het decryptiebevel aan verdachten.

9. Overige opmerkingen decryptiebevel

Vanwege de schrapping van het voorstel voor een decryptiebevel aan de verdachte behoeven deze opmerkingen geen reactie.

C. Strafbaarheid corrumperen minderjarigen en grooming

10. De virtuele «lokpuber»

Ingevolge het voorstel kan ten behoeve van de opsporing van corrumperen van minderjarigen en grooming (het voorstellen van een ontmoeting aan iemand die de leeftijd van zestien jaar nog niet heeft bereikt) gebruik worden gemaakt van opsporingsambtenaren, die zich voordoen als pubers (de zogenaamde «lokpubers»). De jurisprudentie omtrent de strafbaarstelling van grooming maakt de inzet van opsporingsambtenaren als «lokpubers» tot nu toe niet mogelijk; de delictsomschrijving van grooming, wordt door het gebruik van een «lokpuber» die ouder is dan zestien jaar niet vervuld, aldus het Gerechtshof te Den Haag.[112]

De Afdeling adviseert de voorgestelde bepalingen in het licht van het bovenstaande aan te passen.

11. Strafbaarheid poging tot grooming

Grooming is strafbaar gesteld met het bestaande artikel 248e Sr. De toelichting vermeldt dat bij wet de strafbaarheid van poging tot grooming niet is uitgesloten. Daarvan kan volgens de toelichting sprake zijn als de communicatie heeft geleid tot het voorstel voor een ontmoeting; er hoeft geen handeling te zijn ondernomen die gericht is op het verwezenlijken van die ontmoeting. Het voorstel voor de ontmoeting met het oogmerk ontuchtige handelingen te plegen of een afbeelding van een seksuele gedraging te vervaardigen waarbij het slachtoffer is betrokken, vormt dan het begin van uitvoering van het delict grooming, aldus de toelichting.[113] De Afdeling merkt op dat het voorliggende wetsvoorstel geen wijziging aanbrengt die ziet op de strafbaarheid van poging tot grooming. De toelichting op het huidige voorstel kan voor het al dan niet strafbaar zijn van poging tot grooming dan ook geen bepalende rol spelen.

De Afdeling wijst erop dat de jurisprudentie met betrekking tot de (on)mogelijkheid van de strafbaarheid van een poging tot grooming niet eenduidig is.[114] De toelichting vermeldt deze jurisprudentie niet. Daarmee gaat zij met name voorbij aan de uitspraak van de rechtbank Amsterdam, die zich op het standpunt heeft gesteld dat poging tot grooming niet

---

[112] Gerechtshof Den Haag 25 juni 2013, NJ 2014, 123.
[113] Memorie van toelichting, artikelsgewijze toelichting, artikel I, onderdeel H.
[114] Uitspraak van Rechtbank Amsterdam, 2 juli 2013, ECLI:NL:RBAMS:2013:4000, anders: Rechtbank Oost-Brabant, 13 juni 2013, nr. ECLI:NL:RBOBR:2013:CA2959.

strafbaar is.[115] De rechtbank leidt uit de wetsgeschiedenis van artikel 248e Sr af dat de wetgever grooming strafbaar heeft willen stellen vanaf het moment dat het zich concretiseert tot een voorstel voor een ontmoeting met het kind gevolgd door «material acts leading to a meeting».[116] Een verdere verschuiving van de strafbaarheid naar de voorfase zou betekenen dat het loutere internetcontact, hoe laakbaar ook, strafbaar zou zijn. Dat zou te ver voeren, aldus de rechtbank. Daarmee sluit de rechtbank aan bij de wetsgeschiedenis van de strafbaarstelling van grooming.[117] De rechtbank sluit daarmee tevens aan bij de tekst van het verdrag van Lanzarote waarop de strafbaarstelling van grooming is gebaseerd.[118]

De Afdeling merkt op dat de strafbaarstelling van grooming ziet op de intentie van de dader, en niet op de initiële communicatie tussen de dader en het slachtoffer. Hoewel het ontuchtig oogmerk van de voorgestelde ontmoeting vast te stellen moet zijn, hoeft deze communicatie op zichzelf geen ontuchtig karakter te hebben. Dit is dan ook de achtergrond van het feit dat het voorstellen van een ontmoeting zonder aanvullende handelingen niet strafbaar is gesteld.[119] Het strafbaar stellen van een poging tot grooming, hetgeen in zichzelf reeds een strafbare poging tot ontucht betreft, zou in wezen leiden tot de strafbaarstelling van een poging tot een poging. Daarmee raakt men dermate ver verwijderd van hetgeen als strafwaardig gedrag kan worden aangemerkt, dat hiervoor een dragende motivering en een uitdrukkelijke wettelijke regeling noodzakelijk is. Beide ontbreken vooralsnog.

Gelet op het voorgaande adviseert de Afdeling de passage in de toelichting met betrekking tot de poging tot grooming te schrappen.

C. Strafbaarheid corrumperen minderjarigen en grooming

10. De virtuele lokpuber

De Afdeling adviseert het wetsvoorstel zodanig aan te passen, dat daadwerkelijk bereikt wordt dat een virtuele lokpuber kan worden ingezet bij de bestrijding van grooming.

---

115 Volgens de Rechtbank Amsterdam, 2 juli 2013, ECLI:NL:RBAMS:2013:4000 is grooming een (specifieke) voorbereidingshandeling en uit de wetgeschiedenis met betrekking tot de algemene strafbaarstelling van voorbereidingshandelingen blijkt dat poging tot voorbereiding en voorbereiding tot voorbereiding van een misdrijf geen strafbaarheid kunnen vestigen. Zie Kamerstukken II 1990/91, 22 268 nr. 3, blz. 13: «(...) zoals thans poging tot poging straffeloos is, zal in de toekomst poging tot voorbereiding en voorbereiding tot voorbereiding evenmin strafbaarheid kunnen vestigen.»

116 Kamerstukken II 2008/09, 31 810 nr. 3, blz. 6–7.

117 «De strafbaarstelling (...) vereist dat het gedrag van de dader zich concretiseert tot een voorstel voor een ontmoeting met het kind gevolgd door «material acts leading to a meeting». Er is voor strafbaarheid derhalve meer nodig dan het uitsluitend op internet communiceren met een kind en het daarbij maken van seksuele toespelingen. Een zodanige verschuiving van de strafbaarheid naar de voorfase zou te ver voeren en is bovendien niet goed handhaafbaar. Voor de strafwaardigheid is het wezenlijk dat de communicatiefase uitmondt in een voorstel voor een ontmoeting en het verrichten van een handeling gericht op het realiseren van die ontmoeting. Deze gedragingen onderstrepen de vastheid van het voornemen van de dader om zijn digitaal misbruik daadwerkelijk om te zetten in het plegen van fysiek misbruik. Van strafbaarheid kan bijvoorbeeld sprake zijn wanneer de dader zich begeeft naar de voor de ontmoeting afgesproken plek, het slachtoffer van een routebeschrijving naar die plek voorziet of anderszins concrete voorbereidingen treft gericht op het verwezenlijken van de ontmoeting.» Kamerstukken II 2008/09, 31 810, nr. 3, blz. 6–7. Zie ook Kamerstukken II 2008/09, 31 810, nr. 7, blz. 4.

118 Verdrag van 25 oktober 2007 van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, Trb. 2008, 58.

119 R. Kool, *Prevention by all means? A legal comparison of the criminalization of online grooming and its enforcement*, Utrecht Law Review, vol. 7, nr. 3 2011, blz. 49.

Het advies van de Afdeling om het voorgestelde artikel 248e Sr aan te passen omdat anders niet bereikt wordt dat bij de bestrijding van grooming de virtuele lokpuber (animatie van een minderjarige) kan worden ingezet omdat de delictsomschrijving uitgaat van «een persoon», is niet overgenomen. Anders dan de Afdeling kennelijk uit de toelichting lijkt af te leiden, wordt bij de inzet van lokpubers geen gebruik gemaakt van virtuele personen. In de toelichting is verduidelijkt dat bij de inzet van een lokpuber altijd een natuurlijke persoon betrokken is. Voor het leggen van contact via chatsites of via communicatiemiddelen wordt een profiel of een chatnaam aangemaakt waaraan een profielfoto gekoppeld kan zijn. Deze profielfoto kan een willekeurige foto of afbeelding zijn. De communicatie vindt plaats met een natuurlijke persoon, een opsporingsambtenaar, die achter het profiel schuil gaat.

11. Strafbaarheid poging tot grooming

De Afdeling adviseert om de passage in de memorie van toelichting met betrekking tot de poging tot grooming te schrappen.

Anders dan de Afdeling ben ik van mening dat voor de strafbaarstelling van een poging tot grooming geen uitdrukkelijke wettelijke regeling noodzakelijk is. Artikel 24 van het op 25 oktober 2007 te Lanzarote tot stand gekomen Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (Trb. 2008, 58) verplicht verdragspartijen tot het strafbaar stellen van poging tot (onder andere) grooming, tenzij een partij zich het recht heeft voorbehouden de poging niet toe te passen (artikel 24, derde lid). Nederland heeft zich in het kader van het ratificatietraject van het verdrag (Kamerstukken II 31 808, nr. 3; artikelsgewijze toelichting bij artikel 24), onder verwijzing naar artikel 45 Sr, op het standpunt gesteld dat poging tot het plegen van misdrijven in Nederland strafbaar is. Er is geen gebruik gemaakt van de uitzonderingsmogelijkheid die het verdrag biedt. Bij wet is de strafbaarheid van de poging tot grooming derhalve niet uitgesloten. Naar aanleiding van het advies is de toelichting aangevuld.

D. Overige opmerkingen

12. Definitie geautomatiseerde werken

Voorgesteld wordt de bestaande definitie van geautomatiseerd werk in het Wetboek van Strafrecht te verruimen en daartoe de definitie van «informatiesysteem» uit de Richtlijn 2013/40/EU over aanvallen op informatiesystemen (hierna: richtlijn) over te nemen.[120] Anders dan de vigerende definitie van geautomatiseerd werk in het Wetboek van Strafrecht[121], die ziet op fysieke apparaten[122], omvat de definitie van «informatiesysteem» in de richtlijn mede de computergegevens die op het apparaat zijn opgeslagen. De toelichting stelt dat het overnemen van de begripsomschrijving van de richtlijn in de rede ligt vanwege de juridische verplichting tot implementatie daarvan.[123]
De Afdeling merkt allereerst op dat richtlijn 2013/40/EU strekt tot vervanging van Kaderbesluit 2005/222/JBZ van de Raad waarin een gelijkluidende definitie van informatiesysteem was opgenomen. Dit

---

[120] Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van kaderbesluit 2005/222/JBZ van de Raad (PbEU L 218/8).

[121] Een geautomatiseerd werk is in artikel 80sexies Sr gedefinieerd als: inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.

[122] Onder geautomatiseerd werk vallen volgens de Hoge Raad tevens netwerken van computers. HR 26 maart 2013, LJN BY9718.

[123] Memorie van toelichting, artikelsgewijze toelichting op artikel I, onderdeel B, van het voorstel.

Kaderbesluit is geïmplementeerd door middel van het wetsvoorstel Computercriminaliteit II.[124] Daarbij is aangenomen dat de bestaande definitie van geautomatiseerd werk voldeed ter uitvoering van het Kaderbesluit alsmede het Cybercrimeverdrag.[125] Dat thans alsnog wordt gekozen voor het overnemen van de definitie uit de richtlijn behoeft naar het oordeel van de Afdeling in zoverre een nadere motivering.

Voorts wijst de Afdeling erop dat zowel de bestaande definitie van geautomatiseerd werk als de toelichting ervan uitgaan dat onder geautomatiseerd werk apparaten worden verstaan[126] (computers, servers, modems, routers, smartphones en tablets), die op basis van een programma gegevens verwerken.[127] Volgens de voorgestelde definitie valt onder geautomatiseerd werk zoals vermeld echter niet enkel het apparaat, maar tevens de computergegevens die met dat apparaat worden opgeslagen, verwerkt, opgehaald of verzonden.
De Afdeling merkt op dat «apparaten» en «computergegevens» verschillende grootheden betreffen. De betekenis van de toevoeging van «computergegevens», en de betekenis daarvan voor de bestaande strafbaarstellingen en opsporingsbevoegdheden waarin de term «geautomatiseerd werk» is opgenomen, worden in de toelichting niet nader toegelicht. De voorgestelde bevoegdheid tot het binnendringen van een geautomatiseerd werk bijvoorbeeld kan worden aangewend met het oog op het vaststellen van de aanwezigheid van gegevens en het overnemen ervan; onduidelijkheid ontstaat als het geautomatiseerd werk moet worden begrepen als het apparaat alsmede de computergegevens. Bovendien is onduidelijk hoe het begrip «computergegevens» zich verhoudt tot de bestaande definitie van het begrip «gegevens» in het Wetboek van Strafrecht.[128]
In het licht van het voorgaande is de betekenis en de reikwijdte van de voorgestelde bepaling naar het oordeel van de Afdeling vooralsnog onvoldoende duidelijk.
De Afdeling merkt nog op dat het College van procureurs-generaal adviseerde[129] aan te sluiten bij de, duidelijkere, definitie die wordt gehanteerd in het Cybercrimeverdrag.[130] Waarom deze aanbeveling niet is gevolgd blijkt niet uit de toelichting.

De Afdeling adviseert af te zien van het opnemen van het begrip «computergegevens» in de definitie van geautomatiseerd werk. Voorts adviseert de Afdeling op de andere hiervoor gemaakte opmerkingen in de toelichting in te gaan en zo nodig het voorstel aan te passen.

13. Strafbaarstelling online handelsfraude

De strafbaarstelling van online handelsfraude is gemodelleerd naar de strafbaarstelling van flessentrekkerij (artikel 326a Sr). Uit de delictsomschrijving van artikel 326a Sr volgt dat het oogmerk erop gericht moet zijn om niet volledig te betalen. Hiermee wordt voorkomen dat het verweer

---

124 Stb. 2006, 300. Kamerstukken 26 671.
125 Trb. 2002, 18.
126 Dan wel netwerken van apparaten.
127 Memorie van toelichting, artikelsgewijze toelichting op artikel I, onderdeel B, van het voorstel.
128 Onder gegevens wordt volgens artikel 80quinquies Sr verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.
129 Advies College van Procureurs-Generaal, blz. 10.
130 In het Cybercrimeverdrag zijn afzonderlijke definities opgenomen voor een computersysteem en voor computergegevens. In artikel 1, onder a, van het verdrag is de definitie van een computersysteem beperkt tot: «any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.»

kan worden gevoerd dat de verdachte wel de bedoeling had om volledig te betalen, blijkend uit een gedeeltelijke betaling.
In de voorgestelde strafbaarstelling van online handelsfraude is een vergelijkbare nuancering niet opgenomen: verwezen wordt naar het oogmerk om de goederen of diensten na betaling niet te leveren. In de toelichting is wel vermeld dat ook de intentie om na betaling gedeeltelijk te leveren kan worden aangemerkt als het oogmerk om na betaling niet te leveren. Dit volgt evenwel niet dwingend uit de tekst van het voorstel. Uit het oogpunt van rechtszekerheid en het nulla poenabeginsel is aanvulling van de bepaling nodig.

De Afdeling adviseert in artikel 326d Sr tot uitdrukking te brengen dat tevens het oogmerk om niet volledig te leveren voldoende is om de delictsomschrijving te vervullen.

14. Consultatie

De Afdeling merkt op dat twee onderdelen van het wetsvoorstel niet ter advisering zijn voorgelegd aan organisaties zoals de Nederlandse vereniging voor rechtspraak, het College van Procureurs-Generaal, de Raad voor de rechtspraak en de Nederlandse Orde van Advocaten, wier advies voor de kwaliteit van de wetgeving van belang wordt geacht. Het betreft de verruiming van de strafbaarheid van het corrumperen van minderjarigen en grooming alsook de strafbaarstelling van online handelsfraude.

In de toelichting wordt uiteengezet waarom deze onderdelen na de consultatie aan het wetsvoorstel zijn toegevoegd en de relatie aangegeven met de overige onderdelen van het wetsvoorstel. De Afdeling is van oordeel dat over de genoemde onderdelen van het wetsvoorstel alsnog advies dient te worden gevraagd aan de genoemde instanties omdat naar haar oordeel deze adviezen, gelet op de inhoud van de voorgestelde wijzigingen, niet kunnen worden gemist. De Afdeling adviseert daartoe.

15. Redactionele opmerkingen

De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

D. Overige opmerkingen

12. Definitie geautomatiseerde werken

Naar aanleiding van het advies van de Afdeling is de definitie van geautomatiseerd werk aangepast, daarbij is de verwijzing naar het begrip «computergegevens» geschrapt. Dit heeft tevens aanleiding gegeven tot aanvulling van de toelichting

13. Strafbaarstelling online handelsfraude

De Afdeling adviseert om in de strafbaarstelling van online handelsfraude tot uitdrukking te brengen dat tevens het oogmerk om niet volledig te leveren voldoende is om het delictsomschrijving te vervullen.

Naar aanleiding van het advies is het voorgestelde artikel 326d Sr, dat strekt tot strafbaarstelling van online handelsfraude, aangepast. Daarbij is tot uitdrukking gebracht dat tevens het oogmerk om niet volledig te leveren voldoende is om de delictsomschrijving te vervullen. Mede naar aanleiding van een advies van de Raad van de rechtspraak is in de delictsomschrijving meer de nadruk gelegd op het oogmerk, zodat de

strafbaarheid al intreedt als er nadeel kan ontstaan. Hiervoor is niet vereist dat daadwerkelijk betaling heeft plaatsgevonden.

14. Consultatie

De Afdeling merkt op dat twee onderdelen van het wetsvoorstel niet ter advisering zijn voorgelegd aan organisaties wier advies voor de kwaliteit van de wetgeving van belang wordt geacht.

Naar aanleiding van het advies zijn de betreffende onderdelen van het wetsvoorstel, te weten de verruiming van de strafbaarheid van het corrumperen van minderjarigen en grooming (1) en de strafbaarstelling van online handelsfraude (2), voor advies voorgelegd aan de Nationale Politie, de Nederlandse vereniging voor rechtspraak, het College van procureurs-generaal, de Raad voor de rechtspraak, de Nederlandse Orde van Advocaten en het College bescherming persoonsgegevens. De adviezen van deze instanties zijn betrokken bij het wetsvoorstel.

15. Redactionele opmerkingen

Aan de eerste redactionele opmerking is gevolg gegeven. In de toelichting is daar waar wordt verwezen naar artikelen uit het EVRM, tevens aandacht besteed aan de corresponderende artikelen van het Handvest van de grondrechten.

Aan de tweede redactionele opmerking is gevolg gegeven. In de artikelsgewijze toelichting is geëxpliciteerd aan wie het beklagrecht toekomt, dit is ook de verdachte zelf tegen wie het decryptiebevel is gericht.

16. Overige

Van de gelegenheid is gebruik gemaakt om de voorgestelde wijziging van artikel 248d Sr (seksueel corrumperen), waarmee beoogd werd om mogelijk te maken dat de lokpuber kan worden ingezet in situaties waarin het corrumperen langs digitale weg plaatsvindt, te schrappen. Uit een advies van het College van procureurs-generaal is gebleken dat aan een verruiming van de strafbaarheid van het corrumperen van minderjarigen geen behoefte bestaat, nu in de praktijk voor dit feit geen lokpuber wordt ingezet.

In plaats daarvan wordt voorgesteld artikel 248a Sr, dat de verleiding van een minderjarige tot ontucht strafbaar stelt, te wijzigen om de inzet van de lokpuber mogelijk te maken. Het College van procureurs wijst erop dat in veel gevallen waarin verdachten minderjarigen via internet benaderen met het oog op seksuele doeleinden het uiteindelijke doel niet (uitsluitend) het hebben van ontmoeting is, maar het plegen van ontuchtige handelingen door de minderjarige voor de webcam. Het College wijst erop dat dergelijke handelingen soms vergaande consequenties kunnen hebben, wanneer bijvoorbeeld het beeldmateriaal door «groomers» – waaronder zogenaamde loverboys – wordt gebruikt om slachtoffers te chanteren en aan te zetten tot verdergaande seksuele handelingen, zoals gedwongen prostitutie. Om dit schadelijke gedrag tegen te gaan is de inzet van de lokpuber gewenst. Voorgesteld wordt artikel 248a Sr zodanig te wijzigen dat ook het opzettelijk bewegen van iemand die zich voordoet als iemand die de leeftijd van achttien jaren nog niet heeft bereikt tot het plegen of dulden van ontuchtige handelingen strafbaar is.

De Afdeling advisering van de Raad van State geeft U in overweging het voorstel van wet niet te zenden aan de Tweede Kamer der Staten-Generaal dan nadat met het vorenstaande rekening zal zijn gehouden.

De vice-president van de Raad van State,
J.P.H. Donner

Ik moge U verzoeken het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

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

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no. W03.14.0055/II

– In de toelichting, daar waar wordt verwezen naar artikelen uit het EVRM, tevens aandacht besteden aan de corresponderende artikelen van het Handvest van de grondrechten van de Europese Unie, voor zover de voorgestelde maatregelen bedoeld zijn om overtredingen van Unierecht op te sporen (arrest van het Hof van Justitie van 26 februari 2013, Åkerberg Fransson (C-617–10)). Zie in dit verband ook artikel 15, derde lid, van richtlijn 2011/92/EU van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en Kaderbesluit van de Raad van 13 juni 2002, gewijzigd bij Kaderbesluit 2008/919/JBZ van de Raad van 28 november 2008 inzake terrorismebestrijding.
– In de artikelsgewijze toelichitng op artikel II, onderdeel P, expliciteren dat het beklagrecht toekomt aan de verdachte zelf tegen wie het decryptiebevel is gericht.