Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

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)

D

MEMORIE VAN ANTWOORD

Ontvangen 12 juni 2017

1. Inleiding

Met veel belangstelling heb ik kennisgenomen van de opmerkingen en vragen van de leden van de fracties van de VVD, het CDA, D66, de SP, de PvdA, GroenLinks en de ChristenUnie over dit wetsvoorstel. De ontwikkeling van de informatie- en communicatietechnologie stelt de instanties die zijn belast met de bescherming van burgers tegen criminaliteit, in toenemende mate voor uitdagingen. Recente rapporten onderschrijven de zorg van politie en justitie dat de omvang van cybercrime groeit en dat er behoefte is aan meer bevoegdheden voor de opsporing om de dreiging te adresseren. Voor een schets van de omvang van cybercrime en de onderkenning van de urgentie kan worden gewezen op het rapport van het Rathenau instituut[1], de commissie Verhagen[2], het Cybersecuritybeeld Nederland[3] dat jaarlijks wordt gepubliceerd, en de veiligheidsmonitor[4]. Voor de omvang en urgentie op Europees niveau kan worden gewezen op The Internet Organised Crime Threat Assessment (IOCTA)[5], alsook het Serious and Organised Crime Threat Assessment (SOCTA)[6]. De regering onderkent deze behoefte. Het internet mag geen vrijhaven worden voor criminelen en er moet recht worden gedaan aan slachtoffers. Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet. Dit wetsvoorstel is hiervoor van essentieel belang. Ik hoop dat met de beantwoording van de vragen ook de bezwaren van de fracties die hun bezorgdheid over dit wetsvoorstel kenbaar hebben gemaakt,

[1] Rathenau instituut (2017) Een nooit gelopen race: Over cyberdreigingen en versterking van de weerbaarheid. Zie in het bijzonder hoofdstuk 2.

[2] Verhagen, H. (2016) Nederland droge digitale voeten: De economische en maatschappelijke noodzaak van meer Cybersecurity. In het bijzonder paragraaf 1.2. over de aantrekkelijkheid van Nederland voor cybercriminelen.

[3] Nationaal Cyber Security Centrum (2016) Cybersecuritybeeld Nederland.

[4] CBS en het Ministerie van Veiligheid en justitie (2017) Veiligheidsmonitor 2016.

[5] Europol (2016) The Internet Organised crime threat assessment.

[6] Europol (2017) Serious and Organised Crime Threat Assessment. met als ondertitel crime in the age of technolology. In het bijzonder in de conclusies op blz. 56, waarin wordt beschreven dat technologie functioneert als katalysator voor criminele activiteiten en daarvoor een bijzonder faciliterende rol vervult.

kst-34372-D
ISSN 0921 - 7371
's-Gravenhage 2017

onder meer vanwege de proportionaliteit van het wetsvoorstel en de impact op de privacy van burgers, kunnen worden weggenomen.

2. Reikwijdte van het wetsvoorstel

De leden van de fractie van de SP hebben hun teleurstelling uitgesproken over het feit dat de regering twee totaal verschillende problemen, namelijk de toegenomen computercriminaliteit en het gebruik van digitale middelen bij traditionele criminaliteit, heeft proberen te vatten in één wetsvoorstel. Zij hebben gevraagd of de regering kan toelichten waarom zij beide terreinen in een wetsvoorstel heeft willen vatten.

Computercriminaliteit heeft niet uitsluitend betrekking op het handelen in de digitale dimensie, en kan niet strikt worden gescheiden van het handelen in de fysieke wereld. Beide dimensies lopen in elkaar over en werken op elkaar in. Voor de aanpak van computercriminaliteit zijn nieuwe bevoegdheden nodig. De ontwikkeling van de informatie- en communicatietechnologie biedt de criminaliteit nieuwe mogelijkheden voor het plegen van strafbare feiten. Deze mogelijkheden hebben betrekking op verschillende aspecten. Dit betreft bijvoorbeeld de verandering in de wijze waarop de burgers met elkaar communiceren. Het verhandelen van goederen en diensten op internet wordt vergemakkelijkt door de mogelijkheden van digitale communicatie, maar heeft een navenant effect op vormen van fraude of zedenmisdrijven. Tevens biedt de informatie- en communicatietechnologie meer mogelijkheden om het handelen af te schermen, zoals het gebruik van encryptie. De nieuwe bevoegdheden zijn daarmee effectief in het digitale en fysieke domein. Tenslotte zijn de strafbaarstellingen niet meer voldoende toegesneden op de technologische ontwikkeling; daarvoor kan worden gewezen op de in dit wetsvoorstel voorgestelde strafbaarstelling van een delict als het overnemen en helen van gegevens. Deze verschillende aspecten hebben een gezamenlijk kenmerk, namelijk dat deze onderdeel vormen van de computercriminaliteit. Zoals eerder aangegeven, lopen beide dimensies in elkaar over. Een drugshandelaar die voor zijn communicatie met anderen gebruik maakt van een speciale telefoon waarmee de communicatie wordt versleuteld, handelt in de fysieke en digitale dimensie. Ditzelfde geldt voor de «groomer» die een afspraak maakt met een minderjarige, met het voornemen tot het verrichten van seksuele handelingen. Het Wetboek van Strafvordering en het Wetboek van Strafrecht zijn tot stand gekomen in een tijd waarin de digitale wereld niet bestond. Dit betekent dat de bevoegdheden en strafbaarstellingen periodiek moeten worden herijkt, zodat de samenleving adequaat kan worden beveiligd tegen het handelen van personen die gebruik maken van de informatietechnologie om criminele activiteiten te plegen waarvan anderen het slachtoffer zijn, om te communiceren met medeplegers en om hun handelen van de buitenwereld af te schermen. De keuze van de regering berust op een inventarisatie van de behoeften bij politie en justitie. Zowel bevoegdheden van de politie en justitie als de strafrechtelijke normstelling hebben geen gelijke tred gehouden met de ontwikkeling van de computercriminaliteit en daarom dient aanpassing plaats te vinden.De regering acht alle onderdelen van het wetsvoorstel van essentieel belang voor de bestrijding van computercriminaliteit.

De leden van de fractie van de SP hebben aangegeven zich zorgen te maken dat de hackbevoegdheid de politie meer digitale mogelijkheden biedt dan er nu in de offlinewereld mogelijk zijn. De leden van deze fractie hebben geen kennis genomen van wetsvoorstellen die het mogelijk maken camera's te plaatsen in de huizen van verdachte personen, toch is dit naar hun oordeel het effect van het voorstel van de regering.

Het wetsvoorstel introduceert de bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Hieronder valt de uitvoering van een bevel tot observatie als bedoeld in artikel 126g Sv. De stelselmatige observatie van personen betreft een bestaande opsporingsbevoegdheid. De uitvoering van dit bevel dient plaats te vinden binnen de kaders van artikel 126g Sv. Op basis van deze bevoegdheid is het niet toegestaan heimelijk een woning te betreden of heimelijk een webcam in een woning aan te zetten. Ook op basis van de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk is dit niet mogelijk.

De noodzaak van de voorgestelde uitbreiding van bevoegdheden is de leden van de fractie van de SP niet helemaal duidelijk. De leden van deze fractie hebben gevraagd of de regering kan aangeven hoe groot het probleem is dat het wetsvoorstel moet oplossen en hoeveel zaken er nu niet opgelost kunnen worden maar met deze wetgeving waarschijnlijk wel zouden worden opgelost.

Door de ontwikkeling van het internet en de technologische vooruitgang wordt de opsporing van strafbare gedragingen in toenemende mate lastig of zelfs onmogelijk. Drie wezenlijke problemen en gebleken knelpunten worden onderscheiden. Het betreft ten eerste de toenemende versleuteling van elektronische gegevens. Via het internet is het eenvoudig om vanuit het buitenland met behulp van een geautomatiseerd werk strafbare feiten in Nederland te plegen terwijl gebruik wordt gemaakt van anonimiseringstechnieken zodat de locatie van verzending wordt verhuld of de boodschap wordt versleuteld. Daardoor is het vaak niet mogelijk met andere middelen, zoals aftappen en opnemen van communicatie of het in beslag nemen van voorwerpen, een dader of een geautomatiseerd werk met daarop bewijsmateriaal, te identificeren en voldoende bewijs te vergaren. Om toch effectief te kunnen opsporen moet het in bepaalde uitzonderlijke gevallen mogelijk zijn om gericht in het betreffende systeem te kunnen binnendringen zodat de gegevens kunnen worden verkregen voordat deze worden versleuteld. Ten tweede vormt het toenemende gebruik van draadloze netwerken, van «hotspots» en allerlei vormen van dynamische IP-adressen een obstakel voor het vergaren van bewijs. Bijvoorbeeld omdat wanneer een internettap op een router geplaatst wordt alleen de in- en uitgaande communicatie kan worden afgetapt, maar de interne communicatie op het netwerk niet kan worden onderschept. Daarnaast wordt door een internettap alle in- en uitgaande communicatie afgetapt, ook van personen in wie de opsporing niet geïnteresseerd is. Door identificatie van een geautomatiseerd werk of van de gebruiker door middel van het binnendringen in het geautomatiseerde werk kan meer gericht onderzoek worden gedaan. De derde ontwikkeling betreft de toenemende opslag van informatie in de cloud. Bestaande bevoegdheden als een netwerkzoeking en doorzoeking ter vastlegging van gegevens gaan er in belangrijke mate van uit dat de gegevens die voor de opsporing van belang zijn, zich bevinden op een bepaalde gegevensdrager die zich op een vaste plaats bevindt. Deze situatie strookt echter steeds minder met de werkelijkheid. Dit belemmert de effectiviteit van traditionele opsporingsbevoegdheden, zoals het aftappen en opnemen van communicatie, het vorderen van gegevens bij aanbieders en het vragen van rechtshulp aan andere landen. Voor toepassing van de huidige bevoegdheden rond de inbeslagneming van geautomatiseerde werken is de plaats waar het geautomatiseerde werk zich fysiek bevindt doorslaggevend. Hieronder wordt, in antwoord op vragen van de leden van de fractie van GroenLinks, nader ingegaan op de noodzaak en de bruikbaarheid van bestaande bevoegdheden.

In de inleiding is reeds ingegaan op de beschikbare rapporten waarin de omvang van computercriminaliteit wordt geschetst. Er wordt niet per zaak geregistreerd welke niet-bestaande bevoegdheden tot een meer effectieve opsporing hadden kunnen leiden. De opsporingsdiensten en het openbaar ministerie houden daarom geen cijfers bij over het aantal gevallen waarin gedurende de afgelopen vijf jaar de voorgestelde bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk had kunnen worden ingezet. Wel kan worden verwezen naar in de nota naar aanleiding van het verslag gegeven voorbeelden van opsporingsonderzoeken die niet zijn geslaagd omdat de benodigde gegevens in de cloud niet vastgelegd konden worden, omdat de eigenaar van de server niet (tijdig) reageerde op verzoeken of de gegevens inmiddels waren verdwenen (Kamerstukken II 2016/17, 34 372, nr. 6, blz. 15/16).

3. Proportionaliteit en privacy

De leden van de fractie van de VVD hebben gevraagd in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM), in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer.

Voor de bescherming van grondrechten en het recht op eerbiediging van de persoonlijke levenssfeer is artikel 8 van het Europees Verdrag tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EVRM) van bijzonder belang. De recente jurisprudentie van het Europese Hof tot bescherming van Rechten van de Mens en de fundamentele vrijheden (EHRM) rond het heimelijk vergaren van persoonsgegevens ten behoeve van de opsporing en vervolging van strafbare feiten betreft de arresten in de zaken van Digital Rights Ireland en Seitlinger (zaken C-293/12 en C-294/12), Maximilian Schrems/Data protection Commission (zaak C-362/15), Zakharov tegen Rusland (zaak 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306) en Szabó en Vissy tegen Hongarije (zaak 37138/14). Vooropgesteld moet worden dat deze arresten betrekking hebben op verschillende casus rond het heimelijk verzamelen van persoonsgegevens ten behoeve van zwaarwegende publieke belangen, zoals de bescherming van de nationale veiligheid en de opsporing en vervolging van strafbare feiten. Hier komt bij dat de wettelijke regelingen en systemen rond die casus in de verschillende landen uiteen lopen. Niettemin kunnen uit artikel 8, tweede lid, van het EVRM en de jurisprudentie van het EHRM enkele hoofdlijnen worden afgeleid. Het EHRM toetst een inbreuk op het recht op bescherming van de persoonlijke levenssfeer aan de eisen van legaliteit (voorzienbaarheid bij wet) en noodzakelijkheid. Onder voorzienbaarheid valt niet alleen de vraag of de voorgenomen maatregel is geregeld bij wet, maar ook de vraag of de wet voldoende kwaliteit heeft, dat wil zeggen of de inbreuk voldoende gedetailleerd is uitgewerkt en met effectieve waarborgen is omkleed tegen misbruik. Onder noodzakelijkheid in een democratische samenleving wordt verstaan of de voorgenomen maatregel voldoet aan de vereisten van proportionaliteit (de keuze voor het middel dat in verhouding staat tot het te realiseren doel) en subsidiariteit (de keuze voor het minst ingrijpende middel dat geschikt is om het doel te bereiken), waarbij een beoordeling dient plaats te vinden of de voorgenomen maatregel kan worden gerechtvaardigd door een «pressing social need».

Het voorliggende wetsvoorstel bevat de nodige waarborgen waarmee tegemoet wordt gekomen aan de vereisten die uit de Europese jurisprudentie voortvloeien. De voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt bij wet vastgelegd. Het belang van de opsporing van ernstige strafbare feiten is erkend als een belang dat de inmenging van het openbaar gezag in het

recht op bescherming van de persoonlijke levenssfeer kan rechtvaardigen. Aan het vereiste van de voorzienbaarheid is invulling gegeven door middel van een gedetailleerde wettelijke regeling waarin specifiek is omschreven welke misdrijven aanleiding kunnen geven tot de inzet van de bevoegdheid, een omschrijving van de categorie van personen jegens wie deze bevoegdheid kan worden ingezet en een beperking van de tijdsduur tot vier weken. Hiermee wordt voorzien in een wettelijke regeling die voor de burger voldoende toegankelijk is. De te verrichten onderzoekshandelingen zijn nauwkeurig omschreven en sluiten merendeels aan bij de bestaande bevoegdheden van het Wetboek van Strafvordering. Het EHRM heeft geoordeeld dat, in het licht van de mogelijkheden van de moderne communicatietechnologie, het vereiste van de «noodzaak in een democratische samenleving» zowel betrekking heeft op de bescherming van de democratische instituties in zijn algemeenheid als op het verkrijgen van vitale informatie in het individuele geval (Szabó en Vissy tegen Hongarije, §73).

Met het vereiste van het dringende opsporingsbelang in combinatie met de ernst van de strafbare feiten wordt uitdrukking gegeven aan het vereiste van een strikte noodzaak tot de inzet van de bevoegdheid, zowel in zijn algemeenheid als in het concrete geval. De voorgestelde maatregel is onvermijdelijk om het hoofd te kunnen bieden aan de ontwikkeling van de cybercrime gedurende de afgelopen jaren. Met dit vereiste wordt tevens tot uitdrukking gebracht dat de voorgestelde bevoegdheid in een concreet onderzoek uitsluitend mag worden ingezet als blijkt dat met de bestaande wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt. Er moet sprake zijn van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert en waarvoor voorlopige hechtenis mogelijk is. Voor het verrichten van bepaalde onderzoekshandelingen waarbij het geautomatiseerde werk kan worden doorzocht, is een verdenking nodig van een misdrijf 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. Met deze voorwaarden wordt invulling gegeven aan de eisen van legaliteit (voorzienbaarheid) en noodzaak (proportionaliteit). Vooraf wordt de voorgenomen inzet getoetst door de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. Tevens is voorzien in een toetsing door een onafhankelijke rechter, zowel voorafgaand aan de inzet als achteraf ter terechtzitting. Met het wettelijke vereiste van een voorafgaande rechterlijke toetsing wordt het risico van een willekeurige toepassing van de bevoegdheid uitgesloten. De voorgenomen inzet wordt getoetst aan de proportionaliteit en subsidiariteit. De rechterlijke machtiging is gekoppeld aan een periode van vier weken, voor verlenging is rechterlijke instemming nodig. Met het oog op een zorgvuldige toetsing dient de officier van justitie in het bevel een duidelijke omschrijving van de te verrichten onderzoekshandelingen op te nemen, een omschrijving welk deel van het geautomatiseerde werk en welke categorie van gegevens het betreft en een aanduiding van de aard en functionaliteit van het technische hulpmiddel. Het EHRM hecht veel waarde aan onafhankelijk rechterlijk toezicht voor de beoordeling van de rechtmatigheid van de voorgestelde bevoegdheid. Volgens het EHRM vormt rechterlijk toezicht de beste waarborg voor onafhankelijkheid, onpartijdigheid en een degelijke procedure (Zakharov tegen Rusland, §233; Szabó en Vissy tegen Hongarije, §77: «The Court recalls that the rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.»). Het EHRM wijst er verder op dat rechterlijk toezicht het vertrouwen van de burger versterkt dat de rule of law ook geldt in het domein van geheime surveillance. Met het oog op de enorme

hoeveelheid informatie die ter beschikking staat aan de autoriteiten en de geavanceerde technieken die deze autoriteiten gebruiken, kan de waarde van onafhankelijk toezicht volgens het EHRM niet overschat worden (Szabó en Vissy tegen Hongarije, §79).

Er is verder voorzien in de nodige waarborgen voor een zorgvuldige uitvoering. De uitvoering van het onderzoek is voorbehouden aan deskundige opsporingsambtenaren die onderdeel vormen van een speciaal team, dat organisatorisch is gescheiden van het tactische team. Er zullen keuringseisen worden gesteld aan de inrichting en werking van het technische hulpmiddel dat wordt gebruikt voor het detecteren, registreren en transporteren van gegevens. Er wordt voorzien in de geautomatiseerde vastlegging van gegevens over de uitvoering van de onderzoekshandelingen (logging) met het oog op controle op de uitvoering van de bevoegdheid zodat zowel tijdens het onderzoek als op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van het bevel. Dit wordt vastgelegd in het Besluit onderzoek in een geautomatiseerd werk. Op de uitvoering van het onderzoek in een geautomatiseerd werk door de daartoe aangewezen opsporingsambtenaren wordt, aanvullend op de rechterlijke controle, toezicht uitgeoefend door de Inspectie Veiligheid en Justitie. Ten slotte is voorzien in een verplichting tot notificatie van de betrokkene. Hiervoor is aangesloten bij de bestaande regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv). Het EHRM acht het van groot belang dat de betrokkene achteraf op de hoogte kan komen van de geheime surveillance en genoegdoening kan zoeken voor een eventuele inbreuk op zijn privacy (Zakharov tegen Rusland, §234; Szabó en Vissy tegen Hongarije, §86). In het licht van de bestaande en voorgestelde garanties en waarborgen rond de voorgestelde maatregel voldoet deze naar het oordeel van de regering dan ook ruimschoots aan de vereisten die uit het EVRM voortvloeien, in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer.

De leden van de fractie van de VVD hebben gevraagd in hoeverre het wetsvoorstel spoort met de uitgangspunten en vereisten waarin het wetsvoorstel WIV voorziet, en in hoeverre er verschillen bestaan tussen beide wetsvoorstellen op het terrein van de bescherming van de persoonlijke levenssfeer van de burger. De leden van deze fractie hebben tevens gevraagd om, als er verschillen tussen de beide wetsvoorstellen bestaan, een overzicht van de verschillen en of de regering daarbij uitdrukkelijk wil aangeven waarom die verschillen tussen beide wetsvoorstellen bestaan.

Het voorliggende wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te versterken. In dat kader wordt voorgesteld een nieuwe bevoegdheid voor de officier van justitie te creëren om onder voorwaarden een geautomatiseerd werk, dat in gebruik is bij een verdachte, op afstand heimelijk binnen te laten dringen door de daartoe aangewezen opsporingsambtenaren met het oog op het verrichten van bepaalde onderzoekshandelingen (onderzoek in een geautomatiseerd werk). Daarbij gaat het deels om reeds bestaande bevoegdheden. Het heimelijk binnendringen in een geautomatiseerd werk is noodzakelijk geworden door de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens.

Het wetsvoorstel op de inlichtingen- en veiligheidsdiensten 20xx (Kamerstukken I 2016/17, 34 588, A) voorziet in modernisering van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze

modernisering is ingegeven door technologische en maatschappelijke ontwikkelingen, zoals de snelle opkomst en mondiale verspreiding van digitale technologie en het internet, in combinatie met het veranderende dreigingsbeeld.

Een belangrijk verschil tussen het voorliggende wetsvoorstel en het wetsvoorstel Wiv 20xx betreft de reikwijdte. Het voorliggende wetsvoorstel voorziet in opneming in het Wetboek van Strafvordering van een nieuwe bevoegdheid voor de officier van justitie, te weten het bevelen dat een daartoe aangewezen opsporingsambtenaar op afstand heimelijk binnendringt in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Het wetsvoorstel Wiv 20xx voorziet in modernisering van de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), zodat deze diensten hun wettelijke taken op het gebied van de bescherming van de nationale veiligheid beter kunnen uitvoeren. Dit betreft algemene bevoegdheden inzake de verzameling van gegevens, zoals het al dan niet stelselmatig verzamelen van gegevens over personen uit open bronnen en de raadpleging van informanten, alsmede bijzondere bevoegdheden tot verzameling van gegevens, zoals het observeren en volgen, de inzet van agenten, het onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek, het openen van brieven, het verkennen van en binnendringen in geautomatiseerde werken, het onderzoek van communicatie (gerichte en onderzoeksopdrachtgerichte interceptie van communicatie alsmede het opvragen van communicatiegegevens).

Wat betreft de bescherming van de persoonlijke levenssfeer zijn de uitgangspunten en vereisten waarin de beide wetsvoorstellen voorzien, deels gelijk en deels verschillend. De gelijkenis wordt ingegeven doordat de beide wetsvoorstellen voorzien in bevoegdheden voor de overheid om, met het oog op de bescherming van een algemeen belang, inbreuk te maken op de rechten van burgers. Daarbij geldt voor beide wetsvoorstellen dat het EVRM van toepassing is op de taakuitvoering door de rechtshandhavingsdiensten en de inlichtingen- en veiligheidsdiensten, inclusief de verwerking van persoonsgegevens. Daardoor geldt voor beide wetsvoorstellen dat iedere inzet van bevoegdheden moet voldoen aan de vereisten die voortvloeien uit het EVRM, zoals de eisen van proportionaliteit (het doel moet opwegen tegen de inbreuk op de privacy en deze inbreuk rechtvaardigen) en subsidiariteit (het lichtste middel waarmee het doel kan worden bereikt moet worden gekozen). De verschillen in de uitwerking van die eisen in de beide wetsvoorstellen houden verband met de verschillende wettelijke taken van de desbetreffende overheidsorganen, de toepasselijkheid van de EU-regels en de verschillen in de wijze waarop deze organen in het staatsbestel zijn ingebed.

De wettelijke taken van de politie en het openbaar ministerie hebben betrekking op respectievelijk de uitvoering van de politietaak en de vervolging van strafbare feiten. Er gelden specifieke wetten voor de bescherming van persoonsgegevens. De Wet politiegegevens bevat regels voor de verwerking van persoonsgegevens door een ambtenaar van politie met het oog op de uitvoering van de politietaak als bedoeld in de artikel 3 en 4, eerste lid, PW 2012. De Wet justitiële en strafvorderlijke gegevens bevat regels voor de verwerking van persoonsgegevens door het openbaar ministerie ten behoeve van een strafzaak. De verwerking van persoonsgegevens met het oog op de opsporing en vervolging van strafbare feiten valt onder de reikwijdte van het verdrag betreffende de Europese Unie. Inmiddels hebben de Raad en het Europees Parlement een richtlijn aangenomen die regels geeft over de verwerking van persoonsgegevens ten behoeve van de strafrechtspleging (richtlijn 680/2016). De

richtlijn geeft aanleiding tot aanpassing van de Wpg en de Wjsg. De regels van de richtlijn zijn afgeleid van die van de verordening gegevensbescherming (verordening 679/2016). De wettelijke taken van de inlichtingen- en veiligheidsdiensten hebben betrekking op de bescherming van de nationale veiligheid (artikelen 8 en 10 Wiv 20xx). De Europese Unie is niet bevoegd op het gebied van de nationale veiligheid (artikel 4, tweede lid, Verdrag betreffende de Europese Unie). In het wetsvoorstel inlichtingen- en veiligheidsdiensten 20xx is een uitputtende regeling opgenomen voor de verwerking van (persoons)gegevens door de diensten, waaronder een specifieke regeling voor de verstrekking van persoonsgegevens en andere gegevens (par. 3.4. Wiv 20xx) en een afzonderlijk hoofdstuk over de kennisneming van door of ten behoeve van de diensten verwerkte gegevens (hoofdstuk 5 Wiv 20xx).

Vanwege het onderscheid in de wettelijke taken zijn de rechtshandhavingsdiensten staatsrechtelijk op een andere wijze ingebed dan de inlichtingen- en veiligheidsdiensten. Dit heeft consequenties voor de controle en het toezicht op de inzet van de bevoegdheden door deze overheidsdiensten. De inzet van de bevoegdheid van het onderzoek in een geautomatiseerd werk door de daartoe aangewezen opsporingsambtenaren vindt plaats onder gezag van de officier van justitie. Naast de hiërarchische controle binnen het openbaar ministerie (College van procureurs-generaal en de Procureur-Generaal bij de Hoge Raad) wordt de rechtmatigheid van de inzet van de bevoegdheid in individuele gevallen getoetst door de rechter (de rechter-commissaris en de zittingsrechter). De Inspectie Veiligheid en Justitie is belast met het toezicht op de uitvoering. De Autoriteit persoonsgegevens houdt toezicht op de naleving van de wettelijke regels over gegevensbescherming door de opsporingsinstanties en het openbaar ministerie. Bij klachten over strafvorderlijk optreden kan de Nationale ombudsman voor aanvullende rechtsbescherming zorgen in gevallen waarin de burger geen toegang heeft tot de rechter of een rechter zich niet heeft uitgelaten over een gedraging die een strafvorderlijk aspect kent (artikelen 9:22 en 9:23 Awb). Ten slotte kan het parlement een rol vervullen.

De inzet van de bevoegdheden van de inlichtingen- en veiligheidsdiensten vindt plaats onder verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, waar het de AIVD betreft, en de Minister van Defensie, ingeval van de MIVD. In het wetsvoorstel Wiv 20xx wordt erin voorzien dat in de gevallen waarbij de Minister toestemming dient te verlenen, voorafgaand aan de daadwerkelijke uitoefening van de desbetreffende bevoegdheid de rechtmatigheid van de verleende toestemming wordt getoetst door een onafhankelijke commissie, de Toetsingscommissie inzet bevoegdheden (TIB). Indien de TIB van oordeel is dat de toestemming niet rechtmatig is verleend, vervalt deze van rechtswege. De afdeling toezicht van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) is belast met het toezicht op de rechtmatige uitvoering van de Wiv 20xx, waaronder de uitoefening van de bevoegdheden door de inlichtingen- en veiligheidsdiensten. De toezichtsrapporten van de CTIVD worden door de verantwoordelijke Minister met diens reactie aan het parlement aangeboden.

De leden van de fractie van het CDA hebben gevraagd hoe de regering de kritiek van de Afdeling advisering van de Raad van State op de proportionaliteit van het voorstel beoordeelt.

De Afdeling advisering van de Raad van State 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 mogelijk-

heden gebruik moet kunnen worden gemaakt. Het voorstel is in zoverre noodzakelijk. De Afdeling advisering 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 EVRM, niet vast. Deze bevoegdheid behoeft naar het oordeel van de Afdeling advisering derhalve differentiatie.

De regering is met de Afdeling advisering van oordeel 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 en opnemen van communicatie of de stelselmatige observatie. Naar aanleiding van het advies van de Afdeling advisering is daarom 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. Beperking van de toepassing tot zeer ernstige misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld, is echter te beperkend. 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 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.

De leden van de fractie van D66 hebben opgemerkt dat het wetsvoorstel een bevoegdheid voor de politie introduceert om binnen te kunnen dringen in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens, opgeslagen in randapparatuur en uitgewisseld met verbonden communicatiekanalen. Met de groei van het internet of things zou dit een groeiende lijst (digitale) apparatuur omvatten. De leden van deze fractie hebben erop gewezen dat zowel de Afdeling advisering als het College bescherming persoonsgegevens serieuze kritiek hebben geuit ten aanzien van de door de regering gegeven motivatie, en gevraagd of de regering een nadere toelichting kan geven op de noodzakelijkheid en proportionaliteit en of zij kan onder-

bouwen waarom een dusdanige verreikende bevoegdheid daadwerkelijk in lijn is met het recht op privacy, zoals beschermd door artikel 8 van het EVRM.

Graag merk ik hierover het volgende op. Er is geen sprake van inzet van de voorgestelde bevoegdheid jegens willekeurige burgers. Het wetsvoorstel koppelt de inzet juist aan een strafrechtelijke relevante verdenking van betrokkenheid van een persoon jegens wie de bevoegdheid kan worden ingezet, bij ernstige strafbare feiten. Het kabinet is zich bewust van de inbreuk op de persoonlijke levenssfeer die de inzet van de voorgestelde bevoegdheid in concrete gevallen met zich mee kan brengen. De inzet van de bevoegdheid vergt daarom maatwerk, toegesneden op een specifieke situatie. Bij het voorstellen van deze nieuwe bevoegdheid wordt uiteraard rekening gehouden met de privacy van burgers. Het recht op privacy is een belangrijk recht, maar het is geen absoluut recht. In bepaalde gevallen is een inbreuk op dat recht gerechtvaardigd, zoals ten behoeve van de opsporing van strafbare feiten. Een goed voorbeeld is het aftappen en opnemen van communicatie. Ingeval van een absoluut recht op privacy zou dat niet mogelijk zijn. In het voorliggende wetsvoorstel worden de waarborgen van de rechtsstaat uiteraard gerespecteerd. Zo moet het gaan om ernstige strafbare feiten. Het inzetten van deze bevoegdheid is verder pas aan de orde als het onderzoeksbelang dit dringend vereist, er geen andere en minder bezwarende mogelijkheden zijn en als de gevolgen van het optreden in verhouding staan tot het doel. Verder is het binnendringen van een geautomatiseerd werk slechts mogelijk met het oog op het verrichten van bepaalde onderzoekshandelingen. Dit betreft deels bestaande bevoegdheden, zoals het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie. Dit betreft deels nieuwe bevoegdheden, zoals het vastleggen van opgeslagen gegevens. Inzet van de bevoegdheid vergt een zorgvuldige afweging door het openbaar ministerie, op het niveau van de officier van justitie en op het niveau van het College van procureurs generaal via een verplichte beoordeling door de Centrale Toetsing Commissie. Daarnaast is voorzien in onafhankelijke rechterlijke toetsing, zowel vooraf door een rechter-commissaris als achteraf door de zittingsrechter, zodat een adequate rechterlijke controle verzekerd is. Ten slotte geldt een verplichting tot notificatie van de betrokkene, is voorzien in toezicht door de Inspectie Veiligheid en Justitie en zal periodiek aan de Kamer worden gerapporteerd over de toepassing van de bevoegdheid. Dit betreft het aantal malen dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid. Voor de noodzaak voor deze bevoegdheden verwijs ik naar de eerdere beantwoording van een vraag van de leden van de fractie van de SP over hoe groot het probleem is dat dit wetsvoorstel moet oplossen. Voor het antwoord op de vraag hoe de inzet van deze bevoegdheid zich verhoudt met het recht op privacy, zoals beschermd door artikel 8 van het EVRM, wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de VVD.

De leden van de fractie van de SP hebben opgemerkt dat het binnendringen van een geautomatiseerd werk altijd tot gevolg heeft dat er meer data worden verzameld dan doelmatig gezien nodig is en dat hierdoor ook de privacy van onschuldige burgers wordt bedreigd omdat via het netwerk ook deze in de gaten gehouden kunnen worden. Onder verwijzing naar artikel 3 van de Wet politiegegevens en artikel 8 van het EVRM hebben deze leden gevraagd om een reactie hierop.

Het binnendringen van een geautomatiseerd werk heeft niet altijd tot gevolg dat er meer data worden verzameld dan doelmatig gezien nodig is; de toepassing van de bevoegdheden wordt immers beheerst door de beginselen van proportionaliteit en subsidiariteit. Daarnaast zullen er geen onschuldige burgers via het netwerk in de gaten worden gehouden. De term «in de gaten houden» suggereert een structureel gerichte inzet. Dat is bij onschuldige burgers niet het geval, al kan de verzameling van hun gegevens wel het gevolg zijn van de inzet. De regels rond de inzet van de bevoegdheid zijn er echter juist steeds op gericht om zoveel mogelijk te voorkomen dat gegevens worden verzameld die niet nodig zijn voor het opsporingsonderzoek. Daartoe moet de officier van justitie in het bevel het onderdeel van het geautomatiseerde werk vermelden waartegen het bevel is gericht en ook de functionaliteit die daarbij worden ingezet. Niettemin zal het in de uitvoeringspraktijk onvermijdelijk zijn dat gegevens worden verzameld van personen die zelf niet bij criminaliteit zijn betrokken. Dat is bij de inzet van traditionele opsporingsmiddelen, als de telefoon- en de IP-tap, niet anders. Bij het aftappen en opnemen van communicatie komen de uitlatingen van gespreksdeelnemers ter kennis van de opsporing en bij de IP-tap betreft dit alle dataverkeer dat van en naar een huisadres of IP-adres gaat, ook het dataverkeer van huisgenoten die de desbetreffende aansluiting gebruiken.

Op grond van de jurisprudentie van het EHRM inzake artikel 8 van het EVRM gelden strenge eisen voor het heimelijk onderscheppen van communicatie van burgers. Voor de vraag of het wetsvoorstel voldoet aan de eisen die daaraan op grond van het EVRM moeten worden gesteld, wordt verwezen naar de eerdere beantwoording in deze paragraaf van een soortgelijke vraag van de leden van de fractie van de VVD.

De leden van de fractie van GroenLinks hebben gevraagd of de regering meent dat het voorgestelde doel, bestrijding van cybercriminaliteit, de voorgestelde middelen heiligt, namelijk de daarmee gepaard gaande inbreuk op individuele grondrechten.

Het wetsvoorstel maakt door de strikte voorwaarden en de diverse waarborgen de inbreuk op de persoonlijk levenssfeer zo klein mogelijk. Zoals hiervoor reeds aan de orde is gekomen, is de regering van oordeel dat de ontwikkeling van computercriminaliteit een ernstige bedreiging vormt van de veiligheid van de Nederlandse samenleving ten aanzien waarvan de opsporingsdiensten nu niet over een gepast antwoord beschikken. Het internet wordt een vrijplaats voor allerlei vormen van ernstige criminaliteit waartegen burgers en bedrijven zich onvoldoende kunnen verweren. Politie en justitie worden ernstig gehinderd in de mogelijkheden om hiertegen op te treden omdat er geen bevoegdheid is om op afstand heimelijk een geautomatiseerd werk binnen te dringen om een einde te maken aan het strafbaar handelen, door gegevens ontoegankelijk te maken, of de daders op te sporen door bewijsmateriaal te verzamelen. Het is vrijwel overbodig te vermelden dat de persoonlijke levenssfeer van de slachtoffers hierbij in het geding is. Het recht op bescherming van de persoonlijke levenssfeer beoogt burgers te vrijwaren tegen ongeoorloofde inmenging van de overheid in hun persoonlijke levenssfeer. Het recht op privacy is echter geen absoluut recht, dit recht dient te worden afgewogen tegen andere zwaarwegende maatschappelijke belangen, zoals het belang van de opsporing en vervolging van ernstige strafbare feiten. Deze balans komt ook tot uitdrukking in de tekst van artikel 8 EVRM. Te dien aanzien kan een vergelijking worden gemaakt met het huisrecht, dat bescherming geniet op grond van artikel 12 van de Grondwet en artikel 8 EVRM. Het huisrecht is echter evenmin een absoluut recht, onder bepaalde omstandigheden en onder bepaalde voorwaarden kan inbreuk worden gemaakt op dit recht. De regering is van

oordeel dat met het wetsvoorstel een evenwichtige balans is gevonden tussen de betrokken belangen. Voor de ontwikkeling van de wettelijke voorwaarden is nauw aangesloten bij de criteria voor de toepassing van andere ingrijpende bevoegdheden, zoals de doorzoeking van een woning of de toepassing van bijzondere opsporingsbevoegdheden. Deze waarborgen hebben betrekking op de aard van de strafbare feiten, waarvoor de voorgestelde bevoegdheid kan worden ingezet, de ernst van de verdenking, de mogelijkheid van de inzet van alternatieve bevoegdheden. Hierbij is het vereiste van voorafgaande rechterlijke goedkeuring essentieel.

De voorwaarden die gelden voor de inzet van de voorgestelde bevoegdheid komen overeen met de voorwaarden die gelden voor de inzet van bestaande opsporingsbevoegdheden met een vergelijkbaar indringend karakter. Van een ingrijpende wijziging van de positie van de verdachte is derhalve geen sprake. De inzet van de bevoegdheid tot het onderzoek in een geautomatiseerd werk is mogelijk als er sprake is van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Dit vereiste geldt ook voor de inzet van andere bijzondere opsporingsbevoegdheden met een heimelijk karakter, zoals de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s, en 126zf) of het vorderen van bijzondere persoonsgegevens, bijvoorbeeld gegevens over iemands godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv). Wanneer het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens geldt overigens voor het verrichten van die onderzoekshandelingen een zwaarder verdenkingscriterium. In dat geval is de verdenking van een misdrijf vereist waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

De leden van de fractie van GroenLinks hebben gevraagd waar precies het hiaat zit in de bestaande wettelijke bevoegdheden op dit terrein. De leden van deze fractie hebben tevens gevraagd welke andere mogelijkheden er exact zijn onderzocht en of de regering kan uitleggen waarom deze volgens haar niet voldoen.

De bestaande opsporingsbevoegdheden schieten in toenemende mate tekort om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit en het vergaren van elektronisch bewijs tegemoet te komen. Ontwikkelingen als de versleuteling van elektronische gegevens, het gebruik van draadloze netwerken en cloudcomputingdiensten dragen hier in belangrijke mate aan bij. Daarnaast kan de voorgestelde bevoegdheid in bepaalde gevallen worden ingezet om de inbreuk op de persoonlijke levenssfeer in het kader van de opsporing zo beperkt mogelijk te houden. De bestaande opsporingsbevoegdheden zijn gebaseerd op het uitgangspunt dat de gegevens die voor de opsporing van belang zijn, zich op een bepaalde gegevensdrager op een bepaalde locatie bevinden. Alsdan kunnen de bestaande bevoegdheden worden ingezet, zoals de doorzoeking van een besloten plaats ter vastlegging van gegevens (art. 125i Sv) of de vordering aan degene die toegang heeft tot bepaalde opgeslagen of vastgelegde gegevens tot verstrekking van die gegevens (art. 126nd/ud Sv). Dit spoort echter niet meer met de werkelijkheid in gevallen waarin smartphones en laptops worden gebruikt of de gegevens zich in de cloud bevinden. Het gebruik van andere, nu al bestaande bevoegdheden, biedt geen soelaas in de zich steeds vaker manifesterende situaties waarin het niet mogelijk is een

IP-adres te herleiden tot een specifieke internet dienstverlener, een concreet persoon of een concrete locatie. In die gevallen kunnen de verschillende vorderingen ten aanzien van internet service providers niet worden ingezet omdat niet bekend is aan wie de vordering moet worden verstuurd. Als de locatie van het betreffende geautomatiseerde werk of van de gegevens niet bekend is dan kan evenmin een doorzoeking ter vastlegging van gegevens (artikel 125i Sv) worden uitgevoerd. Ditzelfde geldt voor de andere bevoegdheden tot inbeslagneming van een geautomatiseerd werk of een gegevensdrager (artikelen. 95, eerste lid, 95, eerste lid, 96c, eerste lid, 97 eerste lid, 98, eerste lid, en 99, eerste lid, Sv). Maar ook als de locatie wel bekend is kan de versleuteling van de gegevens de opsporing voor grote problemen plaatsen, aangezien sommige vormen van versleuteling vrijwel niet te kraken zijn. Belangrijk bezwaar van deze bevoegdheden is voorts dat de verdachte doorgaans op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Dat is doorgaans niet bevorderlijk voor het verdere verloop van het opsporingsonderzoek, omdat de verdachte alle bewijsmateriaal onmiddellijk zal vernietigen. Het is bijvoorbeeld voorgekomen dat een verdachte van het bezit van kinderpornografie tijdens zijn arrestatie kans zag met zijn voet een schakelaar te bereiken waarmee de stroom van de computer werd afgesloten en de bestanden direct werden gewist. Daardoor ging het bewijsmateriaal verloren. Overigens brengt de inzet van deze bestaande bevoegdheden met zich mee dat politie en justitie kunnen beschikken over alle gegevens die op het geautomatiseerde werk of de gegevensdrager zijn opgeslagen. De wetgever heeft destijds aangegeven dat dit veelal als disproportioneel moet worden aangemerkt in de gevallen waarin een voorwerp in beslag wordt genomen uitsluitend om bepaalde gegevens vast te leggen (Kamerstukken II, 1998/99, 26 671, nr. 3, blz. 19).

Onderzocht is of andere bevoegdheden uitkomst kunnen bieden. Dat lijkt op het eerste gezicht soms het geval, maar bij nadere beschouwing zijn daarbij dikwijls andere zwaarwegende belangen aan de orde. Zo biedt de bevoegdheid tot het opnemen van vertrouwelijke communicatie (artikelen 126l, 126s en 126zf Sv) de mogelijkheid om door middel van een technisch hulpmiddel, zoals een «bug» (een kleine microfoon die opgenomen signalen draadloos verzendt) of een richtmicrofoon, heimelijk vertrouwelijke communicatie op te nemen. Ter uitvoering van de bevoegdheid kan een besloten plaats of een woning worden betreden, zodat het technische hulpmiddel kan worden geplaatst. Deze bevoegdheid biedt echter geen soelaas als de gegevens zijn versleuteld of als de gegevens in de cloud zijn opgeslagen. Verder vormt de noodzaak van fysieke toegang tot de plaats waar het geautomatiseerde werk zich bevindt een grote belemmering voor de opsporing zowel in de gevallen waarin de locatie van het geautomatiseerde werk niet bekend is (terwijl de technische ontwikkelingen het op afstand plaatsen van een «bug» wel mogelijk maken) als in gevallen waarin die locatie wel bekend is, maar de kans bestaat op ontdekking of op onvoorziene omstandigheden ter plaatse. Andere opsporingsbevoegdheden zoals de observatie (artikelen 126g, 126o en 126zd, eerste lid, onderdeel a Sv), het stelselmatig inwinnen van informatie (artikelen 126j, 126qa en 126zd, eerste lid, onderdeel c Sv) of de inkijkoperatie (artikelen 126k, 126r en 126zd, eerste lid, onderdeel d Sv) bieden geen uitzicht op toegang tot gegevens die langs elektronische weg worden verwerkt en bieden dan ook weinig kans op kennisneming van de inhoud van de gegevens die door de verdachte zijn ontvangen of verzonden, of van de communicatie waarbij hij is betrokken.

De leden van de fractie van GroenLinks hebben erop gewezen dat de Afdeling advisering van de Raad van State heeft geoordeeld dat de proportionaliteit van het heimelijk binnendringen in een geautomatiseerd werk onbewezen is gebleven en dat ook andere organisaties stevige

kritiek hebben geuit op het wetsvoorstel. De leden van deze fractie hebben opgemerkt dat het College bescherming persoonsgegevens heeft geadviseerd om het wetsvoorstel niet op deze wijze in te dienen omdat het wetsvoorstel een grondwettelijke toetsing niet zou doorstaan. Zij hebben gevraagd wat de verwachting van de regering is ten aanzien van een dergelijke grondwettelijke toetsing van het wetsvoorstel.

Eerder in deze paragraaf is, naar aanleiding van een vraag van de leden van de fractie van de VVD, reeds ingegaan op de vraag in hoeverre het wetsvoorstel voldoet aan de vereisten die voortvloeien uit het EVRM, in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer. Anders dan het College bescherming persoonsgegevens (thans de Autoriteit persoonsgegevens) ziet de regering geen reden waarom de voorgestelde regeling niet zou voldoen aan de vereisten op het gebied van de bescherming van de persoonlijke levenssfeer, zoals die voortvloeien uit artikel 8 EVRM. Zoals hiervoor aangegeven heeft het advies van de Afdeling advisering van de Raad van State aanleiding gegeven tot aanpassing van het wetsvoorstel.

De leden van de fractie van GroenLinks hebben erop gewezen dat ook de Nederlandse burgerrechtenorganisatie Bits of Freedom het wetsvoorstel te ruim vindt in zijn bevoegdheden. Onder verwijzing naar het voorbeeld van de pacemaker hebben de leden van deze fractie gevraagd waarom, naast de bestaande mogelijkheden en naast de mogelijkheden in de wetten computercriminaliteit I en computercriminaliteit II, nu nog extra bevoegdheden nodig zijn.

Graag benadruk ik nogmaals dat er strikte regels gelden voor de inzet van de bevoegdheid, waaronder het vereiste van een misdrijf waarvoor voorlopige hechtenis is toegelaten. Verder geldt het vereiste van een voorafgaande rechterlijke toetsing. De omschrijving van het begrip geautomatiseerd werk is identiek aan die van het Verdrag van de Raad van Europa (artikel 1: «»computer system»» means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;»). De definitie van de EU is overigens nog iets ruimer, omdat daarin ook computergegevens zijn betrokken. Het is inherent aan de gehanteerde definitie van geautomatiseerd werk dat de ontwikkeling van apparatuur en systemen die aan die definitie voldoen daarmee ook onder de reikwijdte van de bevoegdheid komen te vallen. De ontwikkeling van het internet of things (waarbij «slimme apparaten» als koelkasten, navigatiesystemen en thermostaten via het internet worden aangestuurd) kan meebrengen dat die apparaten via het internet kunnen worden binnengedrongen.

Het bij voorbaat uitsluiten van bepaalde geautomatiseerde werken belemmert de opsporing en biedt criminelen meer mogelijkheden de opsporing te ontlopen door juist dergelijke systemen te misbruiken voor het plegen van strafbare feiten. Dat is niet in het belang van de veiligheid van dergelijke systemen. Bovendien staat de techniek niet stil en kent de creativiteit van de misdaad helaas weinig grenzen. De aard van het geautomatiseerde werk zal reden kunnen zijn voor grote terughoudendheid bij de inzet, of bepalend zijn voor het besluit tot de inzet of juist het afzien daarvan. Uiteraard wordt, indien mogelijk, gekozen voor de inzet van minder vergaande bevoegdheden, zoals een vordering van gegevens aan de beheerder van het desbetreffende systeem. De eisen die aan de uitoefening van de bevoegdheid worden gesteld, gecombineerd met het uitgebreide toezicht door zowel de rechter als de Inspectie Veiligheid en Justitie, brengt naar mijn oordeel mee dat er is voorzien in adequate waarborgen tegen oneigenlijk gebruik van de bevoegdheid. Hoewel een pacemaker in beginsel onder de definitie van geautomati-

seerd werk valt, zullen hierin naar verwachting geen gegevens te vinden zijn die bijdragen aan de opsporing van ernstige vormen van computercriminaliteit of andere ernstige strafbare feiten. In de praktijk is het tevens moeilijk denkbaar dat er zich een zo zwaarwegend belang voordoet dat het binnentreden van een pacemaker proportioneel zou worden geacht.

De leden van de fractie van GroenLinks hebben gevraagd wat precies de reikwijdte is van deze wet, en of in het wetsvoorstel rekening wordt gehouden met eerdere uitspraken van het Hof van Justitie van de Europese Unie, dat de afgelopen jaren meermalen kritiek op wetten had die de privacy van burgers te veel zouden schenden.

Wat betreft de reikwijdte van de voorgestelde bevoegdheid is nauw aangesloten bij het wettelijke systeem voor de toepassing van andere bijzondere opsporingsbevoegdheden. De voorgestelde bevoegdheid kan worden toegepast ingeval van (1) verdenking van een ernstig strafbaar feit waarvoor voorlopige hechtenis kan worden toegepast, (2) het vermoeden dat in georganiseerd verband ernstige strafbare feiten worden beraamd of gepleegd die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, of (3) aanwijzingen van een terroristisch misdrijf. Dit betreft de bestaande criteria voor de toepassing van bijzondere opsporingsbevoegdheden. Daarbij geldt een drempel voor wat betreft de ernst van de strafbare feiten, te weten een misdrijf waarvoor voorlopige hechtenis kan worden toegepast. Verder geldt het vereiste van voorafgaande rechterlijke toestemming.

In antwoord op de vraag over de uitspraken van het Hof van Justitie van de Europese Unie merkt de regering op ervan overtuigd te zijn dat het wetsvoorstel voldoet aan de eisen die daaraan op grond van het Handvest van de grondrechten van de Europese Unie moeten worden gesteld. Voor de toelichting op dit oordeel wordt verwezen naar de eerdere beantwoording in deze paragraaf van een soortgelijke vraag van de leden van de fractie van de VVD.

4. Samenloop bevoegdheden AIVD en MIVD

De leden van de fractie van D66 hebben opgemerkt dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. De leden van deze fractie hebben gevraagd waarom de regering deze bevoegdheid ook wil uitbreiden naar de politie, als de AIVD en MIVD deze bevoegdheid reeds hebben. De leden van deze fractie hebben tevens gevraagd of de regering kan aangeven of dit de afbakening van taken van deze instanties niet juist versnippert en onduidelijker maakt.

De bestrijding van terrorisme is niet alleen relevant in de context van de bescherming van de nationale veiligheid maar eveneens in die van de criminaliteitsbestrijding. Met de Wet terroristische misdrijven van 24 juni 2004 (Stb. 2004, 290) is het materiële strafrecht aangescherpt zodat dit beter is toegesneden op terrorisme en het rekruteren voor de jihad. Daartoe zijn een aantal gedragingen, bij aanwezigheid van het zogenaamde «terroristisch oogmerk», als terroristisch misdrijf strafbaar gesteld. Tevens is de deelneming aan en het leiden van een organisatie die tot oogmerk heeft het plegen van terroristische misdrijven strafbaar gesteld met minimaal acht respectievelijk vijftien jaar gevangenisstraf. Een belangrijke functie van het strafrecht bij terroristische misdrijven ligt in het voorkomen van terroristische aanslagen. Met de wet tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en

vervolging van terroristische misdrijven van 20 november 2006 (Stb. 2006, 580) zijn de toepassingsmogelijkheden van bijzondere opsporingsbevoegdheden verruimd ten behoeve van een adequate bestrijding van terroristische misdrijven. In geval van aanwijzingen van een terroristisch misdrijf kunnen bijzondere opsporingsbevoegdheden, zoals de stelselmatige observatie, de pseudokoop en -dienstverlening, de infiltratie en het aftappen en opnemen van communicatie, worden toegepast. Bij «aanwijzingen» van terroristische misdrijven kan het openbaar ministerie al in een vroeg stadium strafrechtelijk ingrijpen. Vanwege de ernst van terroristische misdrijven en hun mogelijke impact op het maatschappelijk leven en de veiligheid van burgers, het hiermee samenhangende zwaarwegende publieke belang om aanslagen te voorkomen en het tekortschieten van de bestaande opsporingsbevoegdheden bij het gebruik van de moderne informatie- en communicatietechnologie (zoals het gebruik van encryptie bij de communicatie met anderen en de opslag van gegevens in de cloud) ligt het voor de hand dat de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk ook kan worden toegepast ingeval van aanwijzingen van dergelijke misdrijven.

Versnippering in de afbakening van taken van deze instanties vanwege de uitbreiding van deze bevoegdheid naar de politie, zoals gesteld door de leden van de fractie van D66, is niet aan de orde. Het voorkómen van terroristische aanslagen betreft niet een taak die exclusief is toebedeeld aan een bepaalde overheidsorganisatie. Waar de AIVD zich in het kader van de nationale veiligheid – onder meer door het permanent verkennen van tendensen binnen de samenleving – richt op het tijdig onderkennen en zo mogelijk voorkomen van (de realisatie van) terroristische dreigingen, ligt bij de politie en het openbaar ministerie de nadruk op het opsporen en vervolgen van terroristische misdrijven. Dikwijls zal het dan gaan om opsporingsonderzoek naar het voorbereidende stadium van terroristische misdrijven, mede gericht derhalve op het daadwerkelijk voorkomen van terroristische aanslagen, naast – waar mogelijk – het komen tot vervolging. Het voorliggende wetsvoorstel voorziet uitsluitend in aanpassing van de bevoegdheden zodat de bestaande taak beter kan worden uitgevoerd. Voor zover in de praktijk kans zou bestaan op overlap wordt op grond van de Wiv 2002 voorzien in procedures ten behoeve van de afstemming tussen de bescherming van de nationale veiligheid enerzijds en de opsporing van strafbare feiten anderzijds. Als bij de verwerking van gegevens door of ten behoeve van een dienst blijkt van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten, dan kan hiervan mededeling worden gedaan aan de landelijk officier van justitie die is belast met de bestrijding van terroristische misdrijven (artikel 38, eerste lid, Wiv 2002). Andersom zijn de leden van het openbaar ministerie gehouden, door tussenkomst van het College van procureurs-generaal, aan een dienst mededeling te doen van de te hunner kennis gekomen gegevens die zij voor die dienst van belang achten (artikel 61, eerste lid, Wiv 2002). Hierdoor is een goede afstemming tussen de betrokken organen bij de voorkoming en bestrijding van terrorisme verzekerd.

De leden van de fractie van de SP hebben gevraagd waarom de regering met dit wetsvoorstel de bevoegdheid om terroristische aanslagen te voorkomen wil uitbreiden naar de politie, en of het juist is dat de inlichtingendiensten dit tot taak hebben.

Met dit wetsvoorstel wordt geenszins beoogd het werkterrein van politie en justitie uit te breiden. Zoals reeds aangegeven gaat het bij terrorisme om het plegen van de meest ernstige vormen van strafbare feiten. Met behulp van het strafrecht moet daartegen krachtig worden opgetreden en daarmee is gegeven dat ook politie en justitie een belangrijke taak op het

terrein van terrorismebestrijding hebben. Dit wetsvoorstel voorziet overigens wel in een uitbreiding van de strafvorderlijke bevoegdheden voor de bestrijding van terrorisme. Voor de redenen die daaraan ten grondslag liggen kan worden verwezen naar mijn eerdere antwoord op een soortgelijke vraag van de leden van de fractie van D66.

De leden van de fractie van de ChristenUnie hebben opgemerkt dat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk op dit moment al kan worden toegepast door de AIVD en MIVD, en hebben gevraagd naar de noodzaak van de nieuwe voorgestelde bevoegdheid en de ratio achter de geringe clausulering voor het gebruik daarvan door de opsporingsdiensten.

Voor de noodzaak van de voorgestelde bevoegdheid verwijs ik graag naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66. De mening dat de bevoegdheid gering is geclausuleerd wordt dezerzijds niet onderschreven; de bevoegdheid is juist voorzien van strikte waarborgen en garanties, zowel bij de voorbereiding, de uitvoering als de verantwoording daarvan. Voor een nadere toelichting op de strikte clausering verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van D66.

De leden van de fractie van de ChristenUnie hebben gevraagd of er andere terreinen zijn dan de opsporing van terroristische misdrijven en kinderpornografie waar de opsporingsdiensten onvoldoende resultaat boeken als gevolg van het ontbreken van de voorgestelde hackbevoegdheden. De leden van deze fractie hebben tevens gevraagd om een nadere cijfermatige onderbouwing van de noodzaak om deze bevoegdheid zo ruim uit te breiden.

De technologische ontwikkelingen gaan zo snel dat bij vele vormen van criminaliteit gebruik wordt gemaakt van het internet of digitale middelen. De bevoegdheid is dan ook zeer belangrijk voor het kunnen blijven bestrijden van computercriminaliteit, waarvan de omvang groeit en de bestrijding steeds gecompliceerder wordt. In deze vorm van criminaliteit komen de encryptieproblemen, afschermingsproblemen alsmede het internationale karakter van de pleegplaatsen en aanwezigheid van bewijsmateriaal in alle indringendheid naar voren, zoals door vele cybersecurity specialisten wordt onderschreven. Voorts is de bevoegdheid van belang voor de bestrijding van de gevestigde georganiseerde criminaliteit. Zoals uit recente onderzoeken is gebleken, is de invoering van het gebruik van encryptietechnieken en andere afschermingmethodieken, waarbij het niet meer goed mogelijk is voor de politie om de inhoud van de communicatie te onderscheppen, gemeengoed geworden. Organisaties worden gefaciliteerd in het zo anoniem mogelijk communiceren, bijvoorbeeld met het oog op het plegen van moorden, drugstransporten, wapenhandel en ondermijnende criminaliteit, zoals witwassen, fraude en corruptie. In dergelijke zaken is het van groot belang om de anonimiseringstechnieken en versleutelingtechnieken te doorbreken. Er zijn geen cijfers te geven over in hoeveel zaken het wel of niet nodig is geweest om deze bevoegdheid te kunnen inzetten. Er wordt niet per zaak geregistreerd welke niet-bestaande bevoegdheden tot een meer effectieve opsporing hadden kunnen leiden.

De leden van de fractie van de ChristenUnie zouden graag inzicht krijgen in hoe vaak de veiligheidsdiensten op dit moment gebruikmaken van de bevoegdheden tot het heimelijk binnendringen van een geautomatiseerd werk en hoe zich dit verhoudt tot het gebruik van dit instrument in de omliggende landen. De leden van deze fractie hebben tevens gevraagd

hoe vaak gebruik wordt gemaakt van de bemachtigde gegevens van de veiligheidsdiensten in een strafproces.

Informatie over de mate waarin specifieke bijzondere bevoegdheden worden ingezet geeft inzicht in de werkwijze van de diensten. Dergelijke informatie is staatsgeheim, en kan derhalve uitsluitend vertrouwelijk via de daartoe geëigende kanalen aan de Tweede Kamer, in casu de CIVD, worden verstrekt. Als bij de verwerking van gegevens door of ten behoeve van een dienst blijkt van gegevens die tevens van belang kunnen zijn voor de opsporing of vervolging van strafbare feiten, kan daarvan mededeling worden gedaan aan de Landelijk officier van justitie die is belast met de bestrijding van terroristische misdrijven. De procedure is vastgelegd in artikel 38 Wiv 2002. Het is niet bekend hoe vaak gebruik wordt gemaakt van de gegevens van de veiligheidsdiensten in een strafproces

5. Kwetsbaarheden

De leden van de fractie van het CDA hebben erop gewezen dat in de Tweede Kamer uitgebreid debat is gevoerd over de in dit wetsvoorstel verleende bevoegdheid aan het openbaar ministerie om uitstel te verlenen aan het melden van onbekende kwetsbaarheden aan de producent als de opsporing er zwaarwegend belang bij heeft om deze melding nog uit te stellen. In het wetsvoorstel wordt geen termijn aan het – in beginsel ongeoorloofde – uitstel tot melding van een kwetsbaarheid gesteld. In het debat wordt gewag gemaakt van een termijn van vier weken, maar die termijn kan door de rechter-commissaris steeds weer met vier weken worden verlengd. Het lijkt de leden van deze fractie verstandig om de maximale termijn alsnog in de wet te noemen zodat de onbekende kwetsbaarheid kan worden gerepareerd en zij hebben gevraagd of de regering hier nader op in kan gaan.

Als de politie of het openbaar ministerie kennis verwerft van onbekende kwetsbaarheden in hard- of software waarmee heimelijk en op afstand een geautomatiseerd werk kan worden binnengedrongen, dan worden deze in beginsel gemeld aan de fabrikant van de desbetreffende hard- of software. In uitzonderlijke gevallen kunnen er redenen zijn die het melden tijdelijk in de weg staan. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. Het wetsvoorstel voorziet in de mogelijkheid voor de officier van justitie om, op grond van een zwaarwegend opsporingsbelang, te bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk als bedoeld in de artikelen 126nba, 126uba en 126zpa Sv, wordt uitgesteld (artikel 126ffa Sv). Voor het afzien van het melden van een onbekende kwetsbaarheid is machtiging van de rechter-commissaris vereist. Deze machtiging is tijdelijk. De periode van geldigheid van de machtiging is wettelijk niet nader ingekaderd; het wordt aan de interactie tussen officier van justitie en rechter-commissaris gelaten om te komen tot nadere inkadering van de periode van geldigheid van het uitstel. Het ligt echter in de rede om voor de periode van uitstel van de melding aan te sluiten bij de periode van geldigheid van de machtiging voor het onderzoek in het geautomatiseerde werk, waarbij het voornemen bestaat gebruik te maken van de betreffende kwetsbaarheid. De bevoegdheid tot het onderzoek in een geautomatiseerd werk is gekoppeld aan een periode van vier weken, daarna kan het bevel telkens met een periode van vier weken worden verlengd. Dit is vastgelegd in het voorgestelde artikelen 126nba, derde lid, respectievelijk 126uba/zpa, derde lid, Sv. Het ligt in de rede dat de rechter-commissaris bij de beoordeling van een eventueel verzoek tot verlenging van het bevel tot het onderzoek in een geautomati-

seerd werk tevens het bevel tot uitstel van de melding van de kwetsbaarheid toetst.

Een verlenging van de machtiging kan zich bijvoorbeeld voordoen als de melding zou resulteren in het tenietdoen van het heimelijke karakter van het opsporingsonderzoek. Ook kan de onbekende kwetsbaarheid een systeem of computerprogramma betreffen dat door criminelen is vervaardigd en/of vrijwel alleen voor criminele doeleinden wordt gebruikt. Het melden van een onbekende kwetsbaarheid in dergelijke gevallen zou het effect hebben criminaliteit te faciliteren. In dergelijke gevallen kan langduriger uitstel van de melding aan de fabrikant aan de orde zijn. Het uitstel wordt dan periodiek door de rechter-commissaris getoetst. Het uitstellen van het delen van informatie over aangetroffen onbekende kwetsbaarheden in wijdverbreide en regulier gebruikte hard- of software ligt uiteraard niet in de rede.

De leden van de fractie van D66 hebben opgemerkt dat de politie gebruik zal maken van niet bekende kwetsbaarheden om in te breken in geautomatiseerde apparatuur. Hiermee houdt de politie naar het oordeel van de leden van deze fractie het bestaan van dergelijke kwetsbaarheden in stand, waarmee het internet en digitale apparaten onveiliger worden in plaats van veiliger. Deze leden hebben gevraagd waarom de regering niet investeert in het veiliger maken van de digitale wereld in plaats van het financieren en gebruik van niet bekende kwetsbaarheden.

De regering investeert aanzienlijk in het veiliger maken van de digitale wereld. De regering heeft het wetsvoorstel Gegevensverwerking en meldplicht cyber security (Kamerstukken 34 388) aan uw Kamer gezonden. Dit voorstel bevat een meldplicht voor inbreuken op de veiligheid of een verlies van integriteit van elektronische informatiesystemen bij vitale sectoren. Ook wordt informatie en handelingsperspectief geboden aan eindgebruikers via veiliginternetten.nl en de jaarlijkse campagne Alert Online. In aanvulling hierop wordt gestimuleerd om te investeren in het veiliger maken van apparaten en een goede cyber hygiëne. De overheid stimuleert bovendien het verminderen van kwetsbaarheden met het beleid voor «responsible disclosure». Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het Nationaal Cyber Security Centrum van het Ministerie van Veiligheid en Justitie (NCSC) in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. De politie zal overigens geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot binnendringen in geautomatiseerd werk.

De Nederlandse regering werkt aan een open, vrij en veilig internet. Effectieve handhaving van de rechtsstaat in cyberspace is hiervoor een voorwaarde. Dit wetsvoorstel ziet op het versterken van de opsporing van criminaliteit op internet, zodat kwaadwillenden die het digitale domein misbruiken effectief kunnen worden aangepakt. De overheid investeert bovendien ook op diverse andere manieren in het veiliger maken van het internet en stimuleert dit ook actief. Bij het binnendringen in een geautomatiseerd werk met het oog op het uitvoeren van onderzoekshandelingen zal gebruik worden gemaakt van zowel bekende als onbekende kwetsbaarheden. Er zijn veel bruikbare bekende kwetsbaarheden. Anders dan de vragenstellers veronderstellen zullen niet uitsluitend onbekende kwetsbaarheden worden gebruikt, bekende kwetsbaarheden kunnen naar verwachting in veel gevallen bruikbaar zijn.

De leden van de fractie van de SP hebben geconstateerd dat de hacksoftware door externe partijen ontwikkeld zal worden en dat de politie zonder gedegen kennis eigenlijk niet weet wat zij inkoopt, en

gevraagd hoe de regering voorkomt dat de politie schadelijke software inkoopt die weliswaar doet wat het zegt maar tevens informatie over de politie aan derden verschaft.

In het ter uitvoering van het wetsvoorstel opgestelde Besluit onderzoek in een geautomatiseerd werk, waarover uw Kamer bij brief van 10 mei 2017 (Kamerstukken II 2016/17, 34 372, nr. 26) is geïnformeerd, worden verschillende keuringseisen gesteld aan de inrichting en werking van een technisch hulpmiddel dat wordt gebruikt voor het detecteren, registeren en transporteren van gegevens. Eén van de eisen is dat een technisch hulpmiddel beveiligd is tegen wijziging van de werking ervan en tegen wijziging en kennisneming van geregistreerde gegevens door onbevoegden. Ook moet een technisch hulpmiddel in staat zijn om geregistreerde gegevens op zodanige wijze te transporteren dat de gegevens automatisch op een technische infrastructuur binnen de politieorganisatie worden vastgelegd. Met deze eisen wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik en worden de betrouwbaarheid en de integriteit van de vastgelegde gegevens verzekerd. Als bij het onderzoek in een geautomatiseerd werk gebruik wordt gemaakt van een goedgekeurd technisch hulpmiddel, mag er vanuit worden gegaan dat aan de wettelijke eisen is voldaan.

Gedurende de uitvoering van een bevel van de officier van justitie worden doorlopend en automatisch gegevens vastgelegd over de met een technisch hulpmiddel verrichte onderzoekshandelingen en het functioneren van de technische infrastructuur waarop de met een technisch hulpmiddel geregistreerde gegevens worden vastgelegd. Dit wordt ook wel «logging» genoemd. Op deze wijze kan zowel tijdens het verrichten van onderzoekshandelingen als achteraf intern toezicht plaatsvinden binnen de politieorganisatie op de uitvoering van het bevel van de officier van justitie.

Daarnaast houdt de Inspectie Veiligheid en Justitie toezicht op het functioneren van het wettelijke systeem omtrent de binnendring- en onderzoeksbevoegdheid. Dit toezicht heeft onder meer betrekking op aspecten als de inzet van een technisch hulpmiddel, de vastlegging van de met een technisch hulpmiddel geregistreerde gegevens op een technische infrastructuur, de beveiliging van de gegevens en de «logging» over de uitvoering van een bevel.

Bij de leden van de fractie van de SP leeft een grote zorg over het gebruikmaken van de zogenaamde Zero Day-zwaktes. Zij hebben gevraagd hoe de regering erover oordeelt dat dit in de Verenigde Staten heeft geleid tot het seponeren van een zaak van kindermisbruik.

Hierboven, bij de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66 en de SP, is reeds ingegaan op het gebruik van onbekende kwetsbaarheden, door sommigen zero day kwetsbaarheden genoemd. In aanvulling hierop wijs ik er op dat het wetsvoorstel naar aanleiding van het amendement Recourt/Tellegen (Kamerstukken II 2016/17, 30 372, nr. 14) een verplichting introduceert om onbekende kwetsbaarheden die de politie bekend zijn geworden bij het toepassen van de bevoegdheid van 126nba Sv te melden. Slechts in uitzonderlijke situaties kan, uitsluitend bij een zwaarwegend opsporingsbelang en na accordering van het centraal aanspreekpunt bij het Landelijk Parket, worden besloten om de rechter-commissaris toestemming te vragen om de melding uit te stellen. Overigens is de kans klein dat politie en justitie een onbekende kwetsbaarheid ontdekken die niet eerder reeds is ontdekt en besproken. Vanwege de hiervoor genoemde verplichting die volgt uit

het amendement Recourt/Tellegen speelt het al dan niet melden reeds een rol voordat een zaak naar de rechter gaat. De melding van de kwetsbaarheid wordt onafhankelijk getoetst.

De leden van de fractie van de SP hebben gevraagd of het denkbaar is dat de politie een zaak van kindermisbruik (of andere ernstige misdrijven) moet laten varen vanwege het feit dat zij de Zero Day niet wil openbaren. De leden van deze fractie hebben tevens gevraagd hoe de regering oordeelt over de morele kant van de zaak.

Op dit moment ziet de regering geen realistische scenario's waarbij het openbaar ministerie moet besluiten om de vervolging te staken of niet door te zetten vanwege dit dilemma. Dit wordt niet voorzien omdat er rond de inzet van de middelen en de onbekende kwetsbaarheden vele waarborgen worden ingevoerd en vanwege de verplichting die voortvloeit uit het eerdergenoemde amendement Recourt/Tellegen. Mochten er zwaarwegende redenen zijn tot uitstel van de melding, dan worden die onafhankelijk getoetst.

De leden van de fractie van de SP hebben opgemerkt dat de politie op de hoogte is van een zwakte waar vele criminelen gebruik van zullen maken en hebben gevraagd of het niet de taak van de politie is om mensen te beschermen tegen criminaliteit. De leden van de fractie hebben tevens gevraagd of het niet melden van kwetsbaarheden in de beveiliging niet een vorm van meewerken aan de criminaliteit is, en hebben hierover de mening van de regering gevraagd.

In de beantwoording van een eerdere vraag van de leden van de CDA fractie over het opnemen van een maximale termijn is aangegeven dat juist het melden van een onbekende kwetsbaarheid in gevallen het effect zou hebben criminaliteit ongemoeid te laten omdat de opsporing niet kan worden voortgezet. Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet en van belang voor het recht doen aan slachtoffers. Zoals in antwoord op diverse vragen hierboven is aangegeven levert het voorliggende wetsvoorstel hieraan een belangrijke bijdrage. Daarnaast zijn de inzet en het gebruik van onbekende kwetsbaarheden met diverse waarborgen omkleed en geldt een verplichting tot melden van deze kwetsbaarheden met de mogelijkheid van tijdelijk uitstel. In het licht hiervan ziet de regering niet in waarom deze bevoegdheidsuitoefening zou neerkomen op een vorm van meewerken aan criminaliteit.

De leden van de fractie van de PvdA hebben gevraagd of zij het goed hebben begrepen dat de voorgestelde bevoegdheid voor opsporingsinstanties om onder voorwaarden een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen impliceert dat de overheid hackkennis op de markt zal gaan verwerven.

De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorstelde bevoegdheid tot het binnendringen in een geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in geautomatiseerd werk wordt uitgevoerd. Niet kan worden uitgesloten dat dergelijke software gebruik maakt van onbekende kwetsbaarheden. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. Het heimelijk binnendringen is een specialistische techniek, waarvoor grote deskundigheid op het gebied van informatie- en communicatietechnologie is vereist. Toepassing is voorbehouden aan de daartoe speciaal aangewezen opsporingsambtenaren die over deze expertise beschikken en die deel uitmaken van een speciaal team, een technisch

team bij de Landelijke eenheid van de Nationale politie. Om hun kennis actueel te houden zullen zij herhaaldelijk cursussen en opleidingen volgen.

De leden van de fractie van de PvdA hebben opgemerkt dat op grond van het voorliggende wetsvoorstel opsporingsinstanties bij het hacken zelfs gebruik mogen maken van onbekende kwetsbaarheden in de software. De leden van deze fractie hebben gevraagd of de regering zo niet het risico loopt mee te werken aan het in stand houden van de markt van onbekende kwetsbaarheden, waarmee veel geld wordt verdiend ten koste van de digitale veiligheid van de Nederlandse burgers.

In aanvulling op de eerdere beantwoording van de vragen van de leden van de fracties van de SP en de PvdA wordt benadrukt dat de politie zich niet begeeft op de markt voor onbekende kwetsbaarheden. De markt voor software ten behoeve van het binnendringen in een geautomatiseerd werk is internationaal van aard en bestaat onafhankelijk van dit wetsvoorstel. De invloed van de Nederlandse opsporingsdiensten op deze markt is gering. Van het in stand houden van de markt door de aanschaf van dergelijke software is dan ook geen sprake.

De leden van de fractie van de PvdA hebben erop gewezen dat de in artikel 126ffa voorgestelde regeling het mogelijk maakt dat die melding op grond van een zwaarwegend opsporingsbelang wordt uitgesteld en dat Bits of Freedom bij brief van 23 februari 2017 een aantal kritische kanttekeningen heeft geformuleerd bij dit artikel. De leden van deze fractie hebben de regering verzocht ten gronde te reageren op de volgende opmerkingen:

1. De opsporingsinstanties zullen veelal gebruikmaken van softwarepakketten die het hacken sterk vergemakkelijken. Volgens Bits of Freedom zullen opsporingsinstanties vaak niet weten van welke kwetsbaarheden daarbij gebruik wordt gemaakt en of deze gemeld moeten worden: «Als de Nederlandse opsporingsdiensten niet weten of zij gebruik maken van onbekende kwetsbaarheden, dan hoeven zij deze ook niet te melden. Wat je niet weet kun je immers niet melden. De meldplicht wordt dan omzeild.»
   De politie zal geen informatie over onbekende kwetsbaarheden inkopen ten behoeve van de inzet van de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk. Wel is het mogelijk dat de politie software aanschaft waarmee in bepaalde gevallen het binnendringen in een geautomatiseerd werk wordt uitgevoerd. Niet kan worden uitgesloten dat dergelijke software gebruik maakt van onbekende kwetsbaarheden. Leveranciers van dergelijke software geven hun broncode doorgaans niet prijs. Indien de politie of het openbaar ministerie kennis verwerft over onbekende kwetsbaarheden in hard- of software waarmee op afstand heimelijk een geautomatiseerd werk kan worden binnengedrongen, dan worden deze in beginsel gemeld aan de fabrikant van de desbetreffende hard- of software. Dat is ook het geval indien door de politie aangekochte software hiervan gebruik maakt.
2. Het is volgens Bits of Freedom zeer aannemelijk dat onbekende kwetsbaarheden gebruikt worden in hacksoftware. Die zullen door het bedrijf dat die software levert, zelf gevonden of ingekocht zijn: «In ieder geval zal de Nederlandse overheid daarmee wel degelijk een bijdrage leveren aan het vercommercialiseren van onze digitale kwetsbaarheid.»
   Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de PvdA.

3. Als de betreffende opsporingsinstantie al weet welke onbekende kwetsbaarheden worden gebruikt, dan is het nog maar de vraag of zij dat wel zal melden. Op grond van geheimhoudingsverklaringen die de leverancier van de hacksoftware zal bedingen, zal het de opsporingsinstanties verboden zijn om onbekende kwetsbaarheden bekend te maken, aldus Bits of Freedom.
   Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fractie van de PvdA.
4. Het gebruik van de betreffende hacksoftware is volgens Bits of Freedom omstreden, omdat deze ook zal worden geleverd aan landen die het niet zo nauw nemen met de grondrechten van hun burgers. Gezien de mogelijkheden om kennis over kwetsbaarheden voor ongewenste doeleinden in te zetten, is de verkoop ervan aan bepaalde partijen onwenselijk. De mogelijkheid tot anonimiteit op het internet maakt het echter gemakkelijk om heimelijk kennis over kwetsbaarheden aan te bieden en aan te schaffen. Zoals hiervoor is aangegeven is de markt voor software ten behoeve van het binnendringen in een geautomatiseerd werk internationaal van aard en bestaat deze markt onafhankelijk van dit wetsvoorstel. De invloed van de Nederlandse opsporingsdiensten op deze markt is dan ook gering. De verkoop van technologie voor «intrusion software», die gebruik maakt van kwetsbaarheden, is onderhevig aan exportcontrole op grond van de Europese Dual-use verordening. De Europese Commissie heeft een voorstel gedaan voor de herziening van de bestaande verordening met het doel deze te moderniseren en beter aan te laten sluiten op de internationale ontwikkelingen. De Commissie stelt onder meer voor om de controle van export van cybertoezichttechnologie te intensiveren in relatie tot mensenrechtenschendingen. Nederland is voorstander van het uitbreiden van de reeds bestaande controle op apparatuur voor cybertoezicht met het voorkomen van mensenrechtenschendingen als grondslag. De EU loopt daarmee wereldwijd voorop en het sluit aan bij de bestaande Nederlandse praktijk waarbij mensenrechten als criterium voor exportcontrole wordt toegepast.
5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt volgens Bits of Freedom in de praktijk niet, omdat het kan betekenen dat het ene opsporingsteam (gezien het zwaarwegende opsporingsbelang) wel machtiging van de rechter-commissaris krijgt voor uitstel van de melding, terwijl een andere opsporingsteam dat gebruikmaakt van dezelfde onbekende kwetsbaarheid, geen toestemming krijgt (vanwege een geringer opsporingsbelang) en dus de betreffende kwetsbaarheid zou moeten melden, waarna het beveiligingslek gedicht gaat worden. Dat laatste zou echter het werk van het eerstgenoemde opsporingsteam verstoren.

Voor kwetsbaarheden die in een opsporingsonderzoek worden aangetroffen geldt dat er in uitzonderlijke gevallen redenen kunnen zijn die het melden (tijdelijk) in de weg staan. In dergelijke gevallen kan het openbaar ministerie, na machtiging van de rechter-commissaris, besluiten de melding van een kwetsbaarheid uit te stellen. Deze afweging overstijgt het individuele opsporingsonderzoek en wordt daarom binnen het openbaar ministerie centraal gemaakt. Daarbij wordt onder meer gelet op de kans dat de kwetsbaarheid door kwaadwillenden wordt uitgebuit en het aantal onschuldige personen en organisaties dat hierdoor kwetsbaar is. De opdracht om de kwetsbaarheid te melden komt terecht bij hetzelfde team van de Landelijke eenheid van de Nationale politie. Bij dat team is het overzicht over het gebruik en melden van onbekende kwetsbaarheden.

De leden van de fractie van de PvdA hebben aandacht gevraagd voor de aanschaf en veiligheid van de malware die Nederlandse opsporingsinstanties gaan gebruiken. Met verwijzing naar de brief van Bits of Freedom, waarin wordt gewezen op de Bundestrojaner-affaire en de Verint-zaak, hebben de leden van deze fractie gevraagd hoe de opsporingsinstanties aan de malware komen, of bepaalde voorwaarden voor de aanschaf worden gehanteerd en of de Nederlandse overheid te allen tijde inzicht in de broncode van de malware eist. Ook hebben deze leden gevraagd hoe van derden gekochte malware wordt gecontroleerd op veiligheid, bijvoorbeeld op de aanwezigheid van zogenaamde backdoors.

In de eerdere beantwoording van een vraag van de leden van de fractie van de SP is reeds ingegaan op de vraag hoe de integriteit van het technische hulpmiddel wordt getoetst. In aanvulling daarop kan worden gemeld dat de technische hulpmiddelen waarmee tijdens de onderzoeksfase onderzoekshandelingen in een geautomatiseerd werk worden verricht, kunnen worden betrokken van verschillende producenten of binnen de politieorganisatie zelf worden ontwikkeld, mits aan de wettelijke vereisten voor keuring wordt voldaan. Voor de selectie van bedrijven geldt de bestaande regelgeving voor inkoop. Overgave van de broncode maakt daar geen deel van uit. Bij de keuring wordt getoetst of een technisch hulpmiddel voldoet aan de technische eisen die zijn neergelegd in het Besluit onderzoek in een geautomatiseerd werk. Een technisch hulpmiddel dient onder meer in staat te zijn om geregistreerde gegevens automatisch naar een technische infrastructuur binnen de politieorganisatie te transporteren en dient beveiligd te zijn tegen wijziging van de werking ervan en wijziging en kennisneming van geregistreerde gegevens door onbevoegde personen. Als een technisch hulpmiddel wordt goedgekeurd door een keuringsdienst, mag er vanuit worden gegaan dat aan de wettelijke eisen wordt voldaan. De keuring van technische hulpmiddelen vindt proefondervindelijk plaats.

De leden van de fractie van de PvdA hebben gevraagd wat de gevolgen zijn van het gebruik van nog onbekende kwetsbaarheden voor de veiligheid van het internet en hoe dit wetsvoorstel zich daarmee verhoudt tot het rapport «De publieke kern van het internet» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).

Een belangrijk begrip in het WRR rapport is de publieke kern van het internet, de kernprotocollen die het fundament vormen voor een goed functionerend internet, waaronder in het bijzonder de zogenoemde internet protocol suite of TCP/IP suite. Het kabinet onderschrijft het belang van het behoud van het vrije en open karakter van het internet als platform voor onbelemmerd dataverkeer ter stimulering van economische groei en innovatie. Hier wil het kabinet zich beperken tot het borgen van de juridische kaders van de rechtsstaat en het beschermen van burgerlijke vrijheden. Opgemerkt wordt dat veiligheid en het respecteren van mensenrechten tevens voorwaarden zijn voor economische groei en innovatie.

De overheid heeft de verantwoordelijkheid om haar burgers ook in een online omgeving te beschermen door de bescherming van hun persoonlijke informatie te bevorderen, cybersecurity te bevorderen en cybercriminaliteit en bedreigingen van de nationale veiligheid te bestrijden of te voorkomen. Internationale samenwerking wordt steeds belangrijker om deze belangen te beschermen in een grenzeloze digitale omgeving. Afspraken over samenwerking, (gedrags)normen en standaarden moeten dan ook bij voorkeur in Europees en in breder internationaal verband worden gemaakt. Bovengenoemde belangen vragen om een geïntegreerde benadering. In de optiek van de regering vormen vrijheid en

veiligheid geen tegengestelde, maar complementaire belangen. De dynamische balans tussen veiligheid, vrijheid en economische groei wordt tot stand gebracht en in stand gehouden in een constante open dialoog tussen alle stakeholders, zowel nationaal als internationaal. Deze visie op de samenhang tussen veiligheid, vrijheid en economische groei als basis voor beleidsafwegingen is verankerd in de Nationale Cyber Security Strategie 2.0.

In het voorliggende wetsvoorstel is de inzet in het kader van de opsporing alleen mogelijk voor ernstige strafbare feiten en is vooraf toestemming van een rechter-commissaris vereist. De proportionaliteit en subsidiariteit worden zo voorafgaand aan de inzet onafhankelijk getoetst. Net als in de fysieke wereld hebben politie en justitie tot taak de criminaliteit op het internet zoveel mogelijk te voorkómen en op te sporen. Het laten voortbestaan van een onbekende kwetsbaarheid kan een risico inhouden op (meer) slachtoffers van criminaliteit. Kwetsbaarheden die in het kader van een opsporingsonderzoek aan het licht komen, en waarvan aannemelijk is dat ze nog onbekend zijn, worden in beginsel direct of zo spoedig mogelijk gemeld aan de fabrikant van de desbetreffende hard- of software.

De leden van de fractie van GroenLinks hebben de regering gevraagd om, in plaats van te verwijzen naar haar brief van inmiddels een aantal maanden geleden, in haar beantwoording heel precies in te gaan op het gevaar van het laten voortbestaan van een kwetsbaarheid die mogelijk tot meer slachtoffers van criminaliteit leidt. De leden van deze fractie hebben tevens gevraagd of dit wetsvoorstel juist kwetsbaarheden openhoudt in plaats van ze te dichten, om zo van deze gaten gebruik te kunnen maken tijdens het hacken, en zouden hierop graag een toelichting van de regering ontvangen.

Effectieve handhaving van de rechtsstaat in cyberspace is een voorwaarde voor een veilig internet en van belang voor zowel het terugdringen van het slachtofferschap, als het recht doen aan slachtoffers. Zoals hierboven, in de beantwoording van de vragen van de leden van verschillende fracties, is aangegeven wordt met dit wetsvoorstel beoogd hieraan een belangrijke bijdrage te leveren. Het gebruik van onbekende kwetsbaarheden kan hier onderdeel van zijn. De inzet en het gebruik van onbekende kwetsbaarheden is met diverse waarborgen omkleed. Deze zijn hiervoor aan de orde gekomen, eveneens in antwoord op eerdere vragen hierover van leden van verschillende fracties. Naar die antwoorden wordt op deze plaats kortheidshalve verwezen.

6. Lokpuber en grooming

De leden van de fractie van het CDA hebben gevraagd of het klopt dat poging tot grooming strafbaar blijft in het onderhavige wetsvoorstel. De leden van deze fractie hebben opgemerkt op dat, hoewel daar in de optiek van deze leden inhoudelijk veel voor te zeggen is, poging tot grooming volgens de Afdeling advisering van de Raad van State strafbaarstelling van een «poging tot een poging» is, omdat er volgens staande jurisprudentie nog geen uitvoeringshandeling plaatsvindt. De leden van deze fractie hebben de regering gevraagd juridisch te beargumenteren waarom het advies van de Afdeling advisering niet is gevolgd.

In het advies over het wetsvoorstel (Kamerstukken II 2015/16, 34 372, nr. 4) heeft de Afdeling advisering een opmerking gemaakt over de passage in de memorie van toelichting dat bij wet de strafbaarheid van poging tot grooming niet is uitgesloten. De Afdeling advisering heeft opgemerkt dat het wetsvoorstel geen wijziging aanbrengt die ziet op de strafbaarheid van

poging tot grooming, zodat de toelichting op het wetsvoorstel voor het al dan niet strafbaar zijn van poging tot grooming geen bepalende rol kan spelen. Gelet hierop heeft de Afdeling advisering geadviseerd om de bewuste passage te schrappen.

In het nader rapport (Kamerstukken II 2015/16, 34 372, nr. 4) heeft de regering zich op het standpunt gesteld dat voor de strafbaarstelling van een poging tot grooming geen uitdrukkelijke wettelijke regeling noodzakelijk is en heeft de regering nader toegelicht waarom de strafbaarheid van de poging tot grooming niet bij wet is uitgesloten. Gewezen is op 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) (Verdrag van Lanzarote). Dit artikel verplicht tot het strafbaar stellen van poging tot (onder andere) grooming, tenzij een partij zich het recht heeft voorbehouden de poging niet toe te passen (artikel 24, derde lid, van het Verdrag van Lanzarote). Nederland heeft geen gebruik gemaakt van de uitzonderingsmogelijkheid die het verdrag biedt. In het kader van het ratificatietraject van het verdrag is met verwijzing naar artikel 45 Sr opgemerkt dat poging tot het plegen van misdrijven in Nederland strafbaar is (Kamerstukken II 2008/09, 31 808 (R1872), nr. 3; artikelsgewijze toelichting bij artikel 24). In reactie op het advies van de Afdeling advisering is de memorie van toelichting aangevuld met een passage over het ratificatietraject (Kamerstukken II 2015/16, 34 372, nr. 3, blz. 91).

De leden van de fractie van het CDA hebben gevraagd of de regering kan beargumenteren of, en zo ja hoe, het opsporen van pedofielen door middel van een «virtuele lokpuber» door een (meerderjarige) opsporingsambtenaar tot een eventuele strafbaarstelling van de opgespoorde pedofiel kan leiden. De leden van deze fractie hebben erop gewezen dat de jurisprudentie niet eenduidig is over de strafbaarheid van het ingaan op de lokroep van een virtuele lokpuber waarachter een meerderjarige ambtenaar schuilgaat en vragen of dit in de ogen van de regering strafbaar is.

Op grond van de huidige delictsomschrijvingen in de artikelen 248a Sr (verleiding van een minderjarige) en 248e Sr (grooming) is het niet strafbaar om contact te leggen met iemand die in werkelijkheid geen minderjarige is. Het wetsvoorstel wijzigt deze artikelen waardoor het contact leggen voor seksuele doeleinden met iemand die zich voordoet als een minderjarige alsnog strafbaar wordt. Hierdoor wordt de inzet van de lokpuber, een opsporingsambtenaar die zich voordoet als een kind, bij de opsporing van online verleiding van een minderjarige en grooming mogelijk.

Voor de strafbaarheid van verleiding van een minderjarige tot ontucht is in de eerste plaats vereist dat sprake is van verleiding, misbruik van uit feitelijke verhoudingen voorvloeiend overwicht of misleiding. In de tweede plaats dient de dader de minderjarige dan wel degene die zich als zodanig voordoet door middel van voornoemde middelen opzettelijk te bewegen tot het plegen of dulden van ontuchtige handelingen. In de derde plaats dient het opzet gericht te zijn op het plegen van ontuchtige handelingen of het dulden van zodanige handelingen van de verdachte door de minderjarige of degene die zich als zodanig voordoet.

Voor de strafbaarheid van grooming zijn de volgende elementen essentieel. In de eerste plaats dient de dader door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst in contact te komen met een kind beneden de leeftijd van zestien jaren of met iemand die zich als zodanig voordoet. In de tweede plaats is bij de

dader het oogmerk vereist om ontuchtige handelingen te plegen met een persoon die de leeftijd van zestien jaren nog niet bereikt heeft of een afbeelding van een seksuele gedraging te vervaardigen waarbij een persoon die de leeftijd van zestien jaren nog niet bereikt heeft is betrokken. In de derde plaats dient de dader enige handeling te ondernemen gericht op het verwezenlijken van een ontmoeting met een vorenbedoelde persoon.

De leden van de fractie van D66 hebben verwezen naar een recent artikel in de Ars Aequi van mr. dr. K. Lindenberg en opgemerkt dat lokpuberzaken waarbij een opsporingsambtenaar zich op het internet voordoet als jeugdige vooralsnog vaak gedoemd zijn te mislukken, omdat voor de strafbaarheid noodzakelijk is dat de verdachte daadwerkelijk met een minderjarige heeft gecommuniceerd. De leden van deze fractie hebben geconstateerd dat het onderhavige wetsvoorstel het gebruik van de lokpuber mogelijk wil maken door aanvullende strafbaarheid te creëren voor het handelen jegens iemand die zich voordoet als kind. In dit verband hebben zij gevraagd in hoeverre de inzet van de lokpuber in overeenstemming is met het instigatieverbod.

Opsporingsambtenaren kunnen volgens bestendige rechtspraak van de Hoge Raad op basis van algemene taakstellende bepalingen – het betreft de artikelen 3 van de Politiewet 2012 en 141 Sv – onder voorwaarden bevoegd zijn tot het inzetten van lokmiddelen. Eén van de voorwaarden is dat de verdachte door het optreden van de opsporingsambtenaar niet wordt gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht (het zogenoemde Tallon-criterium, Hoge Raad 4 december 1979, NJ 1989, 356; zie Hoge Raad 28 oktober 2008, NJ 2009, 224 voor de inzet van een lokfiets). In de praktijk leidt het uitlokkingsverbod ertoe dat een opsporingsambtenaar in beginsel zelf de communicatie niet start, maar afwacht totdat iemand contact met hem legt voor seksuele doeleinden.

De leden van de fractie van de ChristenUnie hebben gevraagd of het voorgestelde artikel 248a Sr ruimte biedt voor anderen dan opsporingsambtenaren om zich voor te doen als een virtuele creatie van iemand die de leeftijd van achttien jaren nog niet heeft bereikt en zo een bijdrage te leveren aan de opsporing. De leden van deze fractie hebben tevens gevraagd of de regering dergelijke initiatieven wenst of dat de opsporing beperkt dient te blijven tot de politie.

Artikel 248a Sr stelt niet als voorwaarde dat een opsporingsambtenaar zich – al dan niet met behulp van een virtuele kindcreatie – voordoet als een minderjarige. In zoverre laat het artikel ruimte voor betrokkenheid van anderen dan opsporingsambtenaren bij de inzet van de lokpuber voor de opsporing van online zedendelicten. De regering is evenwel geen voorstander van burgeropsporing. De opsporing en vervolging van zedenmisdrijven zijn taken voor de politie en het openbaar ministerie. In het bijzonder bij gevoelige misdrijven als zedenmisdrijven dient de opsporing te worden overgelaten aan de opsporingsorganisaties, die beschikken over de benodigde bevoegdheden en expertise. De inzet van lokmiddelen is maatwerk en vraagt om specifieke deskundigheid. Om te voorkomen dat sprake is van ongeoorloofde uitlokking en onrechtmatig verkregen bewijs zal de opsporingsambtenaar die als lokpuber fungeert zich in de praktijk passief opstellen, wachten tot iemand contact legt voor seksuele doeleinden en tijdens die contacten behoedzaam te werk gaan.

De inzet van de lokpuber, een opsporingsambtenaar die zich online voordoet als minderjarige, moet onderscheiden worden van de inzet van een virtuele kindcreatie. Een virtuele kindcreatie is een softwareapplicatie

waarin een voorgeprogrammeerd virtueel personage (een «avatar») wordt gebruikt als lokprofiel om in contact te komen met mensen die webcamseks willen met een minderjarige. Het openbaar ministerie maakt tot nu toe geen gebruik van virtuele kindcreaties bij de opsporing van online zedendelicten, omdat uit praktijkervaringen is gebleken dat uitlokking hierbij onvermijdelijk is. Naar aanleiding van het Sweetieproject van Terres des Hommes, waarin gebruik werd gemaakt van virtuele kindcreaties, heeft het openbaar ministerie enkele tientallen zaken in onderzoek gehad. In geen van de zaken is vervolging ingesteld ter zake van grooming of verleiding van een minderjarige, omdat telkens sprake was van ongeoorloofde uitlokking (zie ook: Aanhangsel Handelingen, 2016/17, nr. 948).

De leden van de fractie van de ChristenUnie hebben gevraagd om uitleg bij de voorgestelde redactie van artikel 248a Sr.

Door de voorgestelde wijziging van artikel 248a Sr wordt verleiding tot ontucht van iemand die zich voordoet als een minderjarige strafbaar. In de eerste plaats is vereist dat sprake is van verleiding (giften of beloften van geld of goed), misbruik van uit feitelijke verhoudingen voorvloeiend overwicht of misleiding. In de tweede plaats dient de dader de minderjarige of degene die zich als zodanig voordoet door middel van voornoemde middelen opzettelijk te bewegen tot het plegen of dulden van ontuchtige handelingen. In de derde plaats dient het opzet gericht te zijn op het plegen van ontuchtige handelingen of het dulden van zodanige handelingen van de verdachte door de minderjarige of degene die zich als zodanig voordoet. Uit de bewijsmiddelen zal moeten blijken dat er tussen verdachte en de al dan niet zich als zodanig voordoende minderjarige enigerlei voor het plegen dan wel dulden van ontucht relevante interactie is geweest.

De leden van de fractie van de ChristenUnie meenden dat er geen advies aan de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen is gevraagd over de toepassing van het voornoemde artikel. Gelet op het onderwerp zou een advies volgens de leden van deze fractie in de rede liggen en van meerwaarde zijn bij de beoordeling van het wetsvoorstel. Zij wilden hierop graag de reactie van de regering vernemen.

De Nationaal Rapporteur Mensenhandel en Seksueel Geweld is niet formeel om advies gevraagd over het wetsvoorstel. In haar rapport «Op goede grond» (2014) gaat de Nationaal Rapporteur in op de voorgenomen wetswijziging met het oog op de inzet van de lokpuber. Zij merkt op dat hoewel een uitbreiding van de strafrechtelijke aansprakelijkheid tot het contact leggen met iemand die zich voordoet als een minderjarige vanuit opsporingsoogpunt wenselijk is, het wel van belang is dat in de toelichting bij het wetsvoorstel expliciet afstand wordt gedaan van de inzet van deze opsporingsmethode door burgers, zoals zelfbenoemde «pedojagers».

7. Geautomatiseerd werk

De leden van de fractie van D66 hebben opgemerkt dat de criteria voor de inzet van de hackbevoegdheid hetzelfde zijn als voor de inzet van een telefoon- of internettap en dat deze bevoegdheid vrijwel alle elektronische apparaten omvat (hetgeen met het internet of things de komende jaren alleen maar in omvang zal toenemen). De leden van deze fractie hebben gevraagd of de regering kan uitleggen waarom niet is gekozen voor een lijst met een limitatieve opsomming van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden en specifieke apparaten die gehackt

mogen worden. De leden van de fractie van de SP hebben opgemerkt dat nagenoeg alle apparaten onder de hackbevoegdheid vallen en zouden ook graag een lijst zien van apparaten waarvan de regering van mening is dat deze onder het begrip «geautomatiseerd werk» vallen.

De bevoegdheid tot het aftappen en opnemen van communicatie (artikelen 126m/t en 126zg Sv) kan worden gebruikt om door middel van een internettap in kaart te brengen welk verkeer met het internet via een router van een thuisnetwerk of een zogenaamde openbare «hotspot» is waar te nemen. De wettelijke voorwaarden voor de toepassing van deze bevoegdheid zijn deels – voor wat betreft bijvoorbeeld de toepassing van de onderzoekshandelingen van het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie – gelijk aan die voor de voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk. Het doel van het binnendringen met het oog op het verrichten van die onderzoekshandelingen wijkt in dergelijke gevallen – het aftappen en opnemen van communicatie of het opnemen van vertrouwelijke communicatie – niet af van de bestaande bevoegdheid van het aftappen en opnemen van communicatie of het gebruik van een richtmicrofoon. De bevoegdheid van het op afstand heimelijk binnendringen van een smartphone met het oog op het aftappen en opnemen van communicatie kan onvermijdelijk zijn om de versleuteling van de communicatie te omzeilen. Om die reden ligt een beperking van de bevoegdheid tot delicten die op een lijst zijn geplaatst, zoals door de leden van de fractie van D66 gesuggereerd, minder voor de hand. Voor de opsporing zou dat een stap terug betekenen in vergelijking met de bestaande bevoegdheden rond het aftappen en opnemen van (vertrouwelijke) communicatie.

De regering is ook overigens geen voorstander van een lijst van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden. Dit geldt ook voor een eventuele lijst van specifieke apparaten die gehackt zouden mogen worden. In beide gevallen zou dit de opsporing van ernstige strafbare feiten ernstig belemmeren. Zoals in de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van GroenLinks is aangegeven, is niet gekozen voor een limitatieve opsomming van geautomatiseerde werken of voor het uitzonderen van geautomatiseerde werken omdat niet valt te voorzien welke innovaties zich bij diverse apparaten zullen voordoen en welke werkwijzen criminelen zich in de toekomst eigen zullen maken. Bovendien biedt het uitsluiten van bepaalde geautomatiseerde werken criminelen meer mogelijkheden de opsporing te ontlopen door juist dergelijke systemen te misbruiken voor het plegen van strafbare feiten. Dat is niet in het belang van de veiligheid van dergelijke systemen. Indien mogelijk wordt uiteraard gekozen voor de inzet van minder vergaande bevoegdheden, zoals een vordering tot verstrekking van gegevens aan de beheerder van het desbetreffende systeem.

De leden van de fractie van de ChristenUnie hebben geconstateerd dat met de definitie van geautomatiseerd werk in het voorgestelde artikel 80sexies een zeer brede categorie ontstaat omdat naast communicatiemiddelen ook huishoudelijke apparatuur, energiemeters en zelfs apparaten in het menselijk lichaam, zoals de pacemaker, onder deze definitie kunnen vallen. De leden van deze fractie hebben gevraagd of is overwogen een meer limitatieve lijst op te stellen of dat op andere wijze een begrenzing is overwogen. Zij kunnen zich bijvoorbeeld voorstellen dat apparatuur in het menselijk lichaam wordt uitgesloten.

Voor de beantwoording van deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66 en de SP. In aanvulling daarop kan worden opgemerkt dat, hoewel een pacemaker in beginsel onder de definitie van geautomatiseerd werk valt, hierin naar verwachting geen gegevens te vinden zullen zijn die bijdragen aan de opsporing van ernstige vormen van computercriminaliteit of andere ernstige strafbare feiten. Hier komt bij dat de officier van justitie zal moeten onderbouwen dat het bevel voldoet aan de vereisten van proportionaliteit en subsidiariteit. Het is niet waarschijnlijk dat er zich een geval voordoet waarin de rechter-commissaris het binnendringen in een pacemaker als proportioneel zal beschouwen. In de praktijk is het dan ook moeilijk denkbaar dat er zich een zo zwaar wegend belang voordoet dat het op afstand heimelijk binnendringen van een pacemaker proportioneel zou worden geacht.

8. Toezicht

De leden van de fractie van D66 hebben erop gewezen dat een belangrijk onderdeel van het advies van de Afdeling advisering van de Raad van State het instellen van een orgaan dan wel instantie betrof die belast zou worden met het houden van structureel systeemtoezicht op de toepassing van de nieuw voorgestelde bevoegdheden, met name in de gevallen waarin het gebruik van de bevoegdheden ten aanzien van een geautomatiseerd werk niet tot een veroordeling door een (straf)rechter heeft geleid. De leden van deze fractie hebben gevraagd of de regering kan uitleggen waarom er geen structureel toezicht in het leven geroepen wordt. De leden van de fractie van de SP hebben eveneens gewezen op het advies van de Afdeling advisering om te voorzien in onafhankelijk toezicht op het binnendringen in de digitale omgeving en gevraagd waarom de regering niet heeft gekozen om deze wetgeving met goed toezicht te omkleden. De leden van de fractie van de PvdA hebben het advies van de Afdeling advisering van de Raad van State aangehaald, waarin de Afdeling heeft geadviseerd 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. De leden van deze fractie hebben de regering gevraagd nog eens ten gronde uit een te zetten waarom zij meent dat het niet nodig is het advies van de Afdeling en de daarbij gedane concrete suggesties voor de invulling van dat toezicht op te volgen.

Anders dan de Afdeling advisering is de regering van oordeel dat de bestaande regeling voor de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering, aangevuld met de extra maatregelen op grond van het voorliggende wetsvoorstel, in voldoende waarborgen voorziet om een rechtmatige en zorgvuldige toepassing van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk te garanderen. Het wetsvoorstel voorziet niet in een bevoegdheid tot het grootschalig verzamelen van informatie over onschuldige burgers; het wetsvoorstel past veeleer in het bestaande systeem van bijzondere opsporingsbevoegdheden waarbij een strafrechtelijke relevante verdenking van betrokkenheid van een persoon bij het beramen of plegen van strafbare feiten aanleiding kan geven tot het heimelijk inzetten van bijzondere opsporingsbevoegdheden ten behoeve van de waarheidsvinding. Hierbij is geen sprake van het grootschalig verzamelen van informatie met betrekking tot onschuldige burgers. Het wettelijk systeem rond de bijzondere opsporingsbevoegdheden is gebaseerd op het uitgangspunt dat het handelen van de opsporingsambtenaar wordt gecontroleerd door de officier van justitie, als leider van het opsporingsonderzoek. De officier van justitie heeft het gezag over de opsporing van strafbare feiten. Die verantwoordelijkheid omvat het toezicht op de

rechtmatigheid van het optreden van de opsporingsambtenaar in het kader van de strafrechtelijke handhaving van de rechtsorde. De officier van justitie is lid van het openbaar ministerie en is rechterlijk ambtenaar (art. 1, onderdeel b, Wet RO). De procureur-generaal bij de Hoge Raad waakt over de naleving van de wettelijke voorschriften door het openbaar ministerie. Als de officier van justitie strafvervolging instelt dan wordt het toezicht op de rechtmatigheid van het handelen van de opsporingsambtenaar en de officier van justitie uitgeoefend door de rechter. Dit betreft de rechter die ter terechtzitting oordeelt over het tenlastegelegde. De toepassing van bepaalde bijzondere opsporingsbevoegdheden is vanwege de ernst van de inbreuk op de grondrechten van burgers, zoals het recht op bescherming van de persoonlijke levenssfeer (artikel 10 GW), afhankelijk van een voorafgaande rechterlijke instemming. De officier van justitie is gehouden aan de betrokkene schriftelijk mededeling te doen van de uitoefening van een bijzondere opsporingsbevoegdheid, zodra het belang van het onderzoek dat toelaat (artikel 126bb, eerste lid, Sv). Aldus is de betrokkene in staat zich over het inzetten van de bevoegdheid te beklagen. Voor zover de klacht geen betrekking heeft op een gedraging waarop de rechter toeziet, is de Nationale ombudsman bevoegd de klacht in behandeling te nemen (artikel 9:22 en 9:23 Awb). Tenslotte is de Autoriteit persoonsgegevens belast met het toezicht op de naleving van de wetgeving op het gebied van de bescherming van persoonsgegevens door de rechtshandhavingsdiensten. De Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens geven regels met het oog op een zorgvuldige verwerking van persoonsgegevens door ambtenaren van politie en het openbaar ministerie.

Aldus voorziet de regeling rond de inzet van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering op dit moment in uitgebreide waarborgen voor een rechtmatige en zorgvuldige inzet van die bevoegdheden. De kern daarvan wordt gevormd door het onafhankelijk toezicht door een rechter. In sommige gevallen, waarbij dit vanwege de inbreuk van de bevoegdheid op de persoonlijke levenssfeer van de betrokkene aan de orde is, is tevens rechterlijke tussenkomst vereist voordat een bijzondere opsporingsbevoegdheid kan worden ingezet. Voor de voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk zal aanvullend gelden dat de Centrale Toetsingscommissie van het openbaar ministerie vooraf de voorgenomen inzet toetst. De CTC is een adviesorgaan van het College van procureurs-generaal en zal het College ook adviseren over de voorgenomen inzet van het onderzoek in een geautomatiseerd werk. Aldus is de toestemming nodig van het College voordat deze opsporingsbevoegdheid in een concreet geval kan worden toegepast. Hiermee wordt voorzien in een gedegen toezicht binnen het openbaar ministerie op de voorgenomen inzet van de bevoegdheid. Wat betreft het toezicht achteraf geldt dat, op grond van de Politiewet 2012, de Inspectie Veiligheid en Justitie (VenJ) als rijksinspectie is belast met het toezicht op de kwaliteit van de taakuitvoering van de politie. Dit toezicht betreft de naleving van de wet- en regelgeving rond de toepassing van die bevoegdheden en de kwaliteit van de uitvoering en laat het gezag van de burgemeester en de officier van justitie onverlet. Dit toezicht omvat zowel de gevallen die, in het kader van de door het openbaar ministerie ingestelde strafvervolging jegens een verdachte, aan het oordeel van de rechter worden voorgelegd als de gevallen die niet tot strafvervolging jegens een verdachte leiden. Als rijksinspectie heeft de Inspectie VenJ de ruimte om zelf informatie te verzamelen, daarover een oordeel te vormen, en daarover te rapporteren en te adviseren. Er is dus sprake van onafhankelijke oordeelsvorming. De inspecteurs beschikken over de nodige wettelijke toezichtbevoegdheden op grond van de Algemene wet bestuursrecht.

Het toezicht van de Inspectie VenJ is gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk. Het toezicht heeft betrekking op aspecten als de autorisaties van de bevoegde opsporingsambtenaren voor de uitvoering van het bevel van de officier van justitie voor het onderzoek in een geautomatiseerd werk, de expertise en kennis van de betrokken opsporingsambtenaren, de inzet van het technische hulpmiddel (kwaliteit en betrouwbaarheid), de vastlegging van gegevens over de werking van het technische hulpmiddel en over de toepassing van onderzoekshandelingen in het geautomatiseerde werk (logging), de beveiliging van de vastgelegde gegevens en het gebruik van de gegevens, inclusief de bewaring en vernietiging daarvan.

Gelet op de bestaande structuren en voorzieningen is er geen aanleiding te voorzien in meer aanvullend toezicht. Als, naast de besproken instanties, nog een afzonderlijk orgaan wordt ingericht voor het uitoefenen van toezicht op de voorgestelde bevoegdheid tot het binnendringen van een geautomatiseerd werk, dan zullen de verschillende instanties elkaar eenvoudigweg voor de voeten gaan lopen of op zijn minst dubbel werk verrichten. En als het gaat om eventueel onderzoek door een dergelijk orgaan naar klachten moet worden opgemerkt dat de Nationale ombudsman daartoe thans bevoegd is. Ook op dit punt valt dan ook niet goed in te zien hoe een nieuw toezichthoudend orgaan van toegevoegde waarde zou kunnen zijn.
Dit alles overziend is de regering van oordeel dat in het voorliggende wetsvoorstel is voorzien in adequate en effectieve waarborgen tegen misbruik van de voorgestelde bevoegdheid. Deze waarborgen acht de regering ruimschoots voldoende om een rechtmatige en zorgvuldige toepassing van de bevoegdheden te kunnen garanderen. In aanvulling op het rechterlijk toezicht is op grond van de Politiewet 2012 voorzien in toezicht door de Inspectie VenJ. Op basis van haar wettelijke taak is de Inspectie VenJ de aangewezen instantie voor de uitoefening van het toezicht op de uitvoering van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk binnen de grenzen van het bevel van de officier van justitie en de machtiging van de rechter-commissaris.

De leden van de fractie van D66 hebben voorts gevraagd of er voldoende toezicht en rechtsbescherming voor de verdachte is en of de privacy van onschuldige derden is gewaarborgd.

Voor het antwoord op de vraag of er voldoende toezicht is wordt verwezen naar hetgeen daarover is opgemerkt in de beantwoording van de soortgelijke vragen van de leden van de fracties van D66, de SP en ChristenUnie. In aanvulling daarop kan worden opgemerkt dat er een notificatieplicht geldt, zodat de betrokkene in kennis wordt gesteld van de inzet van de bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk. Dit betreft de bestaande wettelijke regeling voor de notificatie van bijzondere opsporingsbevoegdheden (artikel 126bb Sv). De privacy van onschuldige derden is zo veel mogelijk gewaarborgd. Dit komt onder meer tot uitdrukking in het vereiste dat het geautomatiseerde werk dat op afstand heimelijk wordt binnengedrongen, bij de verdachte in gebruik moet zijn (artikel 126nba/uba/zpa, eerste lid, Sv). Verder dient de officier van justitie in het bevel een aanduiding van de aard en functionaliteit van het technische hulpmiddel op te nemen dat wordt gebruikt voor de uitvoering van het bevel, en ten aanzien van welke categorie van gegevens aan het bevel uitvoering wordt gegeven (artikel 126nba/uba/zpa, tweede lid, onderdelen d en f, Sv). De toepassing van sommige uitvoeringshandelingen is echter niet bij voorbaat beperkt tot een verdachte. Dit betreft bijvoorbeeld het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie (artikel 126l/s/zf en 126m/t/zg Sv) die vanwege het belang van de waarheids-

vinding ook gericht kunnen zijn op communicatie van een onbekende verdachte of van anderen dan de verdachte. Voorwaarde is dat toepassing van de opsporingsbevoegdheid jegens een persoon nodig is in het belang van het onderzoek. Overigens heeft de inzet van deze bevoegdheden naar zijn aard tot gevolg dat gegevens van derden ter kennis komen van de opsporing. Als het telefoongesprek wordt afgeluisterd of het vertrouwelijke gesprek met een richtmicrofoon wordt opgenomen komt de inbreng van alle gesprekspartners ter kennis van de opsporing. Op grond van de wet gelden specifieke termijnen voor de bewaring en vernietiging van de met behulp van deze bevoegdheden verzamelde gegevens; deze worden vernietigd binnen twee maanden nadat de zaak geëindigd, behoudens gebruik voor ander strafrechtelijk onderzoek (artikel 126cc, tweede lid, Sv).

Onder verwijzing naar het door de Afdeling advisering genoemde probleem van de internationale omgeving hebben de leden van de fractie van de SP de vraag gesteld hoe de rechter zou moeten oordelen als de indringing heeft plaatsgevonden op het terrein van een ander land.

De Nederlandse wet staat niet in de weg aan optreden buiten het Nederlandse grondgebied. Artikel 539a Sv voorziet in een wettelijke basis om opsporingshandelingen te verrichten buiten Nederland, voor zover het volkenrecht en interregionale recht dit toelaten. Op grond van het volkenrecht is het soevereiniteitsbeginsel relevant, dat ertoe strekt dat een staat slechts uitvoerende rechtsmacht mag uitoefenen op het grondgebied van een andere staat met instemming van die staat. Die instemming kan worden verkregen door middel van een verzoek om rechtshulp. Met een rechtshulpverzoek wordt het respect voor de soevereiniteit en de territoriale integriteit van de aangezochte staat tot uitdrukking gebracht, op grond waarvan de aangezochte staat primair zelf bevoegd is om zelf op te treden tegen inbreuken op de rechtsorde die op het eigen grondgebied worden beraamd of gepleegd.

Uit het beginsel van soevereiniteit vloeit voor dat als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden, een verzoek om rechtshulp aangewezen is. Het soevereiniteitsbeginsel is echter voornamelijk van belang voor de relatie tussen staten en is minder relevant voor de beoordeling van de strafbaarheid van daders. Zo heeft de Hoge Raad geoordeeld dat de vraag of door Nederlandse opsporingsambtenaren het volkenrecht is nageleefd, in die zin dat geen inbreuk is gemaakt op soevereiniteit van de staat binnen de grenzen waarvan is opgetreden, in beginsel in de strafzaak tegen verdachte niet relevant is omdat de belangen die het volkenrecht beoogt te beschermen geen belangen zijn van de verdachte maar van de staat op het grondgebied waarvan buitenlandse opsporingsambtenaren optreden (HR 5 oktober 2010, ECLI: NL: HR: 2010: BL5629 en HR 17 april 2012, ECLI: NL: HR: 2012: BV9070). Op basis van deze jurisprudentie kan worden geconcludeerd dat wanneer Nederlandse opsporingsambtenaren inbreuk zouden maken op de soevereiniteit van een andere staat doordat op afstand heimelijk een geautomatiseerd werk wordt binnengedrongen dat zich op het grondgebied van een andere staat bevindt, dit in de strafzaak tegen de verdachte in beginsel niet relevant is. Daarbij merk ik nog op dat als blijkt dat gegevens zich op het territorium van een andere staat bevinden, een rechtshulpverzoek aangewezen is. Dit komt in paragraaf 11 nader aan de orde, naar aanleiding van een vraag van de leden van de fractie van GroenLinks.

De leden van de fractie van GroenLinks meenden dat onafhankelijk toezicht van fundamenteel belang is voor de Nederlandse rechtsstaat en hebben gevraagd of de regering toezeggingen kan doen over, en zo ja hoe, zij het onafhankelijk toezicht op de hackbevoegdheid wil gaan

regelen. De leden van deze fractie hebben tevens gevraagd in hoeverre de in het wetsvoorstel opgenomen toestemming van de rechter-commissaris en controle door de Centrale Toetsingscommissie hiervoor geschikt is.

Voor het antwoord op deze vragen wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van D66, de SP en de PvdA.

De leden van de fractie van de ChristenUnie hebben gevraagd waarom niet is gekozen voor een vorm van onafhankelijk toezicht door een orgaan buiten het Ministerie van Veiligheid en Justitie. De leden van deze fractie hebben tevens gevraagd om een nadere toelichting op welke wijze het structurele toezicht op het gebruik inzichtelijk wordt gemaakt, en op welke wijze het gebruik en de effectiviteit van de inzet zal worden gemonitord.

In de eerdere beantwoording van vragen van de leden van de fracties van de SP, D66 en de PvdA is reeds ingegaan op het toezicht. De inzet van de bevoegdheid stelt hoge eisen aan de deskundigheid van de betrokken opsporingsambtenaren en vereist een zorgvuldige voorbereiding om te voorkomen dat de inzet mislukt, bijvoorbeeld doordat de verdachte op de hoogte raakt van de activiteiten van politie en justitie en vervolgens bewijsmateriaal vernietigt. De effectiviteit van de inzet zal binnen politie en openbaar ministerie dan ook worden gemonitord zodat een succesvolle inzet van deze bevoegdheid kan worden verzekerd. Verder zal de Kamer in de gelegenheid worden gesteld zich een oordeel te vormen over de inzet van deze bevoegdheid doordat, conform de werkwijze bij het aftappen en opnemen van communicatie, jaarlijks aan de Kamer zal worden gerapporteerd over de inzet van de bevoegdheid (Kamerstukken II 2007/08, 30 517, nrs. 5 en 6). Dit betreft het aantal malen dat de bevoegdheid is ingezet en het resultaat van die inzet op het gebied van de strafvervolging. Daarbij zal ook worden ingegaan op de klachten naar aanleiding van de inzet van deze bevoegdheid (Kamerstukken II 2015/16, 30 372, nr. 3, blz. 40).

9. Begroting

De leden van de fractie van het CDA hebben gevraagd of de regering kan aangeven wanneer de kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens wel en wanneer deze kosten niet worden vergoed, en of deze kosten steeds uit ’s Rijks kas behoren te worden vergoed.

De regeling van artikel 592 Sv past in het systeem dat de kosten die derden moeten maken ten behoeve van het nakomen van een vordering tot verstrekking van gegevens door derden, zoals een aanbieder van een communicatiedienst of een instelling in de financiële sector, op grond van de artikelen 126m, 126n, 126na, 126ua, 126nc tot en met 126ng en 126ni, 126t, 126u, 126uc tot en met 126ug en 126ui, en 126zg, 126zh,126zi, 126zja tot en met 126zo Sv, worden vergoed. Ditzelfde geldt voor de nakoming van een vordering tot ontsleuteling van gegevens, op grond van de artikelen 126nh, 126uh en 126zp Sv. Het gaat daarbij om kosten die verbonden zijn aan een individuele vordering of een individueel verzoek. Kosten die aan de nakoming van de vordering kunnen worden toegerekend in de vorm van extra personeelskosten en extra administratiekosten komen voor vergoeding in aanmerking, voor zover deze kosten inzichtelijk gemaakt worden. Van vergoeding zijn uitgezonderd de kosten die in het kader van de reguliere bedrijfsvoering toch al worden gemaakt.

De leden van de fractie van de ChristenUnie hebben gevraagd op welke wijze de financiële middelen verschuiven binnen het budget van de nationale politie binnen het totaal beschikbare budget. De leden van deze fractie hebben gelezen dat de mate van verschuiving afhankelijk is van de verwachtingen van en ervaring met toepassing van het instrument. Deze leden hebben gevraagd welke verwachting de regering momenteel heeft en ten laste van welke andere inzet dit wetsvoorstel dan bij de invoering zal komen. Ten slotte is gevraagd of voorzien kan worden in enkele scenario's en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel, en of voor de inzet van deze bevoegdheden extra capaciteit nodig is.

Het is de verwachting dat de nieuwe opsporingsbevoegdheid niet leidt tot structurele toename van de totale opsporingsinspanning en ook dat daarvoor, voor zover nu kan worden overzien, geen extra capaciteit nodig is. Eerder zal sprake zijn van verschuiving van het ene onderzoeksmiddel naar het andere middel. De uitvoering van het onderzoek in een geautomatiseerd werk vindt plaats bij een onderdeel van de Landelijke eenheid van de Nationale politie. De Nationale politie ontvangt jaarlijks een bijzondere bijdrage van € 13,8 miljoen voor de digitale professionalisering en vernieuwing van de organisatie onder meer ter bestrijding van cybercrime. De aanschaf en implementatie van ICT-hulpmiddelen ter voorbereiding op de invoering van het onderzoek in een geautomatiseerd werk geschiedt uit dit budget. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Aan de begroting van de politie is bij najaarsnota structureel een bedrag toegevoegd voor de aanpak van cybercrime. Voor 2017 bedraagt de bijdrage € 1,4 miljoen, voor 2018 en verdere jaren € 1,5 miljoen. Deze bijdragen zijn bedoeld voor de versterking van personele en materiële capaciteit door opleiding en ICT-middelen en tools.

De leden van de fractie van de ChristenUnie hebben gevraagd op welke wijze de extra voorziene structurele last voor de rechtspraak van € 500.000 wordt gedekt in de begroting van het ministerie. De leden van deze fractie misten duidelijkheid over de gevolgen van dit wetsvoorstel voor de begroting van het OM.

De rechtspraak wordt gefinancierd middels outputfinanciering. In het kader van zijn wettelijke adviestaak heeft de Raad voor de rechtspraak een inschatting gemaakt van de gevolgen van nieuwe wet- en regelgeving voor de werklast en organisatie van de rechtspraak. Indien er sprake is van een (verwachte) werklastverzwaring die groter is, kan dit worden meegenomen in de driejaarlijkse onderhandelingen tussen Raad en het Ministerie van Veiligheid en Justitie.

10. Gedelegeerde regelgeving

De leden van de fractie van de VVD hebben geconstateerd dat in een algemene maatregel van bestuur of een OM-aanwijzing toetsingscriteria worden vastgelegd met betrekking tot de opsporingshandelingen die worden verricht indien gegevens niet zijn opgeslagen in Nederland. De leden van deze fractie hebben gevraagd of deze criteria inmiddels zijn opgesteld, en zo ja, wat deze criteria zijn en wanneer de tekst naar verwachting beschikbaar komt.

Het voorliggende wetsvoorstel bevat een facultatieve grondslag om bij algemene maatregel van bestuur nadere regels te stellen over de toepassing van de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk in gevallen waarin niet bekend is waar de

gegevens zijn opgeslagen (artikel 126nba, negende lid, Sv, dat van overeenkomstige toepassing is verklaard in de artikelen 126uba/126zpa, derde lid, Sv). Vooralsnog wordt van deze mogelijkheid geen gebruik gemaakt; de uitwerking hiervan vindt plaats in een aanwijzing van het College van procureurs-generaal.

Het uitgangspunt is dat er rechtshulp wordt gevraagd als de te verrichten opsporingshandelingen betrekking hebben op gegevens die zich op het grondgebied van een andere staat bevinden. Als bekend is dat de gegevens niet in Nederland zijn opgeslagen dient dit in het bevel van de officier te worden vermeld, zodat de rechter-commissaris hierover controle kan uitoefenen.

In uitzonderlijke gevallen kan, onder strikte voorwaarden, zelfstandig worden opgetreden op basis van een zoveel mogelijk stapsgewijze aanpak. In het algemeen zal worden gestart met een beperkte eerste vordering, het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker. Als verdergaande handelingen nodig zijn, zal waar mogelijk worden volstaan met het overnemen van de opgeslagen gegevens zodat de beschikkingsmacht van de rechthebbende niet wordt beperkt. Het optreden in het concrete geval zal aan de hand van criteria worden afgewogen. Deze criteria hebben betrekking op de inspanning die is vereist om de identiteit en locatie van een geautomatiseerd werk te achterhalen, de ernst van het strafbare feit, de mate van betrokkenheid van de Nederlandse rechtsorde (betrokkenheid van Nederlandse slachtoffers of de Nederlandse infrastructuur), de aard van de te verrichten opsporingshandelingen (worden gegevens alleen overgenomen of ook ontoegankelijk gemaakt) en de risico's voor het geautomatiseerde werk. Deze criteria worden uitgewerkt in een OM-Aanwijzing, die in voorbereiding is en voor inwerkingtreding van het wetsvoorstel gereed zal zijn.

De leden van de fractie van het CDA hebben opgemerkt dat het op afstand binnendringen in een geautomatiseerd werk niet alleen mag bij een misdrijf waarop een gevangenisstraf van vier jaar of meer gesteld is, maar ook bij misdrijven die bij algemene maatregel van bestuur worden aangewezen. Dat lijkt de leden van de CDA-fractie ongewenst; zonder tussenkomst van de Staten-Generaal kan de regering hierdoor in beginsel ieder misdrijf via een algemene maatregel van bestuur onder de werking van dit wetsvoorstel brengen. De leden van deze fractie hebben gevraagd waarop juist deze misdrijven worden gekozen en op basis van welke criteria er wordt besloten om eventueel misdrijven toe te voegen. In de optiek van de leden van deze fractie dient een dergelijke algemene maatregel van bestuur ten minste te worden voorgehangen. Deze leden hebben tevens gevraagd of de regering bereid is om een reparatiewetsvoorstel in te dienen, waarin dit wordt geregeld.

Om in een geautomatiseerd werk binnen te kunnen dringen en onderzoek te doen met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker en de vastlegging daarvan, met het oog op het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie en met het oog op stelselmatige observatie, moet sprake zijn van een verdenking van een misdrijf als omschreven in artikel 67, eerste lid, Sv, waarvoor een bevel tot voorlopige hechtenis kan worden gegeven. Een bevel tot voorlopige hechtenis kan worden gegeven in geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld of in geval van verdenking van één van de misdrijven, genoemd in artikel 67, eerste lid, onder b en c, Sv, met een lagere wettelijke strafbedreiging.

De voorwaarden voor toepassing van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en doen van onderzoek met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens zijn strikter: in beginsel mag de bevoegdheid met het oog op deze doelen uitsluitend worden toegepast bij een verdenking van een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld. Bij algemene maatregel van bestuur kunnen echter andere misdrijven met een lagere wettelijke strafbedreiging worden aangewezen (artikelen 126nba/126uba/126zpa, eerste lid, onder c, Sv). Deze misdrijven worden aangewezen in het eerdergenoemde Besluit onderzoek in een geautomatiseerd werk. De criteria voor aanwijzing zijn de volgende. Het betreft misdrijven die worden gepleegd met een geautomatiseerd werk (computercriminaliteit in enge zin) en ernstige commune misdrijven die in toenemende mate digitaal worden gepleegd (gedigitaliseerde criminaliteit) waarbij vaak geen ander aanknopingspunt is voor de opsporing dan via het geautomatiseerde werk met behulp waarvan het misdrijf wordt gepleegd. Voorts moet sprake zijn van een duidelijk maatschappelijk belang bij de beëindiging van de strafbare situatie en de vervolging van de daders. Met uitzondering van de computerdelicten in enge zin gaat het bij de aangewezen misdrijven grotendeels om misdrijven met een strafmaximum van zes jaren gevangenisstraf.

De ontwikkelingen in de cybercriminaliteit gaan snel en de maatschappelijke gevolgen hiervan kunnen groot zijn. Door de aanwijzing van misdrijven bij algemene maatregel van bestuur kan hierop flexibel worden ingespeeld. Indien zich in de toekomst nieuwe vormen van computercriminaliteit en/of ernstige gedigitaliseerde criminaliteit voordoen die voldoen aan voornoemde criteria, kan via wijziging van het Besluit onderzoek in een geautomatiseerd werk de toepassing van de bevoegdheid met het oog op het vastleggen van gegevens of het ontoegankelijk maken van gegevens worden uitgebreid tot deze misdrijven.

De regering ziet geen aanleiding tot het indienen van een reparatiewetsvoorstel om voorhang van de algemene maatregel van bestuur te regelen en wijst erop dat reeds op andere wijze in de betrokkenheid van het parlement wordt voorzien. Bij de plenaire behandeling van het wetsvoorstel in de Tweede Kamer is toegezegd dat de algemene maatregel van bestuur voorafgaand aan de inwerkingtreding van het wetsvoorstel naar de Kamer wordt gestuurd. Deze toezegging is gestand gedaan bij de eerdergenoemde brief van 10 mei 2017, waarin beide Kamers zijn geïnformeerd over het conceptbesluit onderzoek in een geautomatiseerd werk (Kamerstukken II 2016/17, 34 372, nr. 26).

De leden van de fractie van het CDA hebben gevraagd of de regering met deze leden van mening is dat een eventuele uitbreiding van het wetsvoorstel met andere misdrijven in het geheel niet bij algemene maatregel van bestuur geregeld kan worden, maar bij wet moeten worden vastgelegd.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van deze fractie.

De leden van de fractie van de PvdA hebben opgemerkt dat het wetsvoorstel op verschillende plaatsen delegatiebepalingen bevat en zij hebben gevraagd of zij het goed begrijpen dat het hierbij steeds gaat om het Besluit technische hulpmiddelen strafvordering.

Het wetsvoorstel bevat een aantal grondslagen om bij of krachtens algemene maatregel van bestuur regels te stellen over de uitoefening van de binnendring- en onderzoeksbevoegdheid. Het betreft ten eerste de grondslag om de inzet van de bevoegdheid voor het doen van onderzoek voor bepaalde onderzoeksdoelen mogelijk te maken bij verdenking van bij algemene maatregel van bestuur aangewezen misdrijven (artikelen 126nba/126uba/126zpa, eerste lid, Sv). Het betreft ten tweede de mogelijkheid om nadere regels te stellen over de deskundigheid en autorisatie van de bij het onderzoek in een geautomatiseerd werk betrokken opsporingsambtenaren, de samenwerking met andere opsporingsambtenaren en de geautomatiseerde vastlegging van gegevens ter uitvoering van een bevel van de officier van justitie (artikel 126nba, achtste lid, onder a en b, Sv). Ten derde kunnen nadere regels gesteld worden over verschillende aspecten met betrekking tot het doen van onderzoek met behulp van een technisch hulpmiddel (artikel 126ee Sv). Omwille van de overzichtelijkheid vindt de uitvoering van deze bepalingen plaats in een nieuw besluit, het eerdergenoemde Besluit onderzoek in een geautomatiseerd werk. Net als het Besluit technische hulpmiddelen strafvordering zal dit besluit gebaseerd zijn op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, integer en herleidbaar dienen te zijn.

De leden van de fractie van de PvdA hebben gevraagd op welke termijn de tekst van de lagere regelgeving (waaronder in ieder geval voornoemd Besluit) beschikbaar zal zijn, of er een voorhangprocedure zal plaatsvinden en of de desbetreffende regelgeving ter internetconsultatie zal worden aangeboden.

Hiervoor is, in antwoord op een soortgelijke vraag van de leden van de fractie van het CDA, aangegeven dat bij de eerdergenoemde brief van 10 mei 2017 aan beide Kamers is toegezonden het conceptbesluit onderzoek in een geautomatiseerd werk. Het conceptbesluit is inmiddels ook voor internetconsultatie aangeboden door middel van plaatsing op de website www.internetconsultatie.nl.

11. Internationale aspecten

De leden van de fractie van de VVD hebben gevraagd naar het tijdpad voor de paraplu-afspraken met andere staten waarbij Nederlandse opsporingsambtenaren toegang krijgen tot geautomatiseerde werken die zich buiten Nederland bevinden of buitenlandse opsporingsambtenaren zich onbedoeld op een Nederlandse server of net bevinden. De leden van deze fractie hebben tevens gevraagd of de regering binnen een termijn van één jaar de Kamer kan informeren over de voortgang van deze paraplu-afspraken en de inhoud daarvan. Deze leden hebben voorts gevraagd of de regering hen kan informeren over de stand van zaken en ontwikkelingen om te komen tot internationale regels met het oog op de bestrijding van internationale computercriminaliteit, en of de regering van plan om in dezen initiatieven te ontwikkelen, mede met het oog op de belangrijke positie die Nederland inneemt op het terrein van de handhaving van de internationale rechtsorde.

Zoals in de eerdere beantwoording van vragen van de leden van de fracties van GroenLinks en de ChristenUnie in paragraaf 3 is aangegeven, bestaat er behoefte aan internationale afspraken inzake het vergaren van bewijs (E-evidence) vanwege het open internationale karakter van het internet. Op de Global Conference on CyberSpace in 2015 is dit onderwerp geagendeerd, vervolgens zijn cybersecurity en de aanpak van cybercrime als prioriteiten benoemd tijdens het Nederlandse EU-voor-

zitterschap en zijn in juni 2016 door de JBZ-Ministers Raadsconclusies aangenomen over criminal justice in cyberspace. Deze conclusies zien op:
– het ontwikkelen van een gezamenlijk EU-kader voor verzoeken aan private partijen voor het verkrijgen van bepaalde typen data. Hierbij wordt gestreefd naar synergie met de formulieren en instrumenten die binnen de Europese Unie voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn;
– het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp en wederzijdse erkenning binnen de Europese Unie en met derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, alsook het vergroten van kennis en vaardigheden van hen die in de lidstaten deze verzoeken behandelen;
– het herijken van de afspraken ten aanzien van handhavende rechtsmacht door te bezien welke onderzoekshandelingen onder welke voorwaarden mogen worden ingezet in cyberspace in de gevallen waarin het huidige kader nog niet voorziet, onder andere wanneer de locatie van elektronisch bewijs of de oorsprong van een cyber aanval (nog) niet bekend of redelijkerwijs niet bekend te maken is.

In vervolg op de Raadsconclusies wordt onder regie van de Commissie, in nauwe samenwerking met lidstaten en met andere zowel nationale als Europese instituties, uitvoering gegeven aan de in de Raadsconclusies genoemde actiepunten. In de Raadsconclusies wordt de Commissie verzocht over de resultaten van het proces inzake handhavende rechtsmacht te rapporteren aan de JBZ-raad in juni 2017.

Er wordt binnen de Raad voor Europa ook gesproken over een additioneel protocol bij het Cybercrimeverdrag uit 2001(Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18 en Trb. 2004, 290). Dit verdrag heeft tot nog toe het meest ruime toepassingsbereik en bevat bepalingen over geharmoniseerde strafbaarstellingen, strafprocessuele bevoegdheden (zoals bevriezing van gegevens) en internationale samenwerking. Op dit moment hebben 52 landen dit verdrag geratificeerd (de landen die lid zijn van de Raad van Europa, met uitzondering van Rusland, en landen zoals VS, Canada, Australië, Japan, Sri Lanka, Paraquay, de Dominicaanse republiek en Senegal). Als model law zijn elementen van het verdrag gebruikt in ongeveer 60 andere landen. Op 16 september 2016 heeft de Cloud Evidence Group, een subgroep van het comité van verdragspartijen van het Cybercrimeverdrag, zijn eindrapport uitgebracht. Het eindrapport bevat diverse aanbevelingen voor het versterken van de mogelijkheden voor toegang tot digitaal bewijs in de cloud ten behoeve van strafrechtelijke handhaving. Eén van de aanbevelingen betreft het voorbereiden van een concept voor een additioneel protocol bij het verdrag. Tijdens de bijeenkomst van het comité van verdragspartijen op 14 en 15 november 2016 heeft het comité bij consensus besloten dat er in beginsel een noodzaak is voor een additioneel protocol. Ten behoeve van een formeel besluit van het comité om een conceptprotocol op te stellen bij de volgende bijeenkomst van het comité in juni 2017, is de Cloud Evidence Group verzocht Terms of Reference voor een dergelijk proces uit te werken. Deze Terms of Reference worden in juni verwacht. Op het verdere verloop van de discussie over dit onderwerp kan echter niet worden vooruit gelopen.

De leden van de fractie van GroenLinks hebben gevraagd hoe het wetsvoorstel zich verhoudt tot de huidige regels op het gebied van internationale samenwerking ten aanzien van cybercriminaliteit. Tevens hebben de leden van deze fractie gevraagd wanneer er precies gebruik gemaakt kan worden van de voorgestelde grensoverschrijdende

bevoegdheid en of het gebruikelijke rechtshulpverzoek niet volstaat voor dit soort gevallen.

Het wetsvoorstel brengt geen verandering in de bestaande regels voor de internationale samenwerking. Een belangrijke bron voor dergelijke regels ten aanzien van cybercriminaliteit wordt gevormd door het eerdergenoemde Cybercrimeverdrag. Met de Wet computercriminaliteit II is dit verdrag in de Nederlandse wetgeving geïmplementeerd. Ter uitvoering van dit verdrag zijn een aantal gedragingen in de Nederlandse wetgeving strafbaar gesteld, zoals de wederrechtelijke toegang tot computersystemen, de wederrechtelijke onderschepping van computergegevens en de verstoring van computersystemen. Tevens zijn de bevoegdheden van politie en justitie op basis van de Nederlandse wetgeving aangepast, zoals die inzake de tijdelijke «bevriezing» van bepaalde opgeslagen gegevens, het doorzoeken van computers en computergegevens en de verstrekking van verkeersgegevens. Deze regels worden op geen enkele wijze door dit wetsvoorstel aangetast.
De voorgestelde bevoegdheid dient om op afstand heimelijk binnen te kunnen dringen in een geautomatiseerd werk. Internet is niet gebonden aan de landsgrenzen; bij de uitvoering van de bevoegdheid zullen dan ook geautomatiseerde werken kunnen worden benaderd die zich in het buitenland bevinden. Zoals in de memorie van toelichting en de nota naar aanleiding van het verslag uiteen is gezet, is een rechtshulpverzoek aangewezen als blijkt dat gegevens zich op het territorium van een andere staat bevinden (Kamerstukken II 2016/17, 34 372, nr. 3, par. 2.8.3. en nr. 6, blz. 94/95). Diverse landen, waaronder Nederland zelf, hebben ten behoeve van de snelle afhandeling van rechtshulp in cybercrimezaken een 24/7 contactpunt ingericht. Wanneer gegevens in de Cloud zijn opgeslagen of het internetgedrag van personen is gericht op het niet kunnen achterhalen van een geografische plaats (bijv. het gebruik anonimiseringssoftware zoals TOR) dan bestaat er geen wetenschap van de locatie van de herkomst of opslag van gegevens. Er kan dan geen rechtshulpverzoek aan een ander land worden gericht. Vooralsnog kunnen die gegevens ook binnen Nederland worden opgeslagen en verwerkt. Onder omstandigheden kan dit betekenen dat op afstand heimelijk wordt binnengedrongen in een geautomatiseerd werk bijvoorbeeld een server, met het oog op het verrichten van bepaalde onderzoekshandelingen waarvan niet bekend is of gegevens worden opgeslagen en verwerkt in Nederland of daarbuiten. Als wetenschap bestaat dat de gegevens niet in Nederland zijn opgeslagen dan moet dat in het bevel worden vermeld, zodat het aspect van de inbreuk op de soevereiniteit van een andere staat onderwerp vormt van een expliciete afweging van de officier van justitie en de rechter-commissaris. Indien in het verdere verloop van het onderzoek duidelijkheid ontstaat over de feitelijke locatie van de gegevens en die locatie in een andere land is dan wordt zo snel mogelijk alsnog een rechtshulpverzoek gedaan en aan de bevoegde buitenlandse autoriteiten verantwoording afgelegd over het handelen en de daaraan ten grondslag liggende afwegingen.

De leden van de fractie van GroenLinks hebben gevraagd hoe de onderhandelingen in EU-verband en in de Raad van Europa over een helder grensoverschrijdend juridisch kader verlopen.

Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de fractie van de VVD.

12. Overige

De leden van de fractie van de VVD hebben gevraagd hoe en waar gegevens worden opgeslagen die beschikbaar komen in het kader van het binnendringen in een geautomatiseerd werk op grond van de wet.

Gedurende het opsporingsonderzoek in het kader waarvan onderzoek wordt verricht in een geautomatiseerd werk, is er sprake van een strikte taakverdeling en functiescheiding. De uitvoering van een bevel tot onderzoek in een geautomatiseerd werk is voorbehouden aan daartoe aangewezen opsporingsambtenaren van een technisch team, vanwege hun specialistische kennis en vaardigheden op het terrein van informatie- en communicatietechnologie. Binnen de Landelijke eenheid van de Nationale politie worden één of meer technische teams ingericht. De gegevens die tijdens het onderzoek in een geautomatiseerd werk met een technisch hulpmiddel zijn geregistreerd, worden automatisch vastgelegd op een technische voorziening bij het betreffende technische team. De vastgelegde gegevens zijn uitsluitend toegankelijk voor door de korpschef aangewezen ambtenaren. De technische infrastructuur is beveiligd tegen wijziging van de vastgelegde gegevens en tegen kennisneming door onbevoegden. Op basis van het bevel worden de vastgelegde gegevens door het technische team beschikbaar gesteld aan het tactische team dat is belast met het operationele onderzoek. De beschikbaar gestelde gegevens worden door het tactische team opgeslagen ten behoeve van het onderzoek.

De leden van de fractie van de VVD hebben gevraagd op welke wijze daarbij een onderscheid wordt gemaakt tussen gegevens die nodig zijn voor de vaststelling van ernstige strafbare feiten en zogenoemde bijvangst. De leden van deze fractie hebben verder gevraagd of de gegevens die als bijvangst gelden worden vernietigd, en zo ja, wanneer en hoe, en zo nee, op welke juridische grondslag de bijvangst wordt opgeslagen.

Hierboven is opgemerkt dat de resultaten van het onderzoek door het technische team ter beschikking worden gesteld aan het tactische team. Zo nodig kan het technische team op basis van technische criteria zorgdragen voor voorafgaande filtering van de onderzoeksgegevens, zodat binnen de categorieën van gegevens die in het bevel van de officier zijn opgenomen uitsluitend de gegevens die van belang zijn voor het opsporingsonderzoek ter beschikking komen van het tactische team. De verzamelde gegevens vallen onder een gedifferentieerd regime wat betreft de bewaartermijnen. De processen-verbaal en andere voorwerpen waaraan gegevens kunnen worden ontleend die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie en het aftappen en opnemen van communicatie worden door de officier van justitie, voor zover die niet bij de processtukken zijn gevoegd, ter beschikking gehouden van het onderzoek (artikel 126cc, eerste lid, Sv). Zodra twee maanden zijn verstreken nadat de zaak is geëindigd en de notificatie, bedoeld in artikel 126bb Sv is verricht, doet de officier van justitie de processen-verbaal en andere voorwerpen vernietigen. De procedure is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken.

De gegevens die zijn verkregen door de toepassing van de bevoegdheid met het oog op andere onderzoekshandelingen vallen onder het regime van de Wet politiegegevens. Afhankelijk van het specifieke doel van de verwerking kan de bewaartermijn verschillen. Doorgaans zullen de gegevens moeten worden verwijderd zodra deze niet langer noodzakelijk

zijn voor het doel van het onderzoek, of gedurende een periode van maximaal een half jaar bewaard teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek. Na afloop van deze termijn worden de gegevens verwijderd (artikel 9, vierde lid, Wpg). De verwijderde politiegegevens worden gedurende een termijn van vijf jaren bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen, en vervolgens gearchiveerd of vernietigd (artikel 14 Wpg).

De leden van de fractie van de VVD hebben gevraagd of bijvangst van fiscale aard wordt doorgestuurd naar de Belastingdienst. De leden van deze fractie hebben tevens gevraagd op grond van welke nationale en internationale rechtsregels, uitspraken en arresten, daaronder begrepen van internationale gerechtshoven, fiscale gegevens die kwalificeren als bijvangst dienen te worden doorgespeeld naar de Belastingdienst eventueel naar de Belastingdienst van een andere staat bijvoorbeeld onder de toepassing van een EU-verordening, verdrag of overeenkomst tot fiscale gegevensuitwisseling.

Het openbaar ministerie heeft de verantwoordelijkheid om een effectieve bijdrage te leveren aan een rechtvaardige en veilige samenleving. Het verstrekken van strafvorderlijke informatie aan anderen – binnen de geldende wettelijke kaders – kan daartoe een belangrijke bijdrage leveren. De Wet justitiële en strafvorderlijke gegevens biedt een wettelijke grondslag voor de verstrekking van strafvorderlijke gegevens aan personen of instanties voor buiten de strafrechtspleging gelegen doeleinden (artikel 37f Wjsg). Het verstrekken van strafvorderlijke gegevens is alleen mogelijk als het past binnen de taakuitoefening van het openbaar ministerie en voor zover dit noodzakelijk is wegens een zwaarwegend algemeen belang. Daarbij doet niet terzake op grond van welke specifieke opsporingsbevoegdheid de gegevens zijn verkregen; als de gegevens onderdeel vormen van het strafdossier dan kunnen deze op grond van de wet aan andere personen of instanties worden verstrekt. Het beleid terzake is uitgewerkt in de Aanwijzing verstrekking van strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden (Aanwijzing wet justitiële en strafvorderlijke gegevens; Stcrt. 2013, 32596).In voorkomende gevallen kunnen de gegevens uit het stafdossier ook aan de Belastingdienst worden verstrekt (Aanwijzing Wet justitiële en strafvorderlijke gegevens, punt 3, onder c). Wanneer een zaak is geëindigd met een sepot of een vrijspraak of wanneer nog geen definitieve vervolgingsbeslissing is genomen, geldt als uitgangspunt dat geen informatie wordt verstrekt tenzij er sprake is van een zwaarwegend belang dat de verstrekking in dat geval rechtvaardigt.

De leden van de fractie van de VVD hebben opgemerkt dat wanneer er bij de provider/aanbieder en de officier van justitie verschil van inzicht bestaat over het ontoegankelijk maken van gegevens in een geautomatiseerd werk, er een formele procedure in gang wordt gezet die mogelijk veel tijd in beslag kan nemen. De leden van deze fractie hebben gevraagd op welke manier wordt gewaarborgd dat deze procedurele route zo spoedig mogelijk verloopt, juist met het oog op de potentiële dreiging die met deze informatie verbonden kan zijn wanneer de informatie voor derden beschikbaar blijft op het net.

Een bevel van de officier van justitie aan de aanbieder tot het ontoegankelijk maken van gegevens betreft een ingrijpende beslissing omdat grondrechten van burgers, zoals de vrijheid van meningsuiting, hierbij kunnen zijn betrokken. Daarom is een voorafgaande rechterlijke toetsing vereist. Gekozen is voor een schriftelijke machtiging van de rechter-commissaris wegens het niet voldoen aan een ambtelijk bevel of het

plegen van of deelnemen aan een strafbaar feit in verband met het verspreiden van de desbetreffende gegevens. De officier van justitie behoeft daarvoor niet te wachten op een definitieve beslissing van de rechter naar aanleiding van de ingestelde strafvervolging. Het zou dan enkele maanden of langer kunnen duren voordat er een definitieve uitspraak van de rechter is. De regeling is echter voorzien van de nodige waarborgen voor een zorgvuldige toepassing. Zo dient de rechter-commissaris de aanbieder in de gelegenheid te stellen te worden gehoord. Vanwege de mogelijk verstrekkende consequenties van een bevel tot ontoegankelijkmaking van gegevens staat voor de belanghebbende, waaronder degene tot wie het bevel is gericht, de mogelijkheid open van beklag bij de raadkamer van de rechtbank op grond van de bestaande beklagregeling voor inbeslaggenomen voorwerpen (artikel 552a Sv). Vanwege het spoedeisende karakter van de beslissing beslist de rechtbank zo spoedig mogelijk. Deze procedure kan binnen een kort tijdsbestek worden doorlopen. De regering is van mening dat hiermee een goed evenwicht is gevonden tussen de betrokken belangen.

De leden van de fractie van het CDA hebben opgemerkt dat de bewoordingen van de aanleiding tot het mogen binnendringen in een geautomatiseerd werk in de verschillende wetsartikelen verschillend worden omschreven en hebben gevraagd of de regering de logica van de verschillende formuleringen kan uitleggen. Verder hebben de leden van deze fractie gevraagd of men in het ene geval eerder mag binnendringen dan in het andere geval en zo ja, wat de verschillen zijn en waarom deze zijn gemaakt.

De bewoordingen van de aanleiding tot het mogen binnendringen in een geautomatiseerd werk zijn in de verschillende wetsartikelen verschillend omschreven vanwege de verschillende verdenkingscriteria die van toepassing zijn. Dit onderscheid vloeit voort uit de systematiek van de Wet bijzondere opsporingsbevoegdheden waarmee (onder meer) Titel IVA van het Eerste Boek van het Wetboek van Strafvordering is gewijzigd. De Wet bijzondere opsporingsbevoegdheden vormt een apart regime voor het onderzoek naar georganiseerde criminaliteit (Kamerstukken II 1996/97, 25 403, nr. 2). Later is, met Titel VB, een afzonderlijk regime ingevoegd voor de opsporing van terroristische misdrijven (Kamerstukken II 2004/05, 30 164, nr. 2).

De voorgestelde bevoegdheid vertoont inhoudelijk overeenkomsten met de bijzondere opsporingsbevoegdheden van Titel IVA van het Eerste Boek van het Wetboek van Strafvordering en wordt – net als de in die titel genoemde bevoegdheden – heimelijk toegepast zonder dat de betrokkene daar weet van heeft. Daarom is gekozen voor plaatsing in die titel. Het is van belang dat de bevoegdheid van het onderzoek in een geautomatiseerd werk ook kan worden toegepast bij het onderzoek naar de georganiseerde criminaliteit en terroristische misdrijven. Daarom wordt voorgesteld deze bevoegdheid tevens op te nemen in de desbetreffende titels van het Eerste Boek.

In titel IVA is als criterium voor de toepassing van de opsporingsbevoegdheden opgenomen de verdenking van een misdrijf. In titel V van het Eerste Boek is als verdenkingscriterium opgenomen: een redelijk vermoeden op grond van feiten of omstandigheden dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid, Sv worden beraamd of gepleegd die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren. Bij enkele in titel V geregelde bevoegdheden, namelijk het aftappen en opnemen van communicatie en het opnemen van vertrouwelijke communicatie, is de

kring van personen beperkt tot personen ten aanzien van wie een redelijk vermoeden bestaat dat zij betrokken zijn bij het in georganiseerd verband beramen of plegen van ernstige misdrijven. Zij behoeven geen verdachte te zijn in de zin van artikel 27 Sv, maar zij dienen wel een meer dan toevallige betrokkenheid te hebben bij het criminele handelen van de groepering, die bijvoorbeeld blijkt uit meer dan incidentele contacten met de criminele organisatie of haar leden. In Titel VB van het Eerste Boek is voor de opsporingsbevoegdheden als verdenkingscriterium opgenomen: aanwijzingen van een terroristisch misdrijf. Van aanwijzingen is sprake indien de beschikbare informatie feiten en omstandigheden bevat die erop duiden dat daadwerkelijk een terroristisch misdrijf zou zijn of zal worden gepleegd. Anders dan bij de opsporing op basis van Titel IV is bij terroristische misdrijven niet vereist een «redelijk vermoeden» van een strafbaar feit, aanwijzingen zijn voldoende.

De leden van de fractie van het CDA hebben gewezen op het gestelde in artikel II, onder X, onder punt 9 van het wetsvoorstel, op grond waarvan het gerecht het bevel kan opheffen als het de klacht gegrond acht. Volgens de leden van deze fractie zou hier geen sprake moeten zijn van «kunnen» maar van «moeten». De leden van deze fractie hebben gevraagd aan welke gevallen de regering denkt waarbij – ondanks de gegrondheid van het beklag – het bevel toch niet zou moeten of mogen worden opgeheven.

In het voorliggende wetsvoorstel wordt voorgesteld de regeling over het beklag tegen inbeslagneming, in artikel 552a Sv, uit te breiden met de mogelijkheid dat belanghebbenden zich kunnen beklagen over een bevel tot het ontoegankelijk maken van gegevens, bedoeld in artikel 125p Sv. Als het gerecht het beklag gegrond acht dan kan het gerecht het bevel geheel of gedeeltelijk opheffen. Niet uitgesloten is dat het gerecht het beklag van een belanghebbende gegrond acht omdat het belang van de belanghebbende om over de gegevens te kunnen beschikken prevaleert boven het belang van de officier van justitie om de gegevens ontoegankelijk te houden, in afwachting van een definitieve beslissing van de rechtbank, op grond van artikel 354 of artikel 552fa Sv. Daarbij kan het gerecht termen aanwezig zien om de ontoegankelijkmaking van de gegevens overigens te handhaven. Dit kan aan de orde zijn als het gaat om kinderpornografisch materiaal en de ouders of hulpverleners kennis willen nemen van de beelden om hulp of ondersteuning te kunnen bieden aan het slachtoffer. De rechter heeft dan de keuze tussen gehele of gedeeltelijke opheffing van de ontoegankelijkmaking van de gegevens.

De leden van de fractie van de SP wilden graag weten wat artikel 125p Sv extra beoogt in vergelijking tot artikel 54a Sr, omdat ook met dit laatste artikel kon worden bevolen websites met bijvoorbeeld materiaal van seksueel misbruik van kinderen offline te halen. Zij hebben gevraagd of de regering kan uitleggen waarom artikel 125p Sv nodig is.

Met het voorgestelde artikel 125p Sv wordt een afzonderlijke en zelfstandige bevoegdheid voor de officier van justitie geïntroduceerd om bij verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegestaan een tussenpersoon te bevelen terstond alle maatregelen te nemen die redelijkerwijs gevergd kunnen worden om gegevens ontoegankelijk te maken. De regeling is bedoeld als aanvulling op de bestaande vrijwillige Notice and take down (NTD) gedragscode, die zich richt op tussenpersonen die in Nederland een openbare telecommunicatiedienst op het internet leveren. De bevoegdheid is van belang in gevallen waarin de tussenpersoon niet bereid is op basis van de gedragscode de gegevens ontoegankelijk te maken, bijvoorbeeld als de officier van justitie en de tussenpersoon van mening verschillen of de vrijheid van meningsuiting in het geding is. Daarnaast kan het bevel ook worden gericht aan tussenper-

sonen die de gedragscode niet hebben ondertekend, waarbij te denken valt aan hosting providers en beheerders van een website.

De leden van de fractie van de SP hebben begrepen dat content die offline is gehaald binnen afzienbare tijd weer online kan komen. De leden van deze fractie hebben gevraagd of zinsnede «[...] of nieuwe strafbare feiten te voorkomen» in artikel 125p, tweede lid, onder b, van het wetsvoorstel suggereert dat een internetserviceprovider die het materiaal offline heeft gehaald aansprakelijk is als het materiaal daarna opnieuw op internet verschijnt.

Op grond van het voorgestelde artikel 125p, eerste lid, Sv dient de aanbieder van een communicatiedienst alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens ontoegankelijk te maken ter beëindiging van een strafbaar feit of ter voorkoming van strafbare feiten. In bepaalde gevallen is het technisch niet goed mogelijk om de gegevens effectief ontoegankelijk te maken, bijvoorbeeld als gegevens op de een of andere manier zijn gedupliceerd en ook nog op andere gegevensdragers staan. De verplichting tot het ontoegankelijk maken is, evenals in het huidige artikel 54a Sr het geval is, geclausuleerd. In het voorgestelde artikel 125p, derde lid, Sv wordt artikel 125o, tweede en derde lid, Sv van overeenkomstige toepassing verklaard. Daarmee wordt onder het ontoegankelijk maken van gegevens hetzelfde verstaan als in artikel 125o, tweede lid, Sv, te weten: het treffen van maatregelen ter voorkoming dat de beheerder van een geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. De ontoegankelijkmaking van de gegevens kan plaatsvinden door de desbetreffende gegevens te verwijderen, dan wel de toegang daartoe te blokkeren. Blokkering kan aan de orde zijn als de gegevens niet kunnen worden verwijderd, zodat de gegevens voor de gebruikers niet raadpleegbaar zijn. Om aan het bevel tot ontoegankelijkmaking te voldoen dient de blokkering voort te duren zolang de gegevens worden aangeboden. Dit laat de situatie onverlet dat dezelfde gegevens op een andere plaats op het internet toegankelijk worden of nog blijken te zijn, omdat ze bijvoorbeeld in eerdere instantie zijn gedupliceerd (in de techniek aangeduid als «mirror»). Voor een dergelijke toegankelijkheid kan de provider niet verantwoordelijk worden gehouden, tenzij de provider hiervan expliciet op de hoogte is. Op grond van artikel 54a Sr blijft vervolging van een tussenpersoon die een communicatiedienst aanbiedt bij een strafbaar feit dat met gebruikmaking van die dienst wordt begaan, achterwege als de tussenpersoon voldoet aan een bevel als bedoeld in artikel 125p Sv.

De leden van de fractie van de ChristenUnie hebben gevraagd om een reflectie op het feit dat Nederland bovenmatig vaak gebruik maakt van telefoon- en gegevenstaps, mede in het licht van de uitwerking op de veiligheid voor Nederlandse burgers vergeleken met andere EU-burgers. De leden van deze fractie hebben tevens gevraagd welke verwachting de regering heeft van het gebruik van de voorgestelde bevoegdheid en of deze zich zal ontwikkelen tot een ultimum remedium of juist tot een gangbaar gebruikte opsporingsbevoegdheid.

Enkele jaren geleden is door het WODC een onderzoek verricht om een beter zicht te verkrijgen op het feitelijke gebruik van de telefoon- en internettap bij de opsporing en vervolging in strafzaken, mede in het licht van de wijze waarop dat in enkele ons omringende landen gebeurt. Dit onderzoek beoogde een beeld te geven van de wettelijke kaders en het gebruik van de telefoon- en internettap in de opsporing in Nederland en enkele ons omringende landen, te weten Engeland en Wales, Zweden en

Duitsland. In het rapport getiteld «Het gebruik van de telefoon- en internettap in de opsporing», dat bij brief van 23 mei 2012 aan uw Kamer is aangeboden (Kamerstukken II, 2011/12, 30 517, nr. 25) wordt vastgesteld dat het heersende beeld is dat er in Nederland veel wordt getapt. Het aantal taps op vaste lijnen is in Nederland al jaren stabiel, maar de opkomst van de mobiele telefoon heeft geresulteerd in een flinke toename van het aantal taps. Hierbij passen enkele belangrijke kanttekeningen. In de eerste plaats blijkt uit de cijfers van het rapport dat het aantal taps slechts een klein percentage betreft van het totale aantal telefoonaansluitingen in Nederland. De toename van het aantal telefoontaps vanaf 1998 is toe te schrijven aan de opkomst van de mobiele telefonie. Daar het aantal taps op vaste lijnen ongeveer gelijk is gebleven, kan hieruit worden opgemaakt dat het aantal telefoontaps het stijgende aantal mobiele telefoons op de voet is gevolgd (blz. 81). Ook in Duitsland is een dergelijke ontwikkeling kenbaar, in het rapport wordt melding gemaakt van een stijging van het aantal tapbevelen in dat land van 6.391 tot 39.200 in de periode van 1998 tot en met 2007. Dit betreft een toename van ruim 600% (blz. 242). In de tweede plaats worden door de verdachten/gebruikers dikwijls meerdere nummers gebruikt. Om verdachten telefonisch toch te kunnen blijven volgen, moet dan steeds een nieuw tapbevel worden aangevraagd. In het rapport wordt melding gemaakt van meerdere nummers per verdachte, in dat kader wordt melding gemaakt van een zaak waarbij bij iemand thuis 150 verschillende telefoons en 380 SIM-kaarten zijn gevonden; op grond van de huidige regeling zijn dan in ieder geval 380 verschillende tapbevelen en machtigingen vereist (blz. 129). Ook uit de Engelse tapstatistieken kan worden afgeleid dat personen frequent wisselen van toestel en van nummer, aangezien het aantal tussentijdse mutaties van de lopende bevelen veel groter is dan het aantal tapbevelen (blz. 259). De onderzoekers geven aan dat overwogen zou kunnen worden om over te stappen naar een tapbevel dat gekoppeld is aan een persoon in plaats van aan een telefoonnummer of telefoontoestel, een werkwijze die ook in een aantal onderzochte landen wordt gebezigd. In de derde plaats wordt in andere landen gekozen voor de inzet van verderstrekkende bevoegdheden. Op dit punt zijn er verschillen in de keuzes die worden gemaakt. Volgens de onderzoekers is dit voor een groot deel te verklaren door het feit dat er tussen de onderzochte landen een verschil van perceptie bestaat als het gaat om de zwaarte van de verschillende opsporingsmiddelen, zoals infiltratie door undercoveragenten.

De onderzoekers concluderen dat een vergelijking van cijfers over de inzet van taps in de onderzochte landen niet één op één is te maken. Taps worden in andere landen anders geregistreerd en de rechtsstelsels verschillen van elkaar. In het algemeen kan worden geconcludeerd dat de telefoontap in Nederland frequenter wordt ingezet dan in de andere onderzochte landen. Daar staat tegenover dat in Nederland op nummer wordt getapt, niet op de persoon, waardoor het aantal taps aanzienlijk hoger is dan het aantal personen van wie de communicatie wordt afgetapt, en dat andere bijzondere opsporingsmiddelen, mede vanwege het verhoogde risico voor de betrokken opsporingsambtenaren, juist minder vaak worden ingezet dan in het buitenland.

De regering verwacht niet dat de voorgestelde bevoegdheid zich zal ontwikkelen tot een gangbaar gebruikte opsporingsbevoegdheid. Daarvoor zijn verschillende redenen. In de eerste plaats gelden er strikte wettelijke voorwaarden voor de inzet van deze bevoegdheid. Dit betreft onder meer het criterium van het dringende opsporingsbelang en een voorafgaande machtiging van de rechter-commissaris. Bij de toetsing van de voorgenomen inzet door in eerste instantie de officier van justitie en vervolgens de rechter-commissaris, vormt de invulling van het criterium

van het dringende opsporingsbelang, aan de hand van een beoordeling van de proportionaliteit en subsidiariteit, een essentieel bestanddeel. Indien er andere, minder ingrijpende middelen zijn waarmee het doel bereikt kan worden en het onderzoek het toelaat (denk hierbij aan gevaarzetting en risico's bij het te laat kunnen ingrijpen), zoals het vorderen van gegevens bij dienstverleners, het plaatsen van een tap, het doen van een doorzoeking, inbeslagneming of een bevriezingsbevel, zal eerst daarvoor moeten worden gekozen. In de tweede plaats betreft dit een specialistische techniek, waarvoor grote deskundigheid op het gebied van informatie- en communicatietechnologie is vereist. Toepassing is voorbehouden aan de daartoe speciaal aangewezen opsporingsambtenaren die over deze expertise beschikken en die deel uitmaken van een speciaal team, het technische team, dat organisatorisch is gescheiden van het tactische team dat is belast met het tactische opsporingsonderzoek en dat kan worden belast met de uitvoering van een bevel van de officier van justitie tot het op afstand binnendringen van een geautomatiseerd werk. In de derde plaats betreft dit een bevoegdheid waarvan de inzet een zorgvuldige voorbereiding vergt vanwege mogelijke beveiligingsmaatregelen rond het geautomatiseerde werk en de noodzaak om heimelijk te opereren. Voorkomen moet worden dat de betrokkene er van op de hoogte raakt dat opsporingsambtenaren op afstand zijn binnengedrongen in het geautomatiseerde werk dat bij hem in gebruik is en maatregelen treft om het opsporingsonderzoek te frustreren. Ieder geautomatiseerd werk is vanuit technisch oogpunt echter anders en dit betekent dat de methode voor het binnendringen nauwkeurig moet worden afgestemd op het geautomatiseerde werk in kwestie. De noodzaak van een zorgvuldige voorbereiding komt eveneens tot uitdrukking in de procedure die voorschrijft dat de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie, die het College van procureurs-generaal adviseert over de voorgenomen inzet van een aantal bijzondere opsporingsmethoden. In het licht van deze omstandigheden ligt een al te gemakkelijke inzet van deze bevoegdheid bepaald niet voor de hand.

De leden van de fractie van de ChristenUnie hebben voorts gevraagd hoe de leeftijdsgrenzen in de voorgestelde artikelen 248a Sr en 248e Sr zich verhouden tot de leeftijdsgrens van 21 jaar in het wetsvoorstel regulering prostitutie en bestrijding misstanden seksbranche.

De in de zedenwetgeving en het wetsvoorstel regulering prostitutie en bestrijding misstanden seksbranche (Wrp) gestelde leeftijdsgrenzen dienen beschouwd te worden in het licht van de door deze wetgeving beschermde belangen. De zedenwetgeving beschermt kinderen tegen inbreuken op hun lichamelijke en seksuele integriteit en doorkruising van hun seksuele ontwikkeling door het plegen van ontucht met een kind strafbaar te stellen. Er zijn verschillende niveaus van strafrechtelijke bescherming al naar gelang de leeftijd van een kind. De grens voor seksuele meerderjarigheid is in beginsel op zestien jaren gesteld. Ontucht met een kind beneden de leeftijd van zestien jaren is strafbaar. In artikel 248e Sr, waarin grooming strafbaar is gesteld, wordt aangesloten bij deze leeftijdsgrens. In bepaalde omstandigheden strekt de strafrechtelijke bescherming tegen ontucht zich uit tot de leeftijd van achttien jaren. Dit is het geval in artikel 248a Sr, waarin kinderen tot en met de leeftijd van achttien jaren beschermd worden tegen seksuele verleiding.

Prostitutie is een legale beroepsactiviteit. Aan de in de Wrp opgenomen minimumleeftijd van 21 jaren voor de uitoefening van prostitutiewerkzaamheden ligt de doelstelling ten grondslag om jeugdige personen buiten de prostitutie te houden. Aangenomen wordt dat personen op de leeftijd van 21 jaren meer levenservaring hebben, weerbaarder zijn en de tijd hebben gehad om als volwassene na te denken over de zwaarte en

risico's van het prostitutievak. Ook is er een grotere kans dat personen op deze leeftijd een vervolgopleiding hebben gevolgd waarmee kennis en vaardigheden zijn opgedaan waardoor er een mogelijk alternatief voor sekswerk aanwezig is.

De leden van de fractie van de ChristenUnie hebben tevens gevraagd met welke reden in het voorgestelde artikel 248a Sr wordt gekozen voor een objectivering van de leeftijdsaanduiding.

Het huidige artikel 248a Sr dat verleiding van een minderjarige strafbaar stelt, bevat de bestanddelen «persoon waarvan hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van achttien jaren nog niet heeft bereikt». Het gaat hier om zogenaamde subjectieve bestanddelen: er is opzet dan wel schuld ten aanzien van de leeftijd van de minderjarige vereist. Uit de jurisprudentie kan worden afgeleid dat dit delictsbestanddeel aan een veroordeling wegens artikel 248a Sr in de weg staat indien de verdachte iemand die zich als minderjarige voordoet verleidt tot ontucht. Hierdoor is de opsporing van dit strafbare feit met behulp van een lokpuber niet mogelijk.

Het wetsvoorstel breidt de strafrechtelijke aansprakelijkheid uit tot verleiding van iemand die zich voordoet als een persoon die de leeftijd van achttien jaren nog niet heeft bereikt. Het is niet goed denkbaar dat een verdachte weet dan wel redelijkerwijs dient te vermoeden dat hij met iemand die zich voordoet als een minderjarige te maken heeft. Daarom is het schuldverband ten aanzien de leeftijd geschrapt. Voor gedragingen waarbij iemand daadwerkelijk een minderjarige verleidt wordt

evenmin opzet of schuld op de leeftijd vereist. Het gebruik van geobjectiveerde leeftijden komt vaker voor in de zedentitel, bijvoorbeeld in artikel 247 Sr waarin het plegen van ontucht met een persoon beneden de leeftijd van zestien jaren strafbaar is gesteld.

De leden van de fractie van de ChristenUnie hebben ook gevraagd of de nieuwe invulling van artikel 248a Sr gevolgen heeft voor de interpretatie van de daaropvolgende artikelen en in het bijzonder artikel 248b Sr. De leden van deze fractie hebben tevens gevraagd of «ontucht plegen» in dit artikel door het voorgestelde artikel 248a Sr in het vervolg ook met een webcam of ander technisch hulpmiddel kan plaatsvinden.

In zowel het huidige artikel 248a Sr als het voorgestelde artikel 248a Sr wordt het opzettelijk bewegen van een minderjarige tot het plegen van ontuchtige handelingen strafbaar gesteld. Handelingen die op afstand via een webcam worden verricht kunnen ook nu al een strafbare gedraging opleveren. Het openbaar ministerie gebruikt artikel 248a Sr regelmatig voor de opsporing en vervolging van digitale kinderlokkers die online kinderen aanzetten tot het zich naakt te tonen voor een webcam of tot het verrichten van seksuele handelingen. Doordat de inzet van de lokpuber op dit moment niet mogelijk is vindt de opsporing van deze strafbare feiten vaak achteraf plaats, als het leed al is geschied. Vaak gaat het om verdachten die zoveel mogelijk kinderen tegelijk benaderen en veel schade aanrichten. In verschillende zaken hebben veroordelingen plaatsgevonden (recent: Rechtbank Amsterdam, 16 maart 2017, ECLI:NL:RBAMS:2017:1627).

Het plegen van ontucht *met* iemand is in artikel 248a Sr geen voorwaarde voor strafrechtelijke aansprakelijkheid; in een aantal andere artikelen in de zedentitel, waaronder het door de leden van de fractie van de ChristenUnie genoemde artikel 248b Sr, wordt dit wel vereist. In het WODC-onderzoek «Herziening van de zedendelicten» is het systematische

vraagstuk in hoeverre voor «ontucht plegen *met*» fysiek contact nodig is aan de orde gesteld. Op dit moment wordt een wetsvoorstel tot modernisering van de zedentitel van het Wetboek van Strafrecht voorbereid. Doel is onder meer om digitaal gepleegde zedenmisdrijven een duidelijke plaats te geven in het wettelijke kader.

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