Tweede Kamer der Staten-Generaal

2

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)

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 8 november 2016

I. ALGEMEEN DEEL

1. Inleiding

Met veel belangstelling heb ik kennis genomen van de vragen van de vaste commissie voor Veiligheid en Justitie, belast met het voorbereidend onderzoek van het voorstel van wet computercriminaliteit III. Dit betreft een wetsvoorstel dat van groot belang is voor de opsporing en vervolging van cybercrime. De leden van de verschillende fracties hebben een groot aantal vragen gesteld over de verschillende onderdelen van dit wetsvoorstel.
Hieronder wordt nader ingegaan op de gestelde vragen. Daarbij wordt, ten behoeve van het overzicht, soms verwezen naar de beantwoording van soortgelijke vragen van andere fracties. Ik hoop met deze nota naar aanleiding van het verslag de onduidelijkheden en vragen die rond dit wetsvoorstel bij de fracties van Uw Kamer leven, naar genoegen te beantwoorden.

De leden van de SP-fractie hebben kennisgenomen van de inhoud van onderhavig wetsvoorstel en hebben hierover veel kritische vragen en opmerkingen. Zij zijn allereerst nog steeds niet voldoende overtuigd van de noodzaak van dit wetsvoorstel, vooral vanwege de vergaande inbreuk op de grondrechten. De leden van deze fractie hebben gevraagd in hoeverre de nieuwe bevoegdheid om heimelijk een geautomatiseerd werk binnen te dringen in het leven wordt geroepen omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is of omdat er echt misdrijven onopgelost blijven door het ontbreken van een dergelijke bevoegdheid. Deze leden hebben tevens gevraagd of ook onderzocht is of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is.
De noodzaak van de nieuwe bevoegdheid ligt in de voortschrijdende techniek en het wijdverbreide gebruik van geautomatiseerde werken voor communicatie en de verwerking en opslag van gegevens. Daardoor wordt het voor de opsporing steeds lastiger om aanknopingspunten te vinden

kst-34372-6
ISSN 0921 - 7371
's-Gravenhage 2016

voor de inzet van bestaande wettelijke bevoegdheden. De huidige bevoegdheden rond de inbeslagneming van geautomatiseerde werken zijn gekoppeld aan de plaats waar het geautomatiseerde werk zich fysiek bevindt. De ontwikkeling van het internet maakt het echter eenvoudig om vanuit een onbekende fysieke locatie met behulp van een geautomatiseerd werk strafbare feiten te plegen jegens personen of objecten die zich in Nederland bevinden. Daarbij kan de locatie van het werk en de betrokkenheid van bepaalde personen eenvoudig worden verhuld door het gebruik van een draadloos netwerk, van de diensten van een buitenlandse aanbieder of van encryptie of andere versleutelings- en anonimiseringstechnieken. Daardoor wordt het voor de opsporing in toenemende mate lastig of zelfs onmogelijk om strafbare gedragingen, die worden gepleegd met behulp van geautomatiseerde werken te koppelen aan bepaalde locaties en/of personen. Dit belemmert de inzet van traditionele opsporingsbevoegdheden, zoals het aftappen van telecommunicatie, het vorderen van gegevens bij aanbieders en het vragen van rechtshulp aan andere landen. In dergelijke gevallen kan het op afstand binnendringen in het geautomatiseerde werk uitkomst bieden. Deze bevoegdheid wordt niet voorgesteld omdat andere methoden tijdrovender zijn en hacken nu eenmaal makkelijker is maar omdat er misdrijven onopgelost blijven door het ontbreken van een bevoegdheden waarmee daders effectief kunnen worden opgespoord.
Bij de voorbereiding van dit voorstel is uiteraard onderzocht in hoeverre er minder vergaande mogelijkheden beschikbaar zijn waarbij de privacy beter is gewaarborgd. Hiervoor kan worden verwezen naar de memorie van toelichting. Geconcludeerd is dat de bestaande bevoegdheden te kort schieten omdat deze ofwel zijn gekoppeld aan een bepaalde fysieke plaats ofwel niet zijn gericht op de toegang tot elektronische gegevens die zich in een geautomatiseerd werk of op een gegevensdrager elders bevinden. Dit komt hieronder, naar aanleiding van soortgelijke vragen van de leden van andere fracties, nader aan de orde.

De leden van de CDA-fractie hebben met belangstelling kennis genomen van voorliggend wetsvoorstel. De leden van deze fractie constateerden dat politie en justitie achter de feiten aanlopen voor wat betreft de bestrijding van digitale criminaliteit en merkten op dat deze analyse wordt gedeeld door zowel voor- als tegenstanders van onderhavig wetsvoorstel. De leden van deze fractie achtten een spoedige inwerkingtreding van dit wetsvoorstel gewenst en hebben gevraagd of de regering deze mening deelt. Tevens hebben deze leden gevraagd waarom dit zo lang geduurd heeft, ook na de aankondiging van het Actieplan Jihadisme in augustus 2014, en vernamen hierop graag een reactie.
De regering deelt de mening van de CDA-fractie dat een spoedige inwerkingtreding van dit wetsvoorstel gewenst is. Het wetsvoorstel bevat verschillende onderdelen die van groot belang zijn voor de opsporing en vervolging van ernstige misdrijven. Dit betreft niet alleen opneming van nieuwe bevoegdheden in het Wetboek van Strafvordering, zoals het op afstand binnendringen van een geautomatiseerd werk, maar ook de aanpassing van bestaande strafbaarstellingen, zoals de strafbaarstelling van grooming, zodat de opsporing en vervolging meer armslag krijgen bij de bestrijding van vormen van computercriminaliteit die de samenleving ernstig bedreigen. De regering spant zich daarom in om de vragen in dit verslag zorgvuldig maar ook met enige voortvarendheid te beantwoorden. De beantwoording heeft echter langer geduurd dan voorzien omdat door de verschillende fracties een groot aantal vragen is gesteld over zowel juridische als technische aspecten rond het wetsvoorstel, die de nodige afstemming hebben vereist met de betrokken partijen om te komen tot een uitgebreide en zorgvuldige beantwoording daarvan.

De leden van de CDA-fractie hebben gevraagd of de regering de mening deelt dat met onderhavig wetsvoorstel niet de privacy van burgers onder druk komt te staan maar dat het juist bijdraagt aan een nog zorgvuldiger optreden dan thans het geval is omdat door digitaal speurwerk kan worden voorkomen dat klassieke opsporingsmethodes als huiszoeking en inbeslagneming van apparatuur moet worden ingezet.
De regering is zich bewust van de mogelijke impact van dit wetsvoorstel op de privacy van burgers. De regering is met de CDA-fractie van mening dat de inzet van de bevoegdheid kan leiden tot een kleinere inbreuk op de persoonlijke levenssfeer van verdachten. De bevoegdheid kan zeer gericht worden ingezet. Een huiszoeking en inbeslagneming kan inderdaad in bepaalde gevallen achterwege blijven als de nodige gegevens middels het binnendringen in een geautomatiseerd werk kunnen worden vergaard. Dit betreft specifiek de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk. In haar advies heeft de Afdeling advisering van de Raad van State erop gewezen dat het heimelijk binnendringen in een geautomatiseerd werk een grote inbreuk op de persoonlijke levenssfeer vormt, die vergelijkbaar is met het betreden van een woning met het oog op het opnemen van vertrouwelijke communicatie (artikel 126l, tweede lid, Sv). Met de Afdeling advisering is de regering van oordeel dat het op afstand, binnendringen en onderzoeken van een geautomatiseerd (net)werk, waarbij zowel historische, actuele als toekomstige gegevens kunnen worden overgenomen, een ingrijpende aantasting van de persoonlijke levenssfeer vormt. Voor een zorgvuldige afweging van de betrokken belangen moeten enkele belangrijke noties worden erkend. De eerste is dat de ontwikkeling van de computercriminaliteit noodzaakt tot aanpassing van de bevoegdheden om die criminaliteit effectief te bestrijden. De huidige opsporingsbevoegdheden zijn niet voldoende om antwoord te kunnen geven op de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. De communicatie tussen mensen en de opslag van gegevens verloopt steeds vaker via internet. Internet is grenzeloos. Gegevens zijn vaak niet meer opgeslagen op een computer van de gebruiker zelf die zich op een bepaalde plaats bevindt en aldaar in beslag kan worden genomen, maar op servers die zich al dan niet in Nederland bevinden en die met het internet zijn verbonden en waarvan de fysieke locatie ook bij de gebruiker niet bekend hoeft te zijn. Hierdoor wordt de opsporing met verschillende problemen geconfronteerd. De opslag van gegevens in de cloud heeft tot gevolg dat de gegevens, behalve door tussenkomst van (het geautomatiseerde werk van) de betrokken persoon, uitsluitend via een aanbieder van een communicatiedienst of een communicatienetwerk kunnen worden bereikt. In de praktijk blijkt dit echter weerbarstig omdat de aanbieder in het buitenland is gevestigd is, en soms zelfs onmogelijk wanneer de aanbieder niet te achterhalen is of de gegevens zijn versleuteld. Door het toenemende gebruik van versleuteling van gegevens in informatiesystemen en software worden bestaande opsporingsbevoegdheden, zoals het aftappen van communicatie, ineffectief. De enige mogelijkheid om de communicatie in toegankelijke vorm af te tappen is door direct vanaf het ontvangende of verzendende apparaat te tappen, voordat versleuteling plaatsvindt. In de memorie van toelichting is hierop reeds nader ingegaan.
In de tweede plaats wordt voorzien in strikte waarborgen voor een zorgvuldige toepassing van de voorgestelde bevoegdheden. Een belangrijke waarborg vormt een voorafgaande rechterlijke toetsing van de voorgenomen inzet. Verder zijn de voorwaarden voor de uitoefening van de bevoegdheid aangescherpt, overeenkomstig het advies van de Afdeling advisering van de Raad van State. Het destijds voorgestelde artikel 125ja Sv is inmiddels, als artikel 126nba/uba/zpa Sv, verplaatst naar Titel IVA dat betrekking heeft op de bijzondere bevoegdheden tot opsporing. Overeenkomstig het advies van de Afdeling advisering is de toepassing van onderzoekshandelingen waarbij het geautomatiseerde

werk op afstand wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens, uitsluitend toegestaan ingeval van een misdrijf 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. Ten slotte moet voor de beoordeling van de impact van de voorgestelde maatregel ook de huidige situatie in ogenschouw worden genomen. Het Wetboek van Strafvordering bevat thans verschillende regels voor de inbeslagneming van voorwerpen en de vastlegging van (elektronische) gegevens. Zoals eerder opgemerkt, zijn deze bevoegdheden in de digitale wereld minder bruikbaar omdat de fysieke locatie van de gegevens minder goed te achterhalen is. Niettemin moet worden opgemerkt dat in de gevallen waarin bekend is dat de gegevens zich in Nederland bevinden, de computer of server in beslag kan worden genomen waarop die gegevens zijn opgeslagen. De doorzoeking ter vastlegging van gegevens dan wel de inbeslagneming van een voorwerp als een computer of server, inclusief alle gegevens die op dat geautomatiseerde werk zijn opgeslagen, vormt eveneens een ingrijpende inbreuk op de persoonlijke levenssfeer van de betrokkenen.

De leden van de CDA-fractie hebben gevraagd waarom de regering er niet voor gekozen heeft het toepassingsbereik van de bestaande bevoegdheid tot het ontoegankelijk maken van gegevens te verruimen ex artikel 54a van het Wetboek van Strafrecht. Zij hebben tevens gevraagd of dit politie en justitie niet enorm zou helpen in de opsporingspraktijk en in het voorkomen van nieuwe strafbare feiten. Verder hebben zij gevraagd of deze keuze is overlegd met politie en justitie en wat hun wensen op dit punt waren, en of de regering kan aangeven hoe wetstechnisch een verruiming op dit punt zou kunnen worden vorm gegeven.
Het bestaande artikel 54a Sr blijkt in de praktijk niet goed te functioneren omdat deze bepaling zowel een vervolgingsuitsluitingsgrond bevat voor een tussenpersoon die een telecommunicatiedienst verleent als een bevoegdheid voor de officier van justitie tot het geven van een bevel tot het ontoegankelijk maken van gegevens. De combinatie van een vervolgingsuitsluitingsgrond en een bevelsbevoegdheid compliceert de toepassing van de regeling. In dit wetsvoorstel wordt daarom voorgesteld om de regeling aan te passen en te voorzien in een afzonderlijk bevoegdheid in het Wetboek van Strafvordering tot het vorderen van de ontoegankelijkmaking van gegevens. 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. Het College van procureurs-generaal heeft in het advies over het eerdere conceptwetsvoorstel gesteld dat de NTD-gedragscode goed functioneert en dat een afzonderlijke bevelsbevoegdheid voor de officier van justitie niet nodig is. In het advies over het voorliggende wetsvoorstel heeft het College evenwel aangegeven dat er enkele internetproviders zijn die de gedragscode niet ondersteunen. Het College van procureurs-generaal is van oordeel dat het voorliggende voorstel in deze tijd en onder deze omstandigheden in een behoefte voorziet. Desondanks heeft het College gewaarschuwd voor de ontwikkeling van een rol voor het openbaar Ministerie van een censurerende internetpolitie en heeft geadviseerd de bevoegdheid tot het geven van een bevel tot het ontoegankelijk maken van gegevens op het internet te beperken tot de gevallen waarin sprake is van verdenking van een ernstig strafbaar feit, waarvoor voorlopige hechtenis mogelijk is. Ook de Nederlandse Orde van Advocaten (NOvA) heeft gewaarschuwd voor toepassing in bagatelgevallen. Vanuit wetstechnisch oogpunt zou een verruiming op dit punt kunnen worden vorm gegeven door de beperking tot ernstige strafbare feiten te schrappen.

Gelet op het voorafgaande ziet de regering daartoe echter geen aanleiding.

De leden van de CDA-fractie hebben gevraagd waarom de regering de voorgestelde bevoegdheden van het geven van een mondelinge vordering van verkeersgegevens en terzake van NAW-gegevens heeft geschrapt.
De desbetreffende bevoegdheden zijn niet geschrapt maar overgeheveld naar het conceptwetsvoorstel voor een bewaarplicht voor telecommunicatiegegevens (dataretentie). Hiervoor is gekozen omdat laatstgenoemd wetsvoorstel voorziet in aanpassing van de bevoegdheid tot het vorderen van verkeersgegevens; het ligt daarom in de rede om deze aanpassing bij dat wetsvoorstel te betrekken.

De leden van de CDA-fractie hebben gevraagd waarom de regering de voorwaarde voor de inzet van de bevoegdheid tot het binnendringen in een geautomatiseerd werk heeft aangescherpt, zodat de lat nu zeer hoog is gelegd, en welke misdrijven nu niet meer onder de reikwijdte van deze bevoegdheden vallen in vergelijking met het conceptwetsvoorstel.
De Afdeling advisering heeft erop gewezen dat de inbreuk op de persoonlijke levenssfeer op basis van het destijds voorgestelde artikel 125ja Sv – inmiddels gewijzigd in artikel 126nba/uba/zpa Sv – kan verschillen, afhankelijk van de onderzoekshandeling die wordt verricht. Naar aanleiding van dit advies heeft de regering de voorwaarden voor de uitoefening van de bevoegdheid aangescherpt voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijkmaken van gegevens. Voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk op afstand wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens 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 strafbaar feit dat bij algemene maatregel van bestuur is aangewezen. De strafbare feiten die bij algemene maatregel van bestuur worden aangewezen betreffen die ernstige strafbare feiten waarop weliswaar een vrijheidsstraf van minder dan acht jaar is gesteld maar die naar hun aard worden gepleegd met behulp van een geautomatiseerd werk – het gebruik van een geautomatiseerd werk is dan instrumenteel voor het plegen van het delict – waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders, en de inzet van andere opsporingsbevoegdheden onvoldoende zicht op resultaat biedt. Het doorzoeken van de gegevens in het geautomatiseerde werk, teneinde deze vast te leggen of ontoegankelijk te maken, is essentieel voor het opsporen van dergelijke delicten. Dit betreft misdrijven als het gebruik van een botnet (art. 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (art. 240b Sr), de verleiding van een minderjarige tot ontucht (art. 248a Sr) de «grooming» (art. 248e Sr) of andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is.
In vergelijking met de regeling van het conceptwetsvoorstel is de kring van misdrijven, ten aanzien waarvan de onderzoekshandelingen van het vastleggen of ontoegankelijk maken van gegevens mogelijk is, dus beperkt. Dit is hierboven toegelicht.

De leden van de CDA-fractie hebben gevraagd wat de gevolgen zijn voor de administratieve lasten bij de opsporingsdiensten, nu de voorgestelde bevoegdheid tot het binnendringen is geplaatst in Titel IVA van het Wetboek van Strafvordering. Verder hebben deze leden gevraagd aan

welke voorwaarden extra moet worden voldaan in vergelijking met de oorspronkelijk gemaakte keuze voor Titel IV.
De plaatsing van de voorgestelde bevoegdheid tot het binnendringen in titel IVA van het Wetboek van Strafvordering heeft nauwelijks consequenties voor de administratieve lasten bij de opsporingsdiensten. Wel is de notificatieplicht ruimer. Op grond van Titel IV is deze van toepassing op de verdachte en op de verantwoordelijke voor de gegevens. Door de huidige plaatsing Titel IVA van het wetboek is de notificatieplicht van toepassing op de persoon ten aanzien van wie de bevoegdheid is uitgeoefend. Verder is de regeling van het wettelijk verschoningsrecht anders vorm gegeven vanwege het specifieke karakter van de bijzondere opsporingsbevoegdheden. Op grond van Titel IV geldt een verbod op het onderzoek naar gegevens die zijn ingevoerd door of vanwege een verschoningsgerechtigde, behoudens met hun instemming (art. 125l Sv). Op grond van Titel IVA geldt een verplichting tot vernietiging van gegevens die mededelingen bevatten gedaan door of aan een verschoningsrechtigde (art. 126aa, tweede lid, Sv). De voorwaarden waaraan moet worden voldaan zijn gelijk gebleven. Wel zijn de mogelijkheden van toepassing van de bevoegdheid uitgebreid. Deze is niet beperkt tot het geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten maar ook mogelijk indien uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven, waarvoor voorlopige hechtenis is toegelaten, 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 (art. 126o Sv) en in geval van aanwijzingen van een terroristisch misdrijf (art. 126zd e.v. Sv).

De leden van de CDA-fractie hebben gevraagd waarom de regering extra drempels heeft opgeworpen door middel van de toets van de rechter-commissaris bij het inzetten van bevoegdheden, zoals het ontoegankelijk maken van gegevens. Verder hebben zij gevraagd wat de schrapping van de zelfstandige bevelsbevoegdheid van de officier van justitie betekent voor de effectiviteit van de opsporing van nieuwe strafbare feiten.
In het toenmalige conceptwetsvoorstel versterking bestrijding computercriminaliteit was een herziening opgenomen van de regeling van de vervolgingsuitsluitingsgrond voor een internetprovider, die geen wetenschap heeft van het feit dat met behulp van zijn dienst strafbare feiten worden begaan of die, zodra hij daarvan kennis draagt, onverwijld alle maatregelen treft die van hem kunnen worden gevergd om de gegevens betreffende dit feit ontoegankelijk te maken (art. 54a Sr). De herziening voorzag onder meer in schrapping van het vereiste van een voorafgaande machtiging van de rechter-commissaris voor de afgifte van een bevel tot het ontoegankelijk maken van gegevens.
Tijdens de consultatie hebben verschillende instanties aangedrongen op handhaving van de voorafgaande machtiging van de rechter-commissaris. Het is niet uitgesloten dat het bevel tot het ontoegankelijk maken van gegevens ook bij uitingsdelicten zoals haatzaaien en bedreiging, wordt gegeven. Van een uitingsdelict is geen sprake indien de uiting op grond van het recht op een vrije meningsuiting is toegelaten. Verschillende adviesorganen, waaronder de Raad voor de rechtspraak, hebben erop gewezen dat het in het belang van een goede rechtsbescherming, in het bijzonder van het recht op vrije meningsuiting, gewenst is dat de voorafgaande toetsing door de rechter wordt gehandhaafd. Dat belang is van dien aard en het ingrijpende karakter van de maatregel zo groot dat is geadviseerd de bevoegdheid tot het uitvaardigen van een bevel bij de rechter-commissaris te beleggen. Hierbij is tevens gewezen op de uitspraak van het EHRM in de zaak Sanoma tegen Nederland van 14 september 2910 (EHRM 14/09/2010, zaaknr. 38224/03, Sanoma/Nederland). De Raad voor de rechtspraak wijst in het bijzonder op hetgeen

het EHRM opmerkt over de positie van de officier van justitie («can hardly be seen as objective and impartial») en over de noodzaak van een preventieve toets door de rechter en de ontoereikendheid van een toetsing achteraf (op grond van art. 552a Sv).
Op grond van deze inbreng heeft de toenmalige Minister van Veiligheid en Justitie besloten het vereiste van de voorafgaande machtiging van de rechter-commissaris te handhaven. Ik onderschrijf deze keuze. Gelet op de belangen die bij een bevel tot ontoegankelijkmaking in het geding zijn, ligt het in de rede om een voorafgaande rechterlijke machtiging te vereisen. Een rechter-commissaris is bij uitstek in staat om een onpartijdige en zorgvuldige afweging tussen de verschillende belangen te maken.

De leden van de CDA-fractie hebben gevraagd waarom de regering de dwangsom uit het wetsvoorstel heeft gehaald wanneer niet is voldaan aan het bevel om gegevens ontoegankelijk te maken. Zij hebben tevens gevraagd wat dit betekent voor de afbreuk van de effectiviteit van dit bevel in de praktijk.
In het toenmalige conceptwetsvoorstel versterking bestrijding computercriminaliteit was voorzien in de mogelijkheid om de vordering tot ontoegankelijkmaking van gegevens, in gevallen waarin daartoe aanleiding bestond, kracht bij te zetten door middel van het opleggen van een last onder dwangsom. Deze diende als «stok achter de deur» in geval snelle ontoegankelijkmaking van gegevens ter voorkoming of beëindiging van strafbare feiten noodzakelijk zou zijn.
In het advies over het toenmalige conceptwetsvoorstel heeft het College van procureurs-generaal aangegeven geen voorstander te zijn van het introduceren van een last onder dwangsom in het Wetboek van Strafvordering. Het College meende dat deze bevoegdheid niet bij een incidenteel onderwerp in het Wetboek van Strafvordering moest worden geïntroduceerd maar dat het vanwege de vele onzekerheden, waarbij de verwevenheid met het bestuursrecht onmiddellijk in het oog sprong, aanbeveling verdiende eerst in kaart te brengen voor welke strafvorderlijke doeleinden deze bevoegdheid een aanwinst zou kunnen zijn, wat de gevolgen zouden zijn in termen van toenemende werklast en vervolgens te bestuderen op welke wijze deze bevoegdheid integraal zou kunnen worden ingericht. Hierdoor moest worden voorkomen dat de mogelijkheid tot het opleggen van een last onder dwangsom tot gevolg zou hebben dat de grens tussen het bestuursrecht en het strafrecht zou vervagen en dat het openbaar ministerie bij de handhaving van de strafrechtelijke rechtsorde in bestuursrechtelijke procedures verwikkeld zou raken, die bovendien een nadelig effect zouden kunnen hebben op het strafvorderlijk optreden. Vanwege deze kritiek is destijds besloten de mogelijkheid van de dwangsom te schrappen. De officier van justitie kan, indien de gegevens niet ontoegankelijk worden gemaakt en hij gegronde redenen heeft om aan te nemen dat degene tot wie het bevel is gericht zich onvoldoende heeft ingespannen om de gegevens ontoegankelijk te maken, overgaan tot vervolging voor het niet voldoen aan een bevoegd gegeven ambtelijk bevel (artikel 184 Sr) dan wel voor het plegen van of deelnemen aan het strafbare feit waarop de gegevens, waarvan de ontoegankelijkmaking is bevolen, betrekking hebben.

De leden van de CDA-fractie hebben gevraagd waarom de onder 2 en 3 genoemde vorderingen uiteindelijk zijn overgeheveld naar een ander, nog niet bij de Kamer ingediend wetsvoorstel. Zij hebben tevens gevraagd of deze bevoegdheden nu op precies dezelfde wijze terugkomen als in het conceptwetsvoorstel voorgesteld en wanneer de Kamer het nog niet ingediende wetsvoorstel kan verwachten. Tenslotte hebben zij gevraagd of de regering de gemaakte keuzes heeft overlegd met politie en justitie. Voor de beantwoording van deze vraag wordt verwezen naar het antwoord op de eerdere vragen van de leden van deze fractie over het

schrappen van de voorgestelde bevoegdheden rond de mondelinge vordering van verkeersgegevens en van NAW-gegevens. In aanvulling op die beantwoording kan worden opgemerkt dat de voorgestelde bevoegdheden materieel op dezelfde wijze terug komen als in het voorliggende wetsvoorstel. Het wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens is inmiddels bij Uw Kamer ingediend (Kamerstukken II 2015/16, 34 537, nr. 2). Het openbaar ministerie heeft gepleit voor de overheveling van deze voorstellen naar het wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens, met instemming van de politie. Op grond van de bovenbeschreven overwegingen heb ik besloten aan dit verzoek gehoor te geven.

De leden van D66-fractie hebben met evenveel verbazing als verontrusting kennis genomen van het onderhavige wetsvoorstel, waarbij gebruik gemaakt wordt van fouten in software. De leden van deze fractie vonden het teleurstellend dat de door mij tijdens het Algemeen Overleg over cybersecurity toegezegde brief over het gebruik van technische kwetsbaarheden niet aan de Kamer is gestuurd voor de inbrengdatum voor dit verslag, waardoor een aantal belangrijke vragen over de toepassing niet op voorhand zijn verduidelijkt. De leden van deze fractie hebben gevraagd om gelijktijdig met deze nota naar aanleiding van het verslag de door mij tijdens het Algemeen Overleg over cybersecurity, gehouden op 20 januari 2016, toegezegde brief over het gebruik van kwetsbaarheden aan de Kamer te doen toekomen.
Tegelijk met deze nota naar aanleiding van het verslag ontvangen de leden van uw Kamer de door mij toegezegde brief over het gebruik van kwetsbaarheden. Hiermee wordt tegemoet gekomen aan het verzoek van de leden van deze fractie.
De leden van de D66-fractie constateerden dat de Kamer drie jaar heeft moeten wachten op dit wetsvoorstel en hebben gevraagd of de regering kan toelichten waarom er tussen de consultatie en het toesturen aan de Kamer zoveel tijd heeft gezeten.
Voor de antwoord op deze vraag wordt verwezen naar de beantwoording van een eerdere, soortgelijke vraag van de leden van de CDA-fractie.

De leden de D66-fractie hebben gevraagd in hoeverre dit wetsvoorstel gevolgen kan hebben voor de bestrijding van terrorisme. Ook hebben zij gevraagd wat de reden is dat de regering dit wetsvoorstel, in tegenstelling tot de consultatielancering drie jaar geleden, nu als een antiterrorisme maatregel neerzet en of de regering de mening deelt dat dit wetsvoorstel voornamelijk gericht is op de traditionele criminaliteit, waarbij de daders gebruik maken van digitale communicatiemiddelen.
Ook voor de bestrijding van terroristische misdrijven waarbij gebruik wordt gemaakt van een geautomatiseerd werk, is de voorgestelde bevoegdheid van groot belang. Terroristen maken steeds vaker gebruik van het internet, zowel voor communicatiedoeleinden als ten behoeve van het plegen van strafbare feiten. Voor de opsporing en vervolging van terrorisme is de toegang tot deze informatie dan ook van groot belang. De verhoogde dreiging van terroristische aanslagen in Europa maakt toegang tot deze informatie nog klemmender. In het kader van de aanpak van terrorisme kan daarnaast de voorgestelde wijziging van artikel 54a Sr, waarin voorzien wordt in een specifieke bevelsbevoegdheid voor de officier van justitie, bijvoorbeeld heel behulpzaam zijn omdat dit de procedure tot verwijdering van strafbare uitingen van het internet verbetert, zoals haatzaaiende uitingen of oproepen tot de gewapende jihad, door de aanbieders van telecommunicatiediensten. Daarnaast ziet de regering voor de in dit wetsvoorstel voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk een bredere toepassing dan enkel traditionele criminaliteit waarbij de daders gebruik maken van digitale communicatiemiddelen.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten op grond waarvan is besloten om de bevoegdheid tot een mondelinge vordering van bepaalde gegevens over te hevelen naar het wetsvoorstel voor een bewaarplicht voor telecommunicatiegegevens. Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van een eerdere, soortgelijke vraag van de leden van de CDA-fractie.

De leden van de D66-fractie hebben de regering gevraagd in te gaan op de tegenstrijdigheid van de beleidskeuze om cybercriminelen te bestrijden door de kwetsbaarheden, die zij gebruiken om hun criminelen activiteiten te ontplooien, niet proberen te dichten maar juist open te houden en zelf te misbruiken.
Tegelijk met deze nota naar aanleiding van het verslag ontvangen de leden van Uw Kamer de door mij toegezegde brief over het gebruik van kwetsbaarheden. Voor het antwoord op de vraag van deze leden verwijs ik naar deze brief. Uitgangspunt is dat een kwetsbaarheid of lek in de beveiliging van software, dat door politie en justitie wordt aangetroffen, wordt gemeld bij de leverancier met het oog op het beëindigen of dichten daarvan.

De leden van de D66-fractie hebben de regering gevraagd in te gaan op de mogelijke situatie dat de Nederlandse regering de nu nog schimmige markt in onbekende kwetsbaarheden, zogeheten «zero days», legitimeert en stimuleert door software te kopen van bijvoorbeeld een HackingTeam. Deze leden hebben tevens gevraagd of de regering het mogelijk acht dat hackers door de legitimering van de markt in «zero days» eerder geneigd zullen zijn om «zero days» te verkopen aan HackingTeam-achtige bedrijven of overheden.
Voor het antwoord op deze vragen verwijs ik naar de eerdergenoemde brief over het gebruik van kwetsbaarheden.

De leden van de D66-fractie constateerden dat het wetsvoorstel in consultatie is gegeven aan tal van relevante belanghebbenden en vroegen waarom niet is gekozen voor bedrijven of belangenorganisaties van bedrijven.
Het wetsvoorstel voorziet in de aanpassing en uitbreiding van strafvorderlijke bevoegdheden met het oog op de bestrijding van computercriminaliteit. Deze bevoegdheden hebben in de eerste plaats gevolgen voor de opsporingsdiensten en de rechterlijke macht. Deze bevoegdheden hebben in de tweede plaats gevolgen voor de instanties die betrokken zijn bij de bescherming van de persoonlijke levenssfeer. Ten slotte zijn de voorgestelde strafvorderlijke bevoegdheden relevant voor de burgers en bedrijven. Met name om deze derde groep betrokkenen de mogelijkheid te geven om te reageren is aanvullend gekozen voor een internetconsultatie. Op deze wijze zijn bedrijven en belangenorganisaties van bedrijven in staat gesteld hun zienswijze kenbaar te maken. De regering stelt met voldoening vast dat in ruime mate van deze gelegenheid gebruik is gemaakt. De internetconsultatie heeft ruim 50 reacties opgeleverd, waaronder reacties van bedrijven die actief zijn op het gebied van ICT.

De leden van de D66-fractie hebben gelezen dat de versleuteling van gegevens ongedaan kan worden gemaakt. Deze leden hebben de regering gevraagd toe te lichten op wat voor manier de versleuteling ongedaan kan worden gemaakt, en of dat gebeurt door kwetsbaarheden in de encryptiesoftware te misbruiken. Ten slotte hebben zij gevraagd of de regering het met deze leden eens is dat het onwenselijk is kwetsbaarheden in encryptiesoftware te misbruiken.
De regering is doordrongen van de ernst van het belang om de veiligheid van burgers te waarborgen en de personen die deze veiligheid aantasten door middel van het beramen of plegen van strafbare feiten, op te sporen

en te vervolgen. Voor een adequate opsporing en vervolging is het van cruciaal belang dat de opsporingsdiensten toegang hebben tot gegevens en communicatie. Daartoe kan het noodzakelijk zijn dat de versleuteling van gegevens ongedaan wordt gemaakt. Het Wetboek van Strafvordering bevat reeds verplichtingen tot het verschaffen van toegang tot geautomatiseerde werken, het ontsleutelen van gegevens of het ter beschikking stellen van kennis omtrent de beveiliging (artikelen 125k en 126nh/uh Sv). Een dergelijk bevel kan niet worden gegeven aan de verdachte. Overigens omvat de verplichting om mee te werken aan het beschikbaar komen van gegevens ten behoeve van opsporing en vervolging geen verplichting om kwetsbaarheden in te bouwen met het oog op mogelijk gebruik door politie en justitie. Daarnaast realiseert de regering zich dat overheden, bedrijven en burgers zijn gebaat bij maximale veiligheid van de digitale systemen. De encryptie van gegevens kan bijdragen aan de veiligheid op internet en de bescherming van de persoonlijke levenssfeer van burgers. In verband met de ontwikkeling van encryptie is er wel nadrukkelijk behoefte aan bevoegdheden als voorgesteld in dit wetsvoorstel. Door de bevoegdheden van dit wetsvoorstel is het mogelijk om, in gevallen bij wet voorzien en op de wijze als bij wet voorgeschreven, toegang te verkrijgen tot de inhoud van versleutelde gegevens. In de brief van 4 januari 2016 over encryptie (Kamerstukken II 2015/16, 26 643, nr. 383) is aangegeven dat het op dit moment niet wenselijk is om verdergaande beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.

De leden van de D66-fractie hebben gevraagd hoe het eventueel misbruiken van fouten in software zich verhoudt tot de brief van 4 januari 2016 van de regering over encryptie, en of de regering van plan is fouten in encryptiesoftware te misbruiken om gegevens te ontsleutelen.
Voor het antwoord op deze vragen wordt verwezen naar de eerdergenoemde brief over het gebruik van kwetsbaarheden.

De leden van de D66-fractie hebben geconstateerd dat de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in zijn advies «De publieke kern van het internet» stelt dat «het geheimhouden van kwetsbaarheden er simpelweg toe leidt dat het internet onveiliger wordt» en hebben gevraagd hoe het wetsvoorstel zich verhoudt tot het aangehaalde WRR advies.
Voor het antwoord op deze vraag wordt verwezen naar de eerdergenoemde brief over het gebruik van kwetsbaarheden.

2. Onderzoek in een geautomatiseerd werk

2.1 De noodzaak van de voorgestelde bevoegdheid

De leden van de PvdA-fractie hebben gevraagd in hoeverre bij het gebruik van de nieuwe bevoegdheid niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben. Tevens hebben deze leden gevraagd hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn.
Er zijn verschillende redenen waarom de voorgestelde nieuwe bevoegdheid niet te gemakkelijk zal worden ingezet zonder dat een zorgvuldige afweging heeft plaatsgevonden, in het kader waarvan ook de mogelijkheid van minder verstrekkende bevoegdheden aan de orde komt. 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, op basis 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, waarop de voorgenomen inzet wordt voorgelegd aan de Centrale Toetsingscommissie (CTC) van het openbaar ministerie. De CTC adviseert het College van procureurs-generaal 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 PvdA-fractie hebben verder gevraagd hoe wordt gewaarborgd dat de bevoegdheid tot het doen van het op afstand en heimelijk onderzoeken in een geautomatiseerd werk het ultimum remedium is in de reeks van bestaande bevoegdheden. Deze leden hebben gevraagd of de rechter-commissaris hierin een afweging maakt, en waarom het niet uitgesloten is dat er in plaats van het op afstand heimelijk binnendringen in een geautomatiseerd werk gekozen wordt voor een van de andere opsporingsbevoegdheden. Tenslotte hebben zij gevraagd waarom niet standaard eerst wordt uitgegaan van bevoegdheden, zoals inbeslagneming van voorwerpen, stelselmatige observatie of het aftappen van communicatie.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de PvdA-fractie. Standaard zal eerst uit worden gegaan van bevoegdheden waarvoor vanuit juridisch oogpunt minder zware eisen gelden en die overigens minder voorbereiding vergen, zoals het gebruik van de internettap. Er zijn echter specifieke situaties waarin een internettap geen soelaas biedt, bijvoorbeeld omdat er gebruik wordt gemaakt van hotspots of omdat er wordt gezocht naar gegevens (bijvoorbeeld kinderpornomateriaal) die zijn opgeslagen en die niet met anderen worden uitgewisseld. De inbeslagneming van een voorwerp is afhankelijk van wetenschap bij de speurders van de vindplaats van dat voorwerp, in het licht van de technologische ontwikkeling is dit bepaald geen vanzelfsprekendheid. De

observatie van personen biedt weliswaar inzicht in de gedragingen van die personen in de openbare ruimte, maar geeft geen inzicht in hun gedragingen in afgeschermde ruimten van het internet.

De leden van de PvdA-fractie hebben gelezen dat ook bijzondere opsporingsdiensten de mogelijkheid krijgen van de nieuwe bevoegdheid gebruik te maken en hebben gevraagd of de regering kan uitleggen waarom dit nodig is. Deze leden hebben tevens gevraagd of de vormen van criminaliteit waarmee deze diensten te maken krijgen ernstig genoeg zijn om de inzet van de nieuwe bevoegdheid te rechtvaardigen, of hier sprake is van misdrijven die een ernstige inbreuk op de rechtsorde opleveren en zo ja, welke.
De bijzondere opsporingsdiensten (BOD'en) houden zich bezig met de strafrechtelijke handhaving van de rechtsorde op beleidsterreinen waarop de ministers van Economische Zaken, Landbouw en innovatie, van Financiën, van Infrastructuur en Milieu en van Sociale Zaken en Werkgelegenheid verantwoordelijkheid dragen. Dit omvat de opsporing van strafbare feiten, onder gezag van de officier van justitie. Dit betreft feiten die strafbaar zijn gesteld in bijzondere wetten, zoals de Wet op de Inkomstenbelasting en de Wet op de economische delicten, en feiten die strafbaar zijn gesteld in het commune strafrecht, zoals fraude en witwassen. Voor de opsporing van deze strafbare feiten zijn de opsporingsambtenaren van de BOD'en bevoegd bijzondere opsporingsbevoegdheden in te zetten, zoals de observatie of het aftappen van telecommunicatie. Vanwege de ontwikkelingen op het gebied van de cybercrime worden de BOD'en geconfronteerd met soortgelijke belemmeringen voor de opsporing van strafbare feiten als de reguliere politie. Om deze belemmeringen adequaat het hoofd te kunnen bieden is het van belang dat ook de opsporingsambtenaren van de BOD'en de bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk kunnen uitvoeren met het oog op de toepassing van bepaalde onderzoekshandelingen, zoals het aftappen van telecommunicatie of de observatie.
De aan te wijzen ambtenaren moeten volden aan eisen op het gebied van de deskundigheid en samenwerking. Dit wordt uitgewerkt bij algemene maatregel van bestuur. De daartoe aangewezen opsporingsambtenaren van het technische team worden beschikken over specialistische kennis op het gebied van de informatie- en communicatietechnologie. Gezien de aard van de bevoegdheid en de strafbare feiten waarvoor deze kan worden ingezet, zal naast de politie naar verwachting voornamelijk de FIOD gebruik maken van de bevoegdheid. FIOD richt zich op financiële fraude. De financiële markten zijn in grote mate doordrongen van het gebruik van het internet, en haar functioneren is hiervan in grote mate afhankelijk. Daarnaast wordt grootschalige financiële fraude steeds vaker door technisch zeer capabele criminelen gepleegd. Zij maken gebruik van de nieuwste technologische ontwikkelingen en zijn soms voorlopers als het gaat om de ontwikkelingen van nieuwe innovatieve hackmethoden. Ook maken zij veelvuldig gebruik van bijvoorbeeld online handelsplaatsen op het Darknet of van alternatieve betalingsvormen zoals Bitcoin. Voor de opsporing van deze criminelen is het voor de FIOD van belang de voorgestelde bevoegdheden in te kunnen zetten, zodat zij over voldoende moderne middelen beschikt om deze criminelen te kunnen opsporen. De voorwaarden voor, en de procedurele waarborgen rond de toepassing van de bevoegdheid, zoals die in dit wetsvoorstel zijn opgenomen, gelden onverkort voor de toepassing door de opsporingsambtenaren van de BOD'en.

De leden van de SP-fractie hebben gevraagd of de regering kan aangeven welke geautomatiseerde werken op dit moment onder de definitie van geautomatiseerd werk vallen en waarom. Tevens hebben zij gevraagd

waar uiteindelijk de grens ligt, wie dat bepaalt en wie dat uiteindelijk controleert.
Het begrip geautomatiseerd werk is ingekaderd in het Cybercrimeverdrag van de Raad van Europa. Op grond van artikel 1, onderdeel a, van dit verdrag wordt onder dit begrip verstaan een apparaat of groep van onderling verbonden apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken. Uit deze begripsomschrijving vloeit voort dat ieder apparaat, dat op basis van een programma automatisch gegevens verwerkt, onder de reikwijdte valt van het begrip geautomatiseerd werk. Nederland is gehouden dit verdrag te implementeren. Vastgesteld kan worden dat deze begripsomschrijving ruim is en, zeker in het licht van de ontwikkeling van «the internet of things», veel verschillende apparaten kan omvatten. Ook een groep van onderling verbonden apparaten valt onder de definitie van het begrip geautomatiseerd werk, mits een of meer van die apparaten op basis van een programma gegevens verwerkt. Dit betekent dat de grens niet zozeer ligt in de definitie van het geautomatiseerde werk, als wel in de beperkingen in de toepassing van de bevoegdheid tot het binnendringen van een dergelijk werk. Echter, als verschillende apparaten met elkaar zijn verbonden, bijvoorbeeld in een thuisnetwerk, terwijl meerdere apparaten zelfstandig op basis van een programma gegevens verwerken, dan zal een bevel tot het op afstand binnendringen van een geautomatiseerd werk meerdere geautomatiseerde werken kunnen omvatten. Vereist is dat de geautomatiseerde werken bij de verdachte in gebruik zijn, en dat het binnendringen van die geautomatiseerde werken noodzakelijk is voor de opsporing van ernstige strafbare feiten. De officier van justitie in het bevel moeten opnemen om welke geautomatiseerde werken het precies gaat zodat de rechter-commissaris zich een oordeel kan vormen over de rechtmatigheid van het binnendringen in die werken. Van belang is dat het object van het binnentreden voldoende precies kan worden vastgesteld. Deze omschrijving vormt de basis voor de toets van proportionaliteit en subsidiariteit. De inzet van de bevoegdheid is vervolgens beperkt tot het geautomatiseerde werk zoals in het bevel omschreven. Welke kenmerken de beschrijving van het geautomatiseerde werk vormen kan per voorgestelde inzet verschillen. Zo zal het bijvoorbeeld wanneer de smartphone van de verdachte bekend is, het in de rede liggen dat het zogenaamde MAC-adres van het betreffende geautomatiseerde werk wordt opgenomen. Een MAC-adres is een uniek nummer dat is verbonden aan de betreffende hardware, zodat deze kan worden geïdentificeerd. Wanneer de bevoegdheid bijvoorbeeld wordt ingezet voor het binnendringen in een zwaar beveiligde server waar zich naar verwachting kinderporno bevindt kan niet altijd van te voren duidelijk zijn om welk MAC-adres het gaat, en kan het meer in de rede liggen dat in het bevel het IP-adres wordt opgenomen dat op dat moment de verbinding vormt tussen het betreffende geautomatiseerde werk en het internet. Essentieel is dat de rechter-commissaris zich op basis van de gegeven omschrijving van het geautomatiseerde werk een goed beeld kan vormen van de reikwijdte van het binnendringen en kan beoordelen in hoeverre dit door de omstandigheden wordt gerechtvaardigd. Als tijdens het onderzoek in een geautomatiseerd werk blijkt dat een ander geautomatiseerd werk op afstand moet worden binnengedrongen, dan zijn een aanvullend bevel evenals een aanvullende machtiging van de rechter-commissaris vereist. Het bevel en de machtiging kunnen mondeling worden afgegeven. Aldus zal zich in de praktijk een stapsgewijze aanpak kunnen ontwikkelen, op basis waarvan de betrokkenheid van de rechter-commissaris verzekerd is zodra een geautomatiseerd werk op afstand wordt binnengedrongen met het oog op het verrichten van bepaalde onderzoekshandelingen.

De leden van de SP-fractie hebben gevraagd hoe men weet waar men moet zijn als er bepaalde gegevens van een geautomatiseerd werk nodig

zijn, hoe groot het risico is dat men ook toegang krijgt tot gegevens van derden of gegevens die niet nodig zijn voor de opsporing en hoe dit risico zoveel mogelijk wordt weggenomen. De leden van deze fractie hebben tevens gevraagd hoe wordt voorkomen dat ongericht gegevens wordt verzameld en hoe de regering dit praktisch voor zich ziet. Ten slotte hebben deze leden begrepen dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn, en hebben zij gevraagd of, als het werk waar de gegevens op staan niet bekend is en het tijdrovend en privacy schendend is om deze te achterhalen, dit betekent dat het plaatsen van software niet altijd mogelijk is.
Een onderzoek in een geautomatiseerd werk kent een zorgvuldige voorbereiding. In de verkennende fase worden gegevens over strafbare feiten en personen die daarbij betrokken zijn in kaart gebracht. Daarbij wordt ook gekeken of, en zo ja welke, geautomatiseerde werken in gebruik zijn bij een persoon. Deze voorbereidende werkzaamheden verschillen niet wezenlijk van de werkzaamheden die worden verricht bij de voorbereiding van andere (bijzondere) opsporingsbevoegdheden. Als er geen aanknopingspunten voor onderzoek in een geautomatiseerd werk zijn, zal de bevoegdheid niet worden ingezet.
Tijdens de verkennende fase wordt zoveel mogelijk een beeld gevormd van de gegevens die nodig zijn voor het onderzoek naar de specifieke strafbare feiten in relatie tot een verdachte. De verkennende fase vormt de basis voor het bevel van de officier van justitie. De onderzoekshandelingen worden in het bevel vermeld. Voorts vermeldt het bevel het deel van het geautomatiseerde werk en de categorie van gegevens waar het onderzoek betrekking op heeft en bevat het een aanduiding van aard en functionaliteit van de software die gebruikt mag worden bij het onderzoek.
Het onderzoek in een geautomatiseerd werk vindt plaats binnen de grenzen van het bevel van de officier van justitie en wordt verricht door het eerdergenoemde technische team. Voor zover het doel van het onderzoek gelegen is in het opnemen van vertrouwelijke communicatie of het opnemen van telecommunicatie of de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, zoals emailverkeer, kan niet worden uitgesloten dat gegevens worden verkregen over andere personen die bij de communicatie zijn betrokken. Dit is thans evenmin anders, als vertrouwelijke communicatie wordt afgeluisterd of communicatie wordt afgetapt (op grond van de artikelen 126l, 126m, 126s, 126t of 126zg Sv) of als gegevens over het emailverkeer van een persoon worden gevorderd bij de aanbieder (artikelen 126nd/ng Sv). Uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier van justitie vallen worden ter beschikking gesteld van het tactische onderzoeksteam.

De leden van de SP-fractie hebben verder begrepen, zoals de regering stelt, dat het nodig is om gegevens te onderscheppen voordat ze versleuteld worden of nadat ze ontsleuteld zijn. Soms is het werk waar de gegevens op staan niet bekend en is het tijdrovend en privacy schendend om deze te achterhalen. De leden van deze fractie hebben gevraagd of dit betekent dat het plaatsen van software niet altijd mogelijk is, en tevens of het achterhalen van geautomatiseerd werk minder privacy-schendend is dan het anoniem inbreken op een geautomatiseerd werk.
Met hun vraagstelling refereren de leden van de SP-fractie kennelijk aan de toelichting op nut en noodzaak van de voorgestelde bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk. Thans wordt de opsporing van cybercrime gehinderd door de technische ontwikkelingen rond het internet, zoals cloudcomputing en de uitbreiding van de mogelijkheden tot encryptie. Daardoor zijn bestaande opsporingsbevoegdheden minder effectief, omdat deze wetenschap van de locatie van het geautomatiseerde werk veronderstellen (de inbeslagneming van voorwerpen of het vorderen van gegevens bij derden) of omdat deze

slechts leiden tot het verzamelen van versleutelde gegevens (internettap). De opsporing staat dan met lege handen. Hieraan kan worden tegemoet gekomen door op afstand (online) een geautomatiseerd werk binnen te dringen. Voor een effectieve toepassing van deze bevoegdheid is het juist niet vereist dat de precieze locatie van het geautomatiseerde werk bekend is. Overigens is het achterhalen van de locatie van een geautomatiseerd werk een minder ingrijpende aantasting van de privacy van de betrokkene dan het op afstand binnendringen van dat geautomatiseerde werk, omdat in het laatste geval toegang wordt verkregen tot de gegevens die in dat werk worden verwerkt.

De aan het woord zijnde leden hebben voorts gevraagd of het klopt dat het op dit moment niet mogelijk is gegevens te achterhalen die zijn opgeslagen in de Cloud. De leden van deze fractie hebben tevens gevraagd of praktijkvoorbeelden kunnen worden gegeven van opsporingsonderzoeken die niet zijn geslaagd puur en alleen omdat de benodigde gegevens in de Cloud niet op een andere manier konden worden verkregen.
Voorbeelden van onderzoeken waarbij het opsporingsonderzoek niet is geslaagd omdat de benodigde gegevens in de cloud niet op een andere manier konden worden verkregen zijn divers. In de huidige praktijk kunnen bijvoorbeeld onoverkomelijke problemen voor opsporingsonderzoeken ontstaan wanneer een cloudaanbieder niet gevestigd is in het land waar de server zich bevindt waarop de informatie van de verdachte staat. Dit zorgt binnen het internationale rechtshulpverkeer voor substantiële vertraging tot wel negen maanden, en bijbehorend risico op verlies van bewijsmateriaal. Deze risico's worden vermeden met het op afstand binnendringen van een geautomatiseerd werk, dat in gebruik is bij de verdachte, zodat gegevens kunnen worden veiliggesteld die op dat werk zijn opgeslagen. Het Team High Tech Crime van de landelijke eenheid van het landelijk politiekorps heeft diverse onderzoeken waarin er geen bewijsmateriaal kon worden verzameld moeten staken, omdat deze zich in de cloud bevonden en de eigenaar van de server (meestal een ISP) niet (tijdig) reageerde op verzoeken. Daarnaast zijn er gevallen bekend waarin er «spamruns» zijn verstuurd waarna er in het desbetreffende opsporingsonderzoek bewijsmateriaal werd gezocht in een googleaccount. Het veiligstellen van die informatie bleek zinloos, omdat de informatie reeds was gewist. Deze zaken zijn zonder resultaat afgesloten. In een zaak waarbij klanten van een Nederlandse bank slachtoffer werden van computervredebreuk, alsmede de daaropvolgende oplichting of diefstal is het onderzoek afgesloten, omdat er geen bewijsmateriaal uit de cloud kon worden veiliggesteld. Ook een aanval op honderden emailadressen van MKB-bedrijven met daarin malware verwerkt die een Remote Acces Tool installeerde op de geautomatiseerde werken van die MKB-bedrijven, moest worden afgesloten omdat het niet mogelijk bleek om nog bewijs uit de cloud veilig te stellen.
Daarnaast is het in de praktijk moeilijk en vaak niet mogelijk om gegevens te achterhalen die zijn opgeslagen in de cloud omdat dat het technisch zeer lastig kan zijn om vast te stellen waar gegevens zich op de wereld bevinden. Als de locatie van gegevens niet te bepalen is, is het juridisch lastig om aan een concreet land een rechtshulpverzoek te doen waarbij deze gegevens kunnen worden gevorderd, omdat onzeker is of dat land jurisdictie heeft.
Deze vorm van «loss of (knowledge of) location» is uitgebreid aan de orde geweest tijdens internationale bijeenkomsten, waaronder de Global Conference on Cyber Space 2015 en diverse bijeenkomsten in het kader van het EU voorzitterschap van Nederland in het eerste deel van 2016. In een in dat kader georganiseerd seminar genaamd «jurisdictie in cyberspace» is naar voren gekomen dat in de EU landen, maar ook daarbuiten, dezelfde problematiek wordt ervaren en dat de oplossingsrichtingen

divers zijn. Zoals aan uw Kamer rondom de JBZ raad van juni 2016 is bericht, zijn mede op grond van dit seminar raadsconclusies over criminal justice in cyberspace aangenomen. Onder regie van de Europese Commissie, in nauwe samenwerking met lidstaten en met andere zowel nationale als Europese instituties, wordt nu op programmatische wijze uitvoering gegeven aan de in de raadsconclusies benoemde actiepunten en planning.
In de praktijk is er op dit moment vaak pas zicht op gegevens die zich in de cloud bevinden nadat in beslag genomen apparaten kunnen worden doorzocht of gedurende een netwerkzoeking bij een (fysieke) doorzoeking ter vastlegging van gegevens. Onder andere vanwege de vluchtigheid van gegevens is het vaak onvoldoende effectief om daarna contact te leggen met het bedrijf die toegang heeft tot die gegevens. Daar komt bij dat ook in deze gevallen de locatie van de gegevens die zich in de cloud bevinden onbekend is en vaak blijft. Daardoor is veelal onduidelijk aan welk land rechtshulp gericht kan worden, dan wel of dat land een bedrijf kan verplichten informatie aan te leveren, waarvan onbekend is of zich dat in dat land bevindt. De voorgestelde bevoegdheid tot het op afstand binnendringen in geautomatiseerd werk kan in dergelijke situaties uitkomst bieden, zodat de opsporing minder afhankelijk is van informatie uit de cloud.

De leden van de SP-fractie hebben opgemerkt dat op dit moment niet is voorzien in de mogelijkheid om een bug te plaatsen die door middel van software buitenaf, dus online, op de computer wordt geplaatst. De leden van deze fractie hebben gevraagd of hiermee eigenlijk ook niet wordt gesuggereerd dat het inzetten van bepaalde spyware niet rechtmatig was, zoals wel werd aangegeven in het antwoord op de Kamervragen over de inzet van Finfisher (Aanhangsel Handelingen II 2014/15, nr. 202). De leden van deze fractie zouden hier graag een toelichting op ontvangen, en ook op de uitspraak van FOX IT in de gespreksnotitie voor het rondetafelgesprek over onderhavig wetsvoorstel op 11 februari 2016, waarin wordt gesteld dat de politie al geoefend heeft met het instrument hacken. Deze leden meenden dat dit dus betekent dat er wel degelijk reeds op afstand heimelijk is binnengedrongen op een geautomatiseerd werk, en hebben gevraagd op basis van welke wettelijke grondslag dat dan is gebeurd.
Zoals eerder is gesteld in het antwoord op de Kamervragen over de inzet van Finfisher is het onder bepaalde omstandigheden op basis van artikel 125i van het Wetboek van Strafvordering, na een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen. In een aantal strafzaken waarin het ging om zeer ernstige strafbare feiten is hiervan sprake geweest. Zoals tevens aangegeven in de antwoorden op deze Kamervragen experimenteert de politie niet met het overnemen van computers van verdachten. In het kader van de voorbereidingen op de invoering van het voorliggende wetsvoorstel hebben opsporingsambtenaren wel al kennis opgedaan van de technieken die hiervoor nodig zijn. Daarbij is geen sprake geweest van het binnendringen in een geautomatiseerd werk. Het opdoen van dergelijke kennis is nodig om de bevoegdheid uit te oefenen als deze voor hen beschikbaar wordt om in te zetten in het kader van een opsporingsonderzoek.

De leden van de SP-fractie hebben opgemerkt dat er een verplichting komt tot vernietiging van de gegevens die onder het geheimhoudingsplicht vallen, en gevraagd wie bepaalt welke gegevens om die redenen kunnen worden vernietigd en om welke gegevens het gaat. Tevens hebben zij gevraagd hoe wordt omgegaan met het feit dat de gegevens op dat moment reeds zijn ingezien, en of de betreffende opsporingsambtenaar dan een afgeleide geheimhoudingsplicht heeft.

De regeling van het bestaande artikel 126aa, tweede lid, Sv is van toepassing op het onderzoek in een geautomatiseerd werk, en voorziet in de verplichting tot vernietiging van de processen-verbaal en andere voorwerpen, voor zover die mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 Sv zou kunnen verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd. Als de officier van justitie vaststelt dat de mededelingen onder deze verplichting vallen dan beveelt hij terstond de vernietiging van de processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen. In de gevallen waarin de geheimhouder verdachte is, wordt het oordeel van een gezaghebbend lid van de betreffende beroepsgroep ingewonnen over de vraag welke gegevens dergelijke mededelingen behelzen. De procedure voor de vernietiging van de vastgelegde gegevens is uitgewerkt in het Besluit bewaren en vernietigen niet-gevoegde stukken. Uit de wettelijke vernietigingsplicht vloeit voort dat de betreffende gegevens niet in het opsporingsonderzoek mogen worden gebruikt.

De leden van de SP-fractie hebben begrepen dat inmiddels ook gebruik wordt gemaakt van internettaps, waardoor communicatiegegevens, die via internet gedeeld worden, afgetapt kunnen worden. De leden van deze fractie hebben gevraagd waarom deze mogelijkheid blijkbaar onvoldoende is zodat opsporingsambtenaren de bevoegdheid krijgen op afstand te kunnen hacken. Deze leden hebben tevens gevraagd om welke opsporingsambtenaren het gaat het en in welke situaties het noodzakelijk is.
Het aftappen van telecommunicatie vormt een waardevol opsporingsmiddel. Met een internettap kan alle internetverkeer, dat door middel van een aanbieder van een communicatiedienst of een communicatienetwerk wordt afgehandeld, worden afgetapt en opgenomen. Een internettap wordt geplaatst op een IP-adres. Bij een internettap wordt het dataverkeer afgetapt dat van en naar een huisadres of IP-adres gaat, dus ook het dataverkeer van huisgenoten of anderen die de betreffende aansluiting gebruiken. Zoals hierboven, naar aanleiding van de beantwoording van vragen van de leden van de PvdA-fractie reeds aan de orde is gekomen, zijn er echter specifieke situaties waarin een internettap geen soelaas biedt. Dit is bijvoorbeeld aan de orde als de betrokken persoon gebruik maakt van hotspots, alsdan moet bij een groot aantal aanbieders een internettap worden geplaatst om het internetverkeer via de verschillende hotspots te onderscheppen. Hier komt nog bij dat de aanbieder voor het aftappen van de communicatie van een laptop een MAC-adres nodig heeft; als gebruik wordt gemaakt van een hotspot dan komt echter niet het MAC-adres van de laptop maar het MAC-adres van de hotspot bij de aanbieder binnen. Verder is de internettap beperkt tot de communicatie die via een aanbieder wordt afgehandeld; deze methode biedt geen inzicht in gegevens die (reeds) op het geautomatiseerde werk zijn opgeslagen en die tijdens de periode van het tappen niet met anderen worden uitgewisseld. Tenslotte biedt de internettap geen soelaas bij het gebruik van encryptie; er wordt dan digitale informatie afgetapt en opgenomen die gecodeerd is. Criminelen maken steeds vaker gebruik van versleuteling van communicatie, zoals TOR, VPN en andere vergelijkbare mogelijkheden. Tenslotte wordt het internetverkeer naar steeds meer websites versleuteld door het beter beveiligde «https» als alternatief voor «http».
Voor het antwoord op de vraag welke opsporingsambtenaren dit betreft kan worden verwezen naar de eerdere beantwoording van de vraag van de leden van de PvdA-fractie over de mogelijkheid van het gebruik van de nieuwe bevoegdheid door de bijzondere opsporingsdiensten.

De leden van de SP-fractie waren benieuwd op welke manier rekening wordt gehouden met de vrijheid van meningsuiting en hebben gevraagd

of er een uitgebreide instructie aan de rechter-commissaris komt voor de afweging over afgifte van een machtiging om een site te blokkeren of te hacken. Tevens hebben deze leden gevraagd hoe rekening wordt gehouden met de wettelijke bronbescherming bij het afgeven van een machtiging.
Het blokkeren van een website is reeds mogelijk op basis van het huidige artikel 54a Sr. Hiervoor is een machtiging van de rechter-commissaris vereist, ook omdat de vrijheid van meningsuiting hierbij in het geding kan zijn. Met dit vereiste is voorzien in een onafhankelijke rechterlijke oordeelsvorming, voordat wordt overgegaan tot het toepassen van de tijdelijke maatregel van het ontoegankelijk maken van gegevens. Hierbij past geen instructie aan de rechter-commissaris over de wijze waarop de rechterlijke afweging plaatsvindt. Journalisten hebben geen wettelijk verschoningsrecht vanwege hun stand, beroep of ambt, als bedoeld in artikel 218 Sv. Inmiddels is het wetsvoorstel bronbescherming in strafzaken bij Uw Kamer ingediend (Kamerstukken II 2014/15, 34 032, nr. 1), dat voorziet in wettelijke verankering van een recht op bronbescherming. In afwachting van de afronding van de parlementaire behandeling en de inwerkingtreding van het wetsvoorstel bronbescherming in strafzaken is het geldend recht vastgelegd in een Aanwijzing van het College van procureurs-generaal (Strct. 2012, 3656). De Aanwijzing van het College van procureurs-generaal bevat het geldende beleid voor justitieel optreden tegen journalisten met in begrip van de toepassing van dwangmiddelen tegen journalisten, zoals het thans wordt uitgevoerd. Het beleid houdt in dat bij de toepassing van dwangmiddelen tegen journalisten grote terughoudendheid wordt betracht.

De leden van de fractie van D66 hebben de regering gevraagd in te gaan op de noodzaak en naast enkele concrete gevallen ook een meer overstijgende algemene noodzaak te formuleren voor de toevoeging van deze bevoegdheid. Daarbij hebben zij gevraagd of ook een andere minder ingrijpende wijze mogelijk is.
In de memorie van toelichting is uitgebreid ingegaan op de bredere ontwikkelingen die de voorgestelde bevoegdheden noodzakelijk maken (paragraaf 2.1). De opkomst van het internet en het wijdverbreide gebruik ervan heeft de samenleving en de economie enorme voordelen opgeleverd, maar deze ook kwetsbaar gemaakt voor criminelen. Ook criminelen gebruiken de mogelijkheden van het internet, onder meer voor vertrouwelijke en versleutelde communicatie en het plegen van strafbare feiten zoals voorbereidingshandelingen van liquidaties, afpersingen, hoogwaardige computercriminaliteit, grootschalige fraude, oplichting en de verspreiding van kinderpornografisch materiaal. Steeds meer informatie en bewijs voor de opsporing van strafbare feiten is alleen nog in elektronische vorm beschikbaar. Daarnaast zijn er strafbare feiten die volledig in de digitale wereld plaatsvinden, zoals de verspreiding van botnets, computervredebreuk en sabotage. Drie wezenlijke problemen en gebleken knelpunten worden onderscheiden. Het betreft ten eerste de toenemende versleuteling van elektronische gegevens. Criminelen gebruiken geavanceerde technieken om zich voor de autoriteiten te verbergen, bijvoorbeeld technieken voor anonimisering en sterke encryptie. Daardoor is het vaak niet mogelijk met andere middelen, zoals aftappen of het in beslag nemen van voorwerpen, een dader of een geautomatiseerd werk met daarop bewijsmateriaal, te identificeren en voldoende bewijs te vergaren. Een verbod op decryptie of een verplichting tot verzwakking van encryptie is niet wenselijk. 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 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. Het binnendringen in een geautomatiseerd werk brengt een inbreuk in de persoonlijke levenssfeer met zich mee. Deze inbreuk kan in ernst en omvang verschillen. Bij de keuze voor de inzet van bevoegdheden zijn de proportionaliteit en de subsidiariteit een uitgangspunt. De inzet dient proportioneel te zijn ten opzichte van de inbreuk op de persoonlijke levenssfeer, het risico op nevenschade en de ernst van het strafbare feit. Bovendien worden eerst andere, minder ingrijpende bevoegdheden overwogen alvorens tot inzet te besluiten. Als deze minder ingrijpende bevoegdheden niet toereikend worden geacht, is de mogelijkheid tot het binnendringen aan de orde. Deze afwegingen worden voorafgaand aan iedere inzet gemaakt door de officier van justitie en getoetst door de rechter-commissaris.

De leden van de D66-fractie hebben gevraagd om een toelichting op de verwachte proportionaliteit en effectiviteit van de bevoegdheid en hoe die is afgewogen. Deze leden hebben tevens gevraagd waaruit bijvoorbeeld blijkt dat sprake is van een leemte in de bestaande wettelijke bevoegdheden.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de SP-fractie of er minder vergaande mogelijkheden zijn waarbij de privacy beter gewaarborgd is (inleiding) en van de leden van de PvdA-fractie of niet eerst wordt overwogen andere bevoegdheden te gebruiken die wellicht een minder zware impact op de persoonlijke levenssfeer of de veiligheid van de internetgebruiker hebben (paragraaf 2.1).

De leden van de D66-fractie hebben de conclusie getrokken dat het belang van sterke encryptie voor de persoonlijke levenssfeer, voor de vertrouwelijke communicatie van overheden en bedrijven en voor de Nederlandse economie dus boven het opsporingsbelang van de politie om de encryptie te verzwakken gaat, en hebben de regering gevraagd toe te lichten waarom dit niet geldt voor het belang van veilige software. De overheid krijgt met dit wetsvoorstel immers een belang bij fouten in de software die nodig zijn om te kunnen hacken en die ook door criminelen gebruikt kunnen worden.
In de brief van 4 januari 2016 over het kabinetsstandpunt encryptie onderstreept het kabinet het belang van de rechtmatige toegang tot gegevens voor de opsporing van strafbare feiten (Kamerstukken II 2015/16, 26 643, nr. 383). Het kabinet concludeert in de brief dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. De brief vermeldt ook dat, gelet op het belang van de opsporing en vervolging van strafbare feiten en de belangen die zijn gemoeid met de nationale veiligheid, de ontwikkelingen nopen tot het zoeken naar nieuwe oplossingen. Het binnendringen in een geautomatiseerd werk is een belangrijke mogelijkheid om elektronisch

bewijs te vergaren, zeker als sprake is van encryptie. Deze bevoegdheid maakt het bijvoorbeeld mogelijk om een specifiek geautomatiseerd werk binnen te dringen en daar niet-versleutelde gegevens over te nemen, bijvoorbeeld op het moment dat een verdachte zelf deze gegevens raadpleegt.
Ter versterking van de digitale veiligheid van Nederland en de beperking van de criminaliteit stimuleert het Ministerie van Veiligheid en Justitie het melden van kwetsbaarheden, onder meer met het beleid voor «responsible disclosure». Naast voorlichting aan haar partners over door derden gemelde kwetsbaarheden zal het NCSC in voorkomende gevallen ontdekte kwetsbaarheden zelf melden aan de fabrikant. Het wetsvoorstel Gegevensverwerking en meldplicht cyber security helpt bij het onderkennen van kwetsbaarheden in de systemen van vitale sectoren, waarbij het NCSC een centrale rol heeft (Kamerstukken II 2015/16, 34 388, nr. 1).
Daarnaast erkent het kabinet dat criminelen voor hun activiteiten steeds vaker gebruik maken van het internet. Strafbare feiten zijn zonder onderzoek te doen op het internet steeds lastiger te onderkennen of te bewijzen. Voor een effectieve opsporing is onderzoek op internet noodzakelijk. Om een zorgvuldige afweging te kunnen maken over de inzet van bevoegdheden, is elke bevoegdheid in de desbetreffende wet van specifieke voorwaarden en waarborgen voorzien. Dat geldt ook voor de bevoegdheid tot binnendringen in een geautomatiseerd werk. De inzet van deze bevoegdheid wordt altijd getoetst aan de eisen van proportionaliteit en subsidiariteit. De inzet moet proportioneel zijn ten opzichte van het doel en het potentiele risico op onbedoelde effecten. Bovendien is de inzet alleen geoorloofd als niet met een minder ingrijpend middel hetzelfde doel kan worden bereikt.
Voorts wordt verwezen naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten bij hoeveel zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, in 2015 de versleuteling van gegevens een cruciale factor heeft gevormd waardoor niet tot vervolging is overgegaan, hoeveel criminelen nu vrij rond lopen doordat zij gebruik maken van encryptie waardoor de politie bepaalde gegevens niet kunnen inzien en of de regering een statistisch overzicht kan geven van het aantal taps dat ineffectief is door het gebruik van encryptie.
Dit wetsvoorstel voorziet niet in een verplichting tot decryptie van versleutelde gegevens. Overigens houden de politie en het openbaar ministerie geen cijfers of statistieken bij van zaken waarin de versleuteling van gegevens een cruciale factor heeft gevormd waardoor niet tot vervolging is overgegaan, hoeveel criminelen nu vrij rond lopen doordat zij gebruik maken van encryptie waardoor de politie bepaalde gegevens niet kunnen inzien en het aantal taps dat ineffectief is door het gebruik van encryptie. Uit het rapport van het WODC over het gebruik van de telefoon- en de internettap in de opsporing (2012, Boom/Lemma uitgevers) komt naar voren dat afscherming en encryptie in toenemende mate de opsporing bemoeilijken. De aanbieders van telecommunicatiediensten op internet zijn encryptie bijna standaard gaan toepassen. Wanneer gebruik wordt gemaakt van een aanbieder van een online telecommunicatiedienst uit het buitenland dan is de inhoud van gesprekken niet te ontsluiten. Wanneer gebruik wordt gemaakt van een Nederlandse aanbieder dan is decodering niet bij voorbaat onmogelijk maar wel tijdrovend. De oplossing hiervoor is gelegen in het onderscheppen van de communicatie nog voordat deze wordt versleuteld (blz. 165/167).
In de meerderheid van de huidige strafrechtelijke onderzoeken naar georganiseerde criminaliteit en cybercrime wordt gebruik gemaakt van diverse vormen van versleutelingstechnieken. Dat brengt op dit moment

met zich mee dat de opsporingsdiensten in die zaken geen of slechts zeer moeilijk toegang krijgen tot belangrijk bewijsmateriaal en er daardoor voor diverse zaken onvoldoende bewijs kan worden verzameld. In verschillende strafzaken waarin het NFI in staat is gebleken om versleutelde berichten die werden uitgewisseld via extra beveiligde Blackberry's te ontsleutelen, kwam naar voren dat er op die manier tussen verdachten werd gecommuniceerd om daarmee hun communicatie verborgen te houden voor de opsporingsdiensten.

De leden van de D66-fractie hebben gelezen dat de toename van het gebruik van meerdere verschillende draadloze netwerken ook als noodzaak wordt genoemd voor dit wetsvoorstel. Deze leden hebben gevraagd of de regering kan aangeven wat zij doet om eigenaren van Wi-Fi-netwerken erop te attenderen dat de beveiliging van het Wi-Fi-netwerk niet op orde is, waardoor onder andere criminelen er gebruik van kunnen maken. Tevens hebben zij gevraagd of de regering op de hoogte is van pilots in Australië en de Verenigde Staten om kwetsbare Wi-Fi-netwerken in kaart te brengen en de eigenaren te helpen de beveiliging op orde te brengen, en of de regering zelf ervaring heeft met deze praktijk. De leden van deze fractie hebben voorts gevraagd waarom de regering niet inzet op het veiliger maken van Wi-Fi-netwerken, zodat criminelen minder snel gebruik kunnen maken van de verschillende Wi-Fi-netwerken.
De regering stimuleert een veilig gebruik van het internet door burgers en bedrijven met verschillende initiatieven. Het NCSC heeft een zogenaamd Whitepaper Cloudcomputing gepubliceerd met adviezen hoe organisaties hun wifi kunnen beveiligen (https://www.ncsc.nl/actueel/whitepapers/whitepaper-cloudcomputing.html). Daarnaast wordt informatie en handelingsperspectief geboden aan eindgebruikers via veiliginternetten.nl en de jaarlijkse campagne Alert Online. De regering is van mening dat het in eerste instantie de verantwoordelijkheid van de burgers zelf is en van de bedrijven die internetdiensten leveren om voor adequate beveiliging te zorgen. Daarnaast is het al zo dat bij de installatie van die netwerken, hetzij door de installateurs, hetzij door de gebruikers zelf, instellingen (kunnen) worden ingesteld waardoor de wifi netwerken beveiligd worden.

De leden van de D66-fractie hebben gevraagd of de regering een overzicht kan geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van verschillende Wi-Fi-netwerken. Deze leden hebben tevens gevraagd of de politie ook andere geautomatiseerde werken op een openbaar Wi-Fi-netwerk kan hacken als een verdachte ook gebruik maakt van dat netwerk.
De vraag van de leden van de D66-fractie of de regering een overzicht kan geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van verschillende Wi-Fi-netwerken kan vanwege het ontbreken van dit soort gegevens helaas niet worden beantwoord. Bij inzet van de bevoegdheid zal de officier van justitie in het bevel moeten opnemen om welke geautomatiseerde werk het precies gaat zodat de rechter-commissaris zich een oordeel kan vormen over de rechtmatigheid van het binnendringen in dat geautomatiseerde werk. Van belang is dat het object van het binnentreden voldoende precies kan worden vastgesteld. Deze omschrijving vormt de basis voor de toets van proportionaliteit en subsidiariteit. De inzet van de bevoegdheid is vervolgens beperkt tot het geautomatiseerde werk zoals in het bevel omschreven.

De leden van de D66-fractie hebben opgemerkt dat de regering stelt dat voor de aanbieders van cloudcomputingdiensten de plaats van opslag vanuit bedrijfseconomisch perspectief vooral van belang is in verband met de kosten daarvan en de zekerheid van de verbindingen, en hebben

gevraagd of de regering zich bewust is van het feit dat ook de veiligheid van de data van de klanten van de cloudcomputingdiensten een belangrijk aspect is voor de keuze van vestiging van een bedrijf of individueel datacenter van een bedrijf. De leden van deze fractie hebben tevens gevraagd of de regering kan aangeven of zij het hacken, dat wil zeggen het hacken door middel van fouten in software, van servers van cloudcomputingdiensten uitsluit en zo nee, of de regering kan aangeven hoe zij de gevolgen hiervan inschat voor de Nederlandse economie en het Nederlandse vestigingsklimaat.
De inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk zal kunnen worden ingezet ten behoeve van de opsporing van ernstige strafbare feiten. De inzet geschiedt onder vooraf bepaalde voorwaarden en met passende waarborgen omkleed. Bij de inzet zijn proportionaliteit en subsidiariteit belangrijke uitgangspunten. Dat betekent dat de bevoegdheid alleen wordt ingezet indien deze inzet in het specifieke geval proportioneel is ten opzichte van het strafbare feit. Bovendien wordt de bevoegdheid ingezet indien de nodige informatie of het bewijs niet met inzet van een minder ingrijpende bevoegdheid kan worden verkregen. Bij cloudcomputingdiensten kan een minder ingrijpende bevoegdheid voorhanden zijn, zoals het vorderen van gegevens bij de dienstverlener (art. 126nd Sv) of het vastleggen van gegevens tijdens een doorzoeken ter vastlegging van gegevens (artikel 125i of 125j WvSv). Inzet van de bevoegdheid op een wijze die de bedrijfsvoering van een clouddienstverlener ernstig aantast, zal niet snel als proportioneel en subsidiair worden goedgekeurd.
De meeste clouddienstverleners werken voldoende samen met de opsporingsdiensten, voornamelijk op basis van vorderingen voor gegevens. Er zijn echter clouddienstverleners die zeer slecht meewerken aan opsporingsonderzoeken en zelfs technische maatregelen nemen om de opsporing van strafbare feiten te verhinderen (zogenaamde bullet proof hosting providers). Een deel van deze dienstverleners adverteert met de mogelijkheid voor klanten om strafbare feiten te plegen buiten het bereik van de opsporingsdiensten. Hoewel het binnendringen bij cloudcomputingdiensten op een wijze die de bedrijfsvoering van een clouddienstverlener aantast in het algemeen niet heel waarschijnlijk is, kan het om bovengenoemde redenen niet bij voorbaat volledig worden uitgesloten. Dit zal echter zijn beperkt tot uitzonderlijke gevallen.
Daarnaast kan worden opgemerkt dat de voorgestelde bevoegdheid ook juist kan bijdragen aan de veiligheid van in Nederland gevestigde bedrijven omdat het de opsporing meer mogelijkheden geeft om op te treden tegen strafbare feiten als jegens de cloudprovider strafbare feiten zijn gepleegd. Mede gelet op de wettelijke criteria voor de inzet van de voorgestelde bevoegdheid, en de aanvullende mogelijkheden om op te treden tegen criminaliteit tegen bedrijven zal de mogelijkheid van de inzet daarvan naar verwachting geen grote negatieve gevolgen hebben voor de Nederlandse economie en het Nederlandse vestigingsklimaat.

De leden van de D66-fractie hebben gevraagd of de regering een overzicht kan geven van het aantal zaken, die onder de reikwijdte van dit wetsvoorstel zouden vallen, dat niet is opgelost doordat criminelen gebruik maakten van Cloudcomputingdiensten.
Zoals hierboven, naar aanleiding van een soortgelijke vraag van de leden van deze fractie reeds is aangegeven, houden de opsporingsdiensten en het openbaar ministerie geen cijfers of statistieken bij van het aantal zaken dat niet is opgelost doordat criminelen gebruik maakten van cloudcomputingdiensten. Deze vraag kan helaas niet worden beantwoord.

De leden van de D66-fractie hebben voorts de regering gevraagd in te gaan op de voordelen van ICT-technologieën die het voor de politie de afgelopen jaren juist makkelijker hebben gemaakt om criminelen op te

pakken, zoals beter beschikbare informatie via telefoons en iPads, het gebruik van drones, «gunshot-detection-systems», het monitoren van tweets en andere social media, het voorspellen van misdaad op basis van «big-data» of GPS-systemen. De leden van deze fractie hebben tevens gevraagd of de regering kan toelichten in hoeverre de technologische ontwikkelingen het werk van de politie de afgelopen jaren per saldo makkelijker of moeilijker hebben gemaakt, en of de regering haar antwoord met statistieken kan onderbouwen.
In algemene zin kan worden gesteld dat nieuwe (ICT-)technologieën inderdaad nieuwe mogelijkheden bieden die voor de opsporing gebruikt kunnen worden. De mate waarin dit leidt tot het «makkelijker» oppakken van criminelen, verschilt van geval tot geval. Er zijn gevallen bekend waarin criminelen bewijsmateriaal rond een strafbaar feit simpelweg op Facebook zetten. Daarnaast zijn er veel gevallen waarin nieuwe technologieën weliswaar helpen, maar ook arbeidsintensief zijn voor de opsporing. De hoeveelheid gegevens en gegevensdragers die onderdeel van een opsporingsonderzoek kunnen zijn, zijn immers toegenomen. Het verkrijgen van bewijs daaruit vergt capaciteit alsmede specifieke vaardigheden en bevoegdheden. Dit geldt in ieder geval voor de genoemde telefoons en tablets, als ook voor het verkrijgen van gegevens uit social media. Tegelijkertijd staat ook de criminaliteit niet stil; ook criminelen maken gebruik van nieuwe technieken die de opsporing bemoeilijken.
Er zijn geen cijfers of statistieken beschikbaar die aangeven of het per saldo makkelijker of moeilijker is geworden; het is dan ook niet mogelijk om per zaak vast te stellen hoe succesvol de opsporing zou zijn geweest als een bepaald middel of een bepaalde bevoegdheid niet zou zijn ingezet.
Wat betreft de andere genoemde technologieën kan daaraan het volgende toegevoegd worden:

– Drones: op 3 september 2015 heeft het eerste Algemeen Overleg over drones plaatsgevonden (Kamerstukken II 2015/16, 30 806, nr. 32). Tijdens dat Algemeen Overleg en in de schriftelijk gewisselde stukken over dit onderwerp is onder meer ingegaan op het gebruik van drones ten behoeve van opsporing. Tot nu toe is er slechts in enkele incidentele gevallen gebruik gemaakt van drones voor de opsporing. Tot in 2015 was het de politie niet toegestaan om zelfstandig met drones te vliegen en werd in incidentele gevallen gebruik gemaakt van toestellen van Defensie. Nu het de politie zelfstandig is toegestaan om met drones te vliegen is dat in een enkel geval ook gebeurd, maar van grootschalig gebruik is zeker nog geen sprake. Dit hangt onder meer samen met beperkingen in het vliegen met drones. Zo mag boven bebouwing in beginsel niet gevlogen worden, en moet het zicht op de drone goed zijn.
– Het voorspellen van misdaad met Big Data: Tot op heden heeft het «voorspellen van misdaad» op basis van Big Data analyses vooral toegevoegde waarde bij het bepalen van de inzet van patrouille-eenheden, en niet voor het voorspellen van individuele strafbare feiten of daders. Met gebruikmaking van Big-Data analyses wordt voor een bepaald gebied en een bepaalde periode vastgesteld of er een verhoogde kans op een strafbaar feit is. Daarop kan de inzet van bijvoorbeeld een surveillance-eenheid worden bepaald. Dit is dus niet gekoppeld aan individuele strafbare feiten.

De leden van de D66-fractie hebben gelezen dat de regering stelt dat de opsporingsbevoegdheden, die zijn gericht op het vastleggen van elektronische gegevens, niet langer voldoen, en hebben gevraagd of de regering deze uitspraak cijfermatig kan onderbouwen. De leden van deze fractie hebben tevens gevraagd hoe dit zich verhoudt dat tot wat de Minister van Veiligheid en Justitie in 2014 in antwoord op bovengenoemde Kamervragen aan de Kamer heeft laten weten, te weten: «(d)e politie beschikt over software die fysiek geïnstalleerd kan worden op de

computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). Voorts is het onder bepaalde omstandig- heden op basis van artikel 125i van het Wetboek van Strafvordering op basis van een machtiging van de rechter-commissaris mogelijk om op afstand een computersysteem te betreden, met als uitsluitende doel de computer te doorzoeken op vooraf bepaalde gegevensbestanden en deze zo nodig in beslag te nemen door ze vast te leggen. In een aantal strafzaken waarin het ging om zeer ernstige feit en is hiervan sprake geweest.» Hieruit blijkt dat de politie al op basis van artikel 125i Sv zich toegang tot computersystemen kan verschaffen en gegevensbestanden kan doorzoeken.
De gevraagde cijfers zijn niet te achterhalen. Verder wordt gewezen op de omstandigheid dat het hier vaak onderzoeken betreft naar zware en georganiseerde criminaliteit, georganiseerde cybercriminaliteit, naar terroristische misdrijven of naar seksueel misbruik van kinderen. Daarin is meer dan gemiddeld sprake van het gebruik van afschermingsmethodieken zoals encryptie en/of anonimisering. Het «handmatig» plaatsen van software, zoals een keylogger, is dan niet mogelijk. Dat is alleen toepasbaar indien de locatie van het geautomatiseerde werk bekend is. Het vergt dan een heimelijke toepassing waarbij de opsporingsambtenaar zich fysiek de toegang verschaft tot de plaats waar het geautomatiseerde werk zich bevindt en aldaar de software kan installeren. Dat brengt grote risico's met zich mee voor de voortgang van het onderzoek en de veiligheid en inzet van personeel in het geval dat de verdachte de opsporingsactiviteiten bemerkt. Daarbij komt dat een dergelijke inzet een hoge mate van inbreuk maakt op de privacy en eventueel het woonrecht schendt van de verdachten en mogelijk anderen.
Op basis van artikel 126l van het Wetboek van Strafvordering is het, met machtiging van de rechter-commissaris, mogelijk om vertrouwelijke communicatie met een technisch hulpmiddel op te nemen (direct afluisteren). Ter uitvoering van dit bevel kan een woning worden betreden zonder toestemming van de bewoner, als het onderzoek dit dringend vordert en dit een misdrijf betreft waarop een gevangenisstraf van acht jaar of meer is gesteld. Op basis van artikel 125i van het Wetboek van Strafvordering is het, met een machtiging van de rechter-commissaris, mogelijk om een besloten plaats te betreden en vanaf die plaats in een elders aanwezig geautomatiseerd werk onderzoek te doen naar de in dat werk opgeslagen gegevens. Als gegevens worden aangetroffen die redelijkerwijs nodig zijn om de waarheid aan de dag te brengen, dan kunnen zij worden vastgelegd. Deze regelingen voldoet vanwege verschillende redenen niet als afdoende middel om deze nieuwe vormen van criminaliteit en de afscherming daarvan efficiënt te bestrijden.
In de eerste plaats biedt dit geen oplossing voor de communicatie die versleuteld plaatsvindt. Het is immers op basis van artikel 125i niet mogelijk om lopende en/of toekomstige communicatie te onderscheppen op een manier waarbij de gegevens inzichtelijk zijn. In de tweede plaats biedt dit geen oplossing voor computers die beschermd zijn met sterke wachtwoorden en zichzelf versleutelen als deze worden uitgezet of tegen versleutelde containers die op het geautomatiseerde werk staan. Voorts zal in veel zaken het moeilijk zo niet onmogelijk zijn om zonder extra bevoegdheden de juiste locatie van het geautomatiseerde werk vaststellen. Tenslotte is een inzet waarbij de woning van verdachte wordt betreden voor het plaatsen van een keylogger niet altijd proportioneel en vraagt het zeer gespecialiseerde inzet van personeel om heimelijk locaties te betreden.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten hoe de reeds bestaande mogelijkheden een verdere uitbreiding van de bevoegdheid tot het heimelijk toegang verschaffen noodzakelijk maakt zoals het wetsvoorstel pretendeert. De leden van deze fractie hebben tevens gevraagd in hoeverre hier louter kan worden volstaan met het toevoegen van enkele strikte waarborgen voor toepassing in plaats van nog verder uitbreiden van de bevoegdheden.
Voor het antwoord op de vraag naar de noodzaak van de bevoegdheid wordt verwezen naar de eerdere beantwoording van een vraag van de leden van deze fractie over de noodzaak tot toevoeging van deze bevoegdheid.

De leden van de SP-fractie hebben gevraagd waaruit blijkt dat de bestaande bevoegdheden in toenemende mate te kort schieten en welke wezenlijke problemen en gebleken knelpunten er zijn.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de D66-fractie over de noodzaak tot toevoeging van deze bevoegdheid.

De leden van de D66-fractie hebben er op gewezen dat het de bedoeling is dat bij het binnendringen van een geautomatiseerd werk de verdachte niet op de hoogte raakt van het feit dat de politie interesse in hem of haar heeft. Deze leden hebben gevraagd of zij het goed begrijpen dat de regering de voorgestelde bevoegdheid tot heimelijk binnendringen beschouwt als een uitgebreide vorm van observatie of dat het hier om een digitale vorm van huiszoeking gaat. In dat laatste geval is de verdachte er wel van op de hoogte dat onderzoek plaatsvindt.
De voorgestelde bevoegdheid vertoont nauwe samenhang met de bestaande bevoegdheden tot doorzoeking ter vastlegging van gegevens. Afhankelijk van de specifieke onderzoekshandeling met het oog waarop de voorgestelde bevoegdheid wordt ingezet, vertoont de wettelijke regeling overeenkomsten met de bestaande regeling voor de betreffende onderzoekshandelingen. Voor zover het doel van het onderzoek is gelegen in het ontoegankelijk maken van gegevens (artikel 126cc, vijfde en zesde lid, Sv), het aftappen en opnemen van communicatie op het opnemen van vertrouwelijke communicatie (artikelen 126l, 126m, 126s, 126t, 126zf, 126zg Sv) en de stelselmatige observatie (artikelen 126g, 126o, 126zd Sv), zijn voornoemde bepalingen over de inzet van deze bijzondere opsporingsbevoegdheden van toepassing. Via plaatsing van de bevoegdheid in Titel IVA van het Eerste Boek Wetboek van Strafvordering wordt bereikt dat er, in verband met het heimelijke karakter van de bevoegdheid, ruimere rechtswaarborgen van toepassing zijn. Daarvoor kan worden gewezen op de notificatieplicht, de voeging van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen die verschoningsgerechtigden raken.

De leden van de D66-fractie hebben tevens gevraagd of door introductie van de bevoegdheid de positie van de verdachte wijzigt, omdat al onderzoek naar een verdachte kan plaatsvinden voordat hij of zij hiervan op de hoogte is en voordat hij of zij in staat van beschuldiging is gesteld. Deze leden wensten te vernemen wat dit betekent voor de verdediging van de verdachte, hoe de rechtspraak hier naar verwachting mee om zal gaan en of dit niet dermate ingrijpend is dat dit meegenomen moet worden bij de vaststelling van de contouren van het modernisering van het Wetboek van Strafvordering.
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, zoals de leden van de D66-fractie lijken te veronderstellen, is

derhalve geen sprake. De inzet van de bevoegdheid tot het op afstand binnendringen met het oog op het verrichten van onderzoekshandelingen in een geautomatiseerd werk is mogelijk als er sprake is van 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 bijzondere opsporingsbevoegdheden met een heimelijk karakter als de infiltratie (artikelen 126h, 126p en 126ze Sv), het direct afluisteren (artikelen 126l, 126s, en 126zf) of het vorderen van bijzondere persoonsgegevens, zoals gegevens over iemand godsdienst of levensovertuiging, ras of politieke gezindheid (artikelen 126nf, 126uf en 126zn, tweede lid, Sv). In het geval het geautomatiseerde werk wordt binnengedrongen met het oog op het veiligstellen of ontoegankelijk maken van gegevens geldt 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.
Op de rechtswaarborgen die van toepassing zijn, is in het antwoord op de vorige vraag van de leden van deze fractie ingegaan.
In het kader van de modernisering van het Wetboek van Strafvordering wordt de regeling van de opsporingsbevoegdheden vereenvoudigd en worden knelpunten in de praktijk weggenomen. De uitgangspunten van de huidige regeling worden uitdrukkelijk niet gewijzigd (Kamerstukken II 2015/16, 29 279, nr. 278, paragraaf 2.2.7).

De leden van de D66-fractie hebben gevraagd hoe het wetsvoorstel zich verhoudt tot de nieuwe Wet op de inlichtingendiensten en de nieuwe Wet bewaarplicht telecomgegevens en in hoeverre sprake is van overlap tussen deze wetsvoorstellen omdat zij voorzien in vergelijkbare bevoegdheden.
De door de leden van de D66-fractie genoemde (nieuwe) bevoegdheden verschillen voor wat betreft het doel waarvoor zij kunnen ingezet. De voorgestelde bevoegdheid tot het op afstand binnendringen van een geautomatiseerd en het verrichten van onderzoekshandelingen en de bevoegdheid tot het vorderen van bewaarde telecomgegevens zijn beide strafvorderlijke bevoegdheden, die kunnen worden ingezet in geval van verdenking van een ernstig strafbaar feit. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) beschikken al geruime tijd over de bevoegdheid tot het binnendringen in een geautomatiseerd werk (artikel 24 Wiv 2002). Deze bevoegdheid kan uitsluitend worden ingezet voor de uitoefening van de wettelijke taken van de diensten in het belang van de nationale veiligheid. Het doel waarvoor de bevoegdheid kan worden ingezet is dan ook verschillend. Er kan vanuit deze optiek bezien dan ook niet gesproken worden van een overlap tussen beide wetsvoorstellen.
Overigens wordt opgemerkt dat de reikwijdte van de bevoegdheid in de strafvorderlijke sfeer beperkter is dan die in de sfeer van de inlichtingen- en veiligheidsdiensten. Zo wordt in het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten onder meer voorzien in de mogelijkheid tot het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten en de bevoegdheid om via het geautomatiseerde werk van een derde in het geautomatiseerde werk van het onderzoekssubject binnen te dringen.
Eén van de onderzoekshandelingen waarvoor de voorgestelde bevoegdheid in het Wetboek van Strafvordering kan worden ingezet is de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen. Het huidige Wetboek van Strafvordering biedt verschillende bevoegdheden om gegevens die op een geautomatiseerd werk zijn opgeslagen vast te leggen, al dan niet met behulp van de

aanbieder van een telecommunicatiedienst. Op grond van het voorgestelde artikel 126n Sv in het wetsvoorstel bewaarplicht telecomgegevens (Kamerstukken II 2015/16 34 537, nr 2), dat dient ter vervanging van het thans buiten werking gestelde artikel 126n Sv dat een vergelijkbare bevoegdheid bevatte, kan de officier van justitie historische telecommunicatiegegevens (verkeersgegevens en gebruikersgegevens) vorderen van de aanbieder van een telecommunicatiedienst.
De bestaande mogelijkheden in het Wetboek van Strafvordering om gegevens te kunnen vastleggen, al dan niet met behulp van de aanbieder, volstaan niet altijd omdat steeds vaker gebruik wordt gemaakt van versleuteling, de geautomatiseerde werken een onderdeel vormen van een netwerk of de gegevens worden opgeslagen in de cloud. Het gebruik van cloudcomputingdiensten kan voorts leiden tot onduidelijkheid over de vraag wie als aanbieder in de zin van de Telecommunicatiewet kan worden aangemerkt. Als een verlener van webdiensten niet als aanbieder kan worden aangemerkt, kan geen bevel tot medewerking worden gegeven. De opsporing heeft behoefte aan de mogelijkheid om heimelijk toegang te kunnen krijgen tot gegevens die zijn opgeslagen, zonder dat de verdachte of aanbieder daarbij betrokken is. Het vereiste van het dringend onderzoeksbelang brengt mee dat het heimelijk binnendringen van een geautomatiseerd werk en het verrichten van onderzoekshandelingen alleen toegepast wordt als andere opsporingsbevoegdheden tekort schieten. De officier van justitie zal in het bevel feiten en omstandigheden moeten opnemen, op grond waarvan de rechter commissaris kan toetsen of aan dit vereiste is voldaan.

De leden van de D66-fractie hebben gevraagd hoe wordt voorkomen dat bij het binnendringen van een geautomatiseerd werk ook inzage ontstaat in communicatie van andere niet-verdachte personen. Deze leden hebben tevens gevraagd hoe wordt gewaarborgd dat de heimelijke inbreuk alleen plaatsvindt op de desbetreffende persoon waarvoor via de rechter-commissaris een machtiging is afgegeven en of de regering het überhaupt mogelijk acht de kring van personen die het zou kunnen betreffen te beperken.
Niet kan worden uitgesloten dat bij het onderzoek in een geautomatiseerd werk inzage ontstaat in communicatie van andere, niet-verdachte personen. Dit is thans niet anders bij de toepassing van bevoegdheden als het aftappen van communicatie of het direct afluisteren. Wel zijn de wettelijke voorwaarden voor de uitoefening zodanig dat zoveel mogelijk wordt voorkomen dat de opsporing in aanraking komt met gegevens van derden. Dit betreft ten eerste het vereiste dat het geautomatiseerde werk bij de verdachte in gebruik is. In het bevel van de officier van justitie dient te worden vermeld welke deel van het geautomatiseerde werk op afstand wordt binnengedrongen, de aard van de software die wordt gebruikt, de functies van de software die worden ingeschakeld en de categorie van gegevens waar het onderzoek betrekking op heeft. Doordat uitsluitend de gegevens die binnen de reikwijdte van het bevel van de officier vallen ter beschikking kunnen komen van de opsporing, worden de gegevens van derden zoveel mogelijk beschermd.

De leden van de D66-fractie hebben in het wetsvoorstel gelezen dat met behulp van deze bevoegdheid het geautomatiseerde werk of de gebruiker kan worden geïdentificeerd ten behoeve van een meer gericht bevel tot het aftappen en opnemen van communicatie en hebben de indruk dat in eerste instantie met een sleepnetmethode wordt gewerkt en pas daarna meer gerichte onderzoeksmethoden plaatsvinden. Zij hebben gevraagd of die veronderstelling klopt.
In reactie op deze vraag moet voorop worden gesteld dat de toepassing van andere bijzondere opsporingsbevoegdheden niet is beperkt tot een verdachte. Voor de toepassing van bijzondere opsporingsbevoegdheden,

zoals de observatie (art. 126g Sv), het stelselmatig inwinnen van informatie (art. 126j Sv) of het aftappen van telecommunicatie (art. 126m Sv), is een verdenking van een misdrijf vereist. Voor het aftappen betreft dit een ernstige misdrijf, waarvoor voorlopige hechtenis mogelijk is. Het is echter niet uitgesloten dat voormelde bevoegdheden jegens anderen dan de verdachte worden ingezet, wanneer dit van belang is voor de waarheidsvinding. Voor de voorgestelde bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk is echter wel als nadere beperking gesteld dat het geautomatiseerde werk bij de verdachte in gebruik is. Niet is vereist dat de verdachte de enige gebruiker is. Het is derhalve niet bij voorbaat uitgesloten dat het onderzoek in een geautomatiseerd werk, dat bij de verdachte in gebruik is, ook gegevens van anderen in beeld komen.
De veronderstelling van de leden van deze fractie, dat in eerste instantie met een sleepnetmethode wordt gewerkt, is niet juist. De voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk kan uitsluitend worden uitgeoefend in geval van verdenking van een ernstig misdrijf dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. De wettelijke voorwaarde van de verdenking van betrokkenheid van een persoon bij een ernstig strafbaar feit staat in de weg aan de inzet van deze bevoegdheid in de vorm van een zogenaamde sleepnetmethode.
Daarnaast moet tevoren duidelijk zijn naar welke gegevens wordt gezocht, dit moet in het bevel van de officier van justitie worden opgenomen.
Vanwege de functiescheiding wordt het onderzoek in een geautomatiseerd werk uitgevoerd door speciaal daarvoor opgeleide opsporingsambtenaren die niet betrokken zijn bij het betreffende opsporingsonderzoek.
Voor het binnendringen en verzamelen van gegevens wordt doorgaans gebruik gemaakt van speciale software die is afgeregeld op de specifieke gegevens waarnaar wordt gezocht. Het is dan niet heel waarschijnlijk dat gegevens van andere gebruikers, als deze geen verband hebben met de gegevens waarnaar wordt gezocht ten behoeve van het opsporingsonderzoek, worden verzameld en vastgelegd. In die gevallen waarin dat wel zo zou zijn ligt het voor de hand dat deze gegevens worden gewist omdat deze niet van belang zijn voor het betreffende opsporingsonderzoek. Het wetsvoorstel bevat dan ook verschillende waarborgen die voorkomen dat deze wet leidt tot een «dragnet», waar ook de omgeving van de verdachte in meegetrokken wordt.

De leden van de D66-fractie hebben geconstateerd dat niet alleen de politie de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk krijgt, maar ook de Koninklijke Marechaussee en de bijzondere opsporingsdiensten, zoals de FIOD/ECD. De leden van deze fractie hebben gevraagd of de regering kan toelichten waarom al deze organisaties deze vergaande bevoegdheid nodig hebben, en wat voor soort misdrijven deze bijzondere opsporingsdiensten bestrijden waarvoor deze bevoegdheid nodig is.
Voor het antwoord op de vraag waarom de Koninklijke marechaussee en de bijzondere opsporingsdiensten, zoals de FIOD, deze bevoegdheid krijgen wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de PvdA fractie over de mogelijkheid dat ook bijzondere opsporingsdiensten de mogelijkheid krijgen van de nieuwe bevoegdheid gebruik te maken.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten wat voor misdrijven onder «ernstige vormen van fraude en witwassen» of «omvangrijke milieumisdrijven» vallen.
Ernstige vormen van fraude zullen doorgaans gepaard gaan met het beramen of plegen van strafbare feiten als valsheid in geschrift, waarvoor een gevangenisstraf van ten hoogste zes jaren kan worden opgelegd (art.

225, eerste lid, Sr), ambtelijke corruptie, waarvoor een gevangenisstraf van zes jaren kan worden opgelegd (art. 363 Sr), of bedrieglijke bankbreuk (art. 341 Sr.) waarvoor een gevangenisstraf van ten hoogte zes jaren kan worden opgelegd. Een ernstige vorm van witwassen betreft het gewoontewitwassen, waarvoor een gevangenisstraf van ten hoogste zes jaren mogelijk is (art. 420bis, eerste lid, Sr). Omvangrijke milieumisdrijven zullen doorgaans gepaard gaan met het beramen of plegen van strafbare feiten als het opzettelijk verontreinigen van de bodem, de lucht of het oppervlaktewater, waarvoor een gevangenisstraf van ten hoogste twaalf jaren kan worden opgelegd (art. 173a Sr), al dan niet in combinatie met de eerdergenoemde strafbare feiten als valsheid in geschrift en ambtelijke corruptie. In deze gevallen is het ook mogelijk dat de daders zich schuldig maken aan deelneming aan een criminele organisatie, waarvoor een gevangenisstraf van ten hoogste zes jaar kan worden opgelegd (art. 140, eerste lid, Sr).

De leden van de ChristenUnie-fractie hebben gevraagd naar de reikwijdte van de term geautomatiseerd werk. Deze leden meenden dat de noodzaak van een brede reikwijdte van dit begrip nadere onderbouwing vraagt en hebben gevraagd om een reactie van de regering hierop.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de SP-fractie over welke geautomatiseerde werken op dit moment onder de reikwijdte van het begrip geautomatiseerd werk vallen.

De leden van de GroenLinks-fractie hebben gevraagd hoe de introductie van een hackbevoegdheid zich verhoudt tot de rechtsstatelijke uitgangspunten. Deze leden van deze fractie hebben tevens gevraagd in hoeveel gevallen in de afgelopen vijf jaar zo'n hackbevoegdheid had kunnen worden ingezet en waarom bestaande dwangmiddelen en bevoegdheden te kort schoten. Deze leden hebben voorts gevraagd hoeveel en welke zaken zijn misgegaan door het ontbreken van deze onderzoeksbevoegdheid. Zij zouden graag een nauwgezet overzicht ontvangen.
Op de verhouding van de voorgestelde bevoegdheid met de rechtsstatelijke uitgangspunten wordt verderop nader ingegaan, naar aanleiding van vragen van de fracties over de bescherming van grondrechten (paragraaf 2.9). 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 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 en welke zaken zijn misgegaan vanwege het ontbreken van deze bevoegdheid. Het is helaas dan ook niet mogelijk het nauwgezette overzicht, waar door de leden van deze fractie om is verzocht, te verstrekken.

De leden van de PvdD-fractie hebben vastgesteld dat het wetsvoorstel het mogelijk maakt dat de politie op grote schaal met internet verbonden apparaten mag hacken. Bij hacken worden apparaten via zwakheden in de software binnengedrongen. De leden van deze fractie hebben gewezen op het gevaar van bugs die het mogelijk maken op grote schaal persoonsgegevens te stelen en die met het voorliggende wetsvoorstel juist gebruikt zouden worden door de politie. Deze leden hebben gevraagd of de regering het acceptabel vindt dat de veiligheid van miljoenen apparaten aangetast wordt, alles in dienst van de hackbevoegdheid van de politie, of de regering uiteen kan zetten welke afweging is gemaakt tussen de het belang van de veiligheid van burgers tegenover de opsporingsbehoeften van de politie en waar de prioriteit is gelegd. Graag ontvingen zij een reactie hierop van de regering.

Voor het antwoord op deze vragen verwijs ik naar de afwegingen zoals die uiteen zijn gezet in de eerdergenoemde brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de PvdD-fractie zijn geschrokken van de breedte van het in het wetsvoorstel gehanteerde begrip geautomatiseerd werk en meenden dat het niet de bedoeling kan zijn dat de regering doelbewust zwakheden in pacemakers niet zal melden, waardoor deze ook door kwaadwillende hackers aangetast kunnen worden. Zij hebben gevraagd of de regering bereid is de wet aan te passen en specifiek aan te geven welke apparaten wel en niet gehackt mogen worden.
Voor het antwoord op de vraag over de reikwijdte van het begrip geautomatiseerd werk wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de SP-fractie. Voor de afwegingen over het gebruik en het melden van onbekende kwetsbaarheden verwijs ik naar de eerdergenoemde brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.
Daarnaast zal ik ingaan op het specifieke voorbeeld dat door de PvdD-fractie genoemd wordt. Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. Hoewel een pacemaker onder de definitie van geautomatiseerd 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 zwaar wegend belang voordoet dat het door de PvdD gesuggereerde binnentreden van een pacemaker proportioneel zou worden geacht.

De leden van de PvdD-fractie hebben opgemerkt dat het wetsvoorstel niet is beperkt tot cybercriminaliteit en de politie feitelijk een oncontroleerbare hackbevoegdheid geeft om in alle met internet verbonden apparaten in te kunnen breken bij verdenking van een misdrijf. Zij hebben gevraagd of de regering bereid is expliciet aan te geven welk misdrijf wel en welk misdrijf niet in aanmerking zal komen om onder de wet te kunnen vallen en hier harde criteria voor op te stellen.
De regering is van oordeel dat het wetsvoorstel voldoende waarborgen bevat om tegemoet te komen aan de zorg van de PvdD-fractie dat de politie feitelijk een oncontroleerbare bevoegdheid tot inbreken zou verkrijgen. In de eerste plaats is het niet de politie maar de officier van justitie die de beslissing kan nemen dat het wenselijk is dat op afstand wordt binnengedrongen in een geautomatiseerd werk. De officier kan hierover niet zelfstandig beslissen maar heeft een machtiging nodig van de rechter-commissaris. Er is dus een voorafgaande rechterlijke toetsing voorzien. In de tweede plaats is het onderzoek in een geautomatiseerd werk beperkt tot bepaalde onderzoekshandelingen, dit betreft enerzijds de toepassing van bestaande bevoegdheden zoals het aftappen van telecommunicatie of het direct afluisteren. In deze gevallen is het binnendringen voorwaardelijk om de bestaande opsporingsbevoegdheid te kunnen uitoefenen. Het aftappen van telecommunicatie is mogelijk voor misdrijven waarvoor voorlopige hechtenis mogelijk is, binnen deze kring van misdrijven is nadere inperking onwenselijk omdat dit de opsporing bij voorbaat zal belemmeren; het aftappen van telecommunicatie is een buitengewoon nuttig middel voor de opsporing van ernstige misdrijven. Het onderzoek in een geautomatiseerd werk betreft anderzijds nieuwe bevoegdheden, zoals het vastleggen of ontoegankelijk maken van gegevens. Naar aanleiding van het advies van de Afdeling advisering van

de Raad van State is voor deze bevoegdheden een nadere beperking opgenomen, namelijk dat het een zeer ernstig misdrijf moet betreffen, waarop een gevangenisstraf van acht jaar of meer is gesteld of dat bij algemene maatregel van bestuur is aangewezen. Naar het oordeel van de regering worden hiermee voldoende waarborgen geboden voor een zorgvuldige toepassing in de praktijk.

De leden van de PvdD-fractie hebben zich afgevraagd hoe het zit met de huisgenoten van de verdachte omdat een computer niet alleen gegevens van de persoon zelf bevat maar ook van vrienden, familie en netwerken. Zij hebben gevraagd welke waarborgen de wet geeft dat hun privacy niet aangetast wordt en hoe de regering voorkomt dat de wet leidt tot een «dragnet», waar ook de omgeving van een verdachte in meegetrokken wordt.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de D66-fractie over het werken met een sleepnetmethode.

De leden van de PvdD-fractie hebben vraagtekens gezet bij de bredere inzet van het wetsvoorstel als efficiencymiddel, en hebben gevraagd wat de implicatie is van de financiële paragraaf, waarin staat dat kosten kunnen worden bespaard omdat de voorgestelde bevoegdheid andere bevoegdheden kan vervangen. Deze leden hebben tevens gevraagd of deze bevoegdheid ook in andere domeinen kan worden toegepast en of de regering de mening deelt dat efficiency nooit een drijfveer zou mogen zijn als het gaat om de grondrechten en privacy van burgers.
Steeds meer informatie over en bewijs voor strafbare feiten bestaat alleen nog maar in digitale vorm, en is vaak alleen via het internet te benaderen. In dergelijke gevallen is de inzet van bestaande opsporingsmethoden niet toereikend of niet mogelijk. Dat geldt onder meer in gevallen waarin technisch capabele criminelen gebruik maken van geavanceerde technieken om buiten het bereik van de opsporing te blijven. Voor de noodzaak van het wetsvoorstel verwijs ik naar het antwoord op vraag 1. De inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk kan in bepaalde gevallen voldoende informatie opleveren, zodat aanvullende inzet van andere bevoegdheden niet meer nodig is of kan worden beperkt. Uiteraard wordt de inzet altijd getoetst aan de beginselen van proportionaliteit en subsidiariteit.

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

Naar aanleiding van een reactie van de ANWB hebben de leden van de PvdA-fractie gevraagd of tot een geautomatiseerd werk ook een «connected car» of connecties infotainment met de daarbij behorende servers behoren en zo ja, of de politie daarmee op grond van het voorliggende wetsvoorstel de bevoegdheid krijgt op afstand en heimelijk een dergelijk geautomatiseerd werk te onderzoeken.
Hierboven is, in antwoord op vragen van de SP-fractie, reeds ingegaan op de reikwijdte van het begrip geautomatiseerd werk. Voor zover de in een voertuig aanwezige apparaten voldoen aan de definitie van het begrip geautomatiseerd werk, zoals deze ook in het Cybercrimeverdrag wordt gehanteerd, kunnen deze in theorie op afstand worden binnengedrongen als in die apparaten gegevens zijn of worden verwerkt die van belang zou zijn voor de opsporing van ernstige strafbare feiten. Een voorbeeld betreft een navigatiesysteem, dat informatie kan bevatten over de route of verblijfplaats van een voertuig. Het behoeft nauwelijks betoog dat dergelijke informatie zeer waardevol kan zijn voor de opsporing van ernstige strafbare feiten, zoals een liquidatie. Dit voorbeeld toont aan dat het bij voorbaat niet eenvoudig is beperkingen aan te brengen in het type

geautomatiseerd werk, omdat de techniek niet stil staat en de creativiteit van de misdaad helaas weinig grenzen kent.
In het algemeen is het niet wenselijk specifieke apparaten van de bevoegdheid uit te sluiten. Eén van de doelen van de wet is het verbeteren van de mogelijkheden om cybercriminelen op te sporen en bewijs te vergaren. Het aanwijzen van een specifieke categorie apparaten waar de bevoegdheid niet voor kan worden toegepast, zou betekenen dat cybercriminelen die deze apparaten voor criminele doeleinden gebruiken niet effectief kunnen worden aangepakt en het strafbaar feit onvoldoende kan worden onderzocht. Wel kan de aard van het geautomatiseerde werk reden zijn voor grote terughoudendheid bij de inzet, of bepalend zijn voor het besluit tot de inzet of juist het afzien daarvan.
Deze leden hebben tevens gevraagd of de politie deze bevoegdheid of eventueel een andere bevoegdheid mag gebruiken om een voertuig staande te houden en zo ja, wat de politie mag doen om het voertuig op afstand te stoppen, waar dat in de wet of onderlinge regelgeving is vastgelegd en hoe die bevoegdheid zich verhoudt tot de veiligheid van verkeersdeelnemers.
De bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk is gekoppeld aan het uitvoeren van bepaalde onderzoekshandelingen. Dit betreft het aftappen van telecommunicatie, het direct afluisteren, de observatie, het vastleggen van gegevens en het ontoegankelijk maken van gegevens. Het op afstand laten stoppen van een voertuig is hieronder mogelijk te begrijpen, als een vorm van het ontoegankelijk maken van gegevens. Deze bevoegdheid vormt thans reeds onderdeel van het wetboek van Strafvordering (art. 125o Sv) en strekt tot het ontoegankelijk maken van gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Deze bevoegdheid wordt toegepast om te voorkomen dat de beheerder van dat geautomatiseerd werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens (Kamerstukken II 1998/99, 26 671, nr. 3. blz. 21). Het toepassen van deze bevoegdheid voor het stoppen van een voertuig ligt niet voor de hand, vanwege het beperkte verband tussen de gegevens van een boordcomputer van een voertuig en het plegen van een strafbaar feit. Bovendien vormen de gegevens van een boordcomputer geen gegevens waarvan het bezit of de verspreiding minder wenselijk is vanuit het oogpunt van het belang van de bescherming van slachtoffers of van kwetsbare groepen in de samenleving. Het is dan ook niet waarschijnlijk dat een officier van justitie of een rechter-commissaris hiervoor een bevel respectievelijk een machtiging zullen afgeven. Dit betekent overigens niet dat de politie niet bevoegd zou zijn om een voertuig op afstand te stoppen. Als de overvaller van een bankoverval met een voertuig vluchten, dan zal de politie – als een stopteken geen resultaat heeft – kunnen proberen het voertuig klem te rijden of op andere wijze tot stilstand te brengen. Hiervoor kan worden gedacht aan een wegafzetting of -blokkade of het gebruik van spijkerstrips. Deze bevoegdheid vloeit voort uit de bevoegdheid van de opsporingsambtenaar tot aanhouding van de verdachte in geval van ontdekking op heterdaad van een strafbaar feit (art. 53, eerste lid, Sv) dan wel buiten het geval van heterdaad bij een strafbaar feit waarvoor voorlopige hechtenis is toegelaten (art. 54, eerste lid, Sv).

De leden van de CDA-fractie hebben de regering gevraagd dieper in te gaan op de keuze het binnendringen van een geautomatiseerd werk als bijzondere opsporingsbevoegdheid aan te merken en of voor alle bijzondere opsporingsbevoegdheden geldt dat dit heimelijk gebeurt. Daarbij hebben zij verzocht in te gaan op de situatie dat de verdachte bij de toepassing van de bevoegdheid lucht krijgt van het ingrijpen door

politie en justitie en of dan het argument vervalt om veel zwaardere voorwaarden te stellen aan de toepassing daarvan.
De Afdeling advisering heeft erop gewezen dat de essentie van de voorgestelde bevoegdheid is dat de voorgestelde bevoegdheid heimelijk wordt uitgeoefend, zonder dat de verdachte daar kennis van krijgt, en daarom in de kern samenhang vertoont met de bijzondere opsporingsbevoegdheden die zijn vervat in Titel IVA van het Eerste Boek Sv. De voorgestelde bevoegdheid past derhalve minder goed bij de regeling van de bijzondere dwangmiddelen (Titel IV van het Eerste Boek Sv), die niet heimelijk worden toegepast. Bij de toepassing van bijzondere opsporingsbevoegdheden zijn meer rechtswaarborgen van toepassing dan bij Titel IV het geval is, waarbij door de Afdeling advisering wordt gewezen op de ruimere notificatieplicht, de voeging van processen-verbaal bij de processtukken en de vernietiging van processen-verbaal of andere voorwerpen die verschoningsgerechtigden raken.
Naar aanleiding van dit advies is de voorgestelde bevoegdheid opgenomen in de Titels IVa, V en VB Sv. Deze titels beslaan de bijzondere bevoegdheden tot opsporing, inclusief het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband, en de opsporing van terroristische misdrijven. Deze keuze heeft tot gevolg dat de bevoegdheid ruimer kan worden ingezet, niet alleen in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten maar ook in geval uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven, waarvoor voorlopige hechtenis is toegelaten, 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 (art. 126o Sv), en in geval van aanwijzingen van een terroristisch misdrijf (art. 126zd Sv). Voor alle bijzondere opsporingsbevoegdheden geldt dat deze heimelijk worden toegepast, dat wil zeggen zonder dat de betrokkene daarvan kennis heeft. Als de verdachte lucht krijgt van de toepassing van een bijzondere opsporingsbevoegdheid dan zal hij zijn gedrag aanpassen en/of informatie die van belang kan zijn voor het bewijs van strafbare feiten proberen te vernietigen of anderszins te laten verdwijnen. Voortzetting van de inzet van de bevoegdheid is dan weinig zinvol, zodat ook de voorwaarden waaronder die voortzetting zou kunnen plaatsvinden minder relevant zijn. Daarnaast zijn de voorwaarden voor de inzet van de voorgestelde bevoegdheid niet zwaarder dan die welke oorspronkelijk werden voorgesteld in het conceptwetsvoorstel dat in consulatie is gegeven. In dat voorstel was de voorgestelde bevoegdheid opgenomen in Titel IV («Enige bijzondere dwangmiddelen»).

De leden van de CDA-fractie hebben met betrekking tot de verschoningsregeling gevraagd hoe in de praktijk bepaald wordt dat er sprake van een geheimhoudingsrelatie. Zij hebben opgemerkt dat in het bijzonder de relatie met een geestelijke vragen kan oproepen en gevraagd of hieronder ook een imam geschaard kan worden. Ook hebben zij gevraagd of chatgesprekken en/of emailuitwisselingen tussen een radicaliserende verdachte en een zogeheten haatprediker hieronder vallen. Ten slotte hebben zij gevraagd of de regering de mening deelt dat het in dat kader gewenst is dat dergelijke informatie inzichtelijk wordt voor politie en justitie en zo ja, hoe zij gaat dat in onderhavig wetsvoorstel hiervoor een uitzondering wordt gecreëerd. Zo nee, waarom niet gelet op de Actieplan Jihadisme.
Het verschoningsrecht van getuigen met een geheimhoudingsplicht is in het Wetboek van Strafvordering geregeld in artikel 218 Sv. In dit artikel is bepaald dat personen zich kunnen verschonen «die uit hoofde van hun stand, hun beroep of hun ambt tot geheimhouding verplicht zijn». Dit betreft de zogenoemde professioneel verschoningsgerechtigden. Het is aan de rechter om invulling te geven aan de open norm van artikel 218 Sv.

Op grond van de wetsgeschiedenis en de jurisprudentie van de Hoge Raad kan worden aangenomen dat ook geestelijken een beroep kunnen doen op het wettelijke verschoningsrecht. Het vereiste dat op gronden van algemeen belang het onbelemmerd beroep op een bepaalde groep geestelijken moet prevaleren boven de waarheidsvinding in rechte, moet zo worden ingevuld dat de voorgangers van religieuze stromingen een beroep kunnen doen op het verschoningsrecht. Het verschoningsrecht komt dus toe aan de dominee, pastoor, imam en voorganger van de pinkstergemeente (Wetboek van Strafvordering, suppl. 136, art. 218, aant. 9.4). Aldus zou, op grond van de wetsgeschiedenis, de jurisprudentie van de Hoge Raad en de interpretatie van de reikwijdte van het wettelijke verschoningsrecht in de wetenschap, ook een imam in beginsel een beroep kunnen doen op het wettelijk verschoningsrecht.
Van belang is dat het professioneel verschoningsrecht zich niet over alle activiteiten van de verschoningsgerechtigde uitstrekt. Het verschoningsrecht is beperkt tot die informatie die onder een geheimhoudingsplicht valt en aan de verschoningsgerechtigde als zodanig is toevertrouwd. De informatie die niet in het kader van advies of bijstand aan de vertrouwenspersoon bekend wordt, valt dus niet onder het wettelijke verschoningsrecht. De uitingen van een haatprediker die niet vertrouwelijk worden gedaan, zoals tijdens een openbare gebedssamenkomst of een preek in een moskee, zullen niet onder het wettelijke verschoningsrecht vallen.
Ten aanzien van chatgesprekken en/of mailwisselingen geldt dat zij onder het bereik van het verschoningsrecht kunnen vallen, voor zover zij vallen binnen het hierboven geduide vertrouwelijke verkeer. Het verschoningsrecht is evenwel niet absoluut. Allereerst kunnen gegevens die voorwerp van het strafbare feit uitmaken («corpora delicti») of tot het plegen daarvan hebben gediend («instrumenta delicti»), achteraf inbeslaggenomen worden (art. 98, vijfde lid, Sv).
Bovendien kan het verschoningsrecht in zeer uitzonderlijke omstandigheden worden doorbroken, waardoor gegevens alsnog in beslag genomen kunnen worden. Van zeer uitzonderlijke omstandigheden kan onder meer sprake zijn als de verschoningsgerechtigde zelf verdacht wordt van ernstige strafbare feiten.[1] Ook ten aanzien van bijzondere opsporingsbevoegdheden geldt dat de informatie aan het procesdossier toegevoegd mag worden als de verschoningsgerechtigde zelf verdachte is.[2]
In het geval dat een haatprediker zou oproepen tot deelname aan de jihad is het dus niet uitgesloten dat de emails of chatgesprekken die daarop betrekking hebben worden aangemerkt als corpora en instrumenta of dat de prediker zelf als verdachte worden aangemerkt van het beramen of plegen van bepaalde strafbare feiten, zoals de opruiing (art. 131 Sr), waardoor mogelijk sprake is van een doorbrekingsgrond. Het bestaande recht stelt dus al beperkingen aan het verschoningsrecht, waardoor informatie die wordt gewisseld met een verschoningsgerechtigde in voorkomende gevallen waarin de verschoningsgerechtigde zelf kwade bedoelingen heeft, in strafzaken gebruikt kan worden.

De leden van de CDA-fractie hebben gevraagd hoe voorkomen gaat worden dat het verschoningsrecht wordt misbruikt door kwaadwillenden als een map op de harde schijf van een personal computer «medisch dossier» of «gesprekken met mijn advocaat» wordt genoemd, de seinen voor politie en justitie direct op rood staan of dat zij wel degelijk verder mogen zoeken naar de informatie die hierachter ligt. Daarbij hebben zij gevraagd hoe bovenstaande aandachtspunten worden verwerkt in het aangekondigde Besluit bewaren en vernietigen niet-gevoegde stukken.

---

[1] Zie bijvoorbeeld HR 19 mei 2009, NJ 2009/443.
[2] Zie Kamerstukken II 1996/97, 25 403, nr. 3, blz. 61 en nr. 7, blz. 77.

De naamgeving «medisch dossier» of «gesprekken met mijn advocaat» van een map op een computer kan aanleiding geven om te doen vermoeden dat de gegevens in die map onder het verschoningsrecht vallen. Indien twijfel bestaat over of de gegevens daadwerkelijk onder het verschoningsrecht vallen of wanneer er vermoedelijk een doorbrekingsgrond is, kan de officier van justitie overeenkomstig artikel 126aa, tweede lid, derde volzin, Sv de gegevens voorleggen aan de rechter-commissaris. Wanneer die oordeelt dat de gegevens niet onder het verschoningsrecht vallen (bijvoorbeeld omdat ondanks de naam «medisch dossier» een map helemaal geen gegevens bevat die onder het medisch beroepsgeheim vallen) of er een doorbrekingsgrond van toepassing is (bijvoorbeeld omdat de verschoningsgerechtigde zelf ook (mede)verdachte is), kunnen de gegevens in het opsporingsonderzoek worden gebruikt.

De leden van de CDA-fractie hebben tevens gevraagd of de regering het medisch beroepsgeheim afdoende kan borgen en bewaken, ook en juist als de verschoningsgerechtigden zelf verdachten zijn.
In verband met hun medisch beroepsgeheim hebben ook artsen een professioneel verschoningsrecht op grond van artikel 218 Sv. Het verschoningsrecht waarborgt dat het medisch beroepsgeheim in beginsel ook ten opzichte van politie en justitie wordt beschermd. Zoals hierboven, naar aanleiding van andere vragen van de CDA-fractie met betrekking tot de verschoningsregeling aan de orde is gekomen, is het wettelijke verschoningsrecht evenwel geen absoluut recht, omdat het op grond van zwaarwegende maatschappelijke belangen door de rechter kan worden doorbroken. Voor de beoordeling van de vraag of sprake is van zeer uitzonderlijke omstandigheden die een doorbreking van het verschoningsrecht rechtvaardigen, heeft de Hoge Raad in zijn jurisprudentie maatstaven ontwikkeld (Vgl. HR 26 mei 2009, NJ 2009/263 en HR 28 februari 2012, NJ 2012/537). Naast de vraag of de verschoningsgerechtigde zelf verdachte is, spelen ook andere factoren een rol, zoals de aard, omvang en context van de gegevens, het belang van de strafzaak, het belang van de gegevens en de vraag in hoeverre belanghebbenden (patiënten) toestemming hebben gegeven voor het gebruik van de gegevens. Het gaat om een belangenafweging, waarbij het moet gaan om zwaarwegende maatschappelijke belangen. De doorbreking mag niet verder gaan dan strikt noodzakelijk is, juist vanwege het belang dat door de geheimhoudingsplicht beschermd wordt. Dit kan er bijvoorbeeld toe leiden dat alleen een beperkt aantal gegevens of alleen geanonimiseerde gegevens in de strafzaak gebruikt mogen worden.

De leden van de D66-fractie hebben grote vraagtekens geplaatst bij het brede toepassingsterrein en hebben de regering gevraagd een overzicht te geven van alle soorten misdrijven waarvoor de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruikt kan worden. Ook hebben zij gevraagd waarom niet is gekozen voor een gesloten lijst van delicten en, gezien de ingrijpendheid van de bevoegdheid, een beperking tot levensbedreigende en terroristische delicten.
Zoals in de memorie van toelichting uiteen gezet is, in lijn met het advies van de Afdeling advisering van de Raad van State, ervoor gekozen om de voorwaarden voor de inzet van de bevoegdheid tot heimelijk binnendringen in een geautomatiseerd werk te differentiëren naar de mate waarin een inbreuk gemaakt wordt op de persoonlijke levenssfeer. Dit heeft tot gevolg dat het binnendringen van een geautomatiseerd werk met het oog op de het vaststellen van bepaalde kenmerken van het geautomatiseerde werk, het opnemen van communicatie of vertrouwelijke communicatie en de stelselmatige observatie mogelijk is als er sprake is van 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. Het gaat hier om alle misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld (onderdeel a) en de specifiek in de in de onderdelen b en c aangewezen misdrijven.
In het geval het geautomatiseerde werk wordt binnengedrongen voor doelen waarbij de mate waarin inbreuk gemaakt wordt op de persoonlijke levenssfeer ingrijpender is, zoals het vastleggen of ontoegankelijk maken van gegevens, geldt een zwaarder verdenkingscriterium. In dergelijke gevallen 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 misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld zijn alle zeer ernstige delicten met ingrijpende gevolgen zoals de deelneming aan een terroristische organisatie (art. 140a Sr), het maken van een beroep of gewoonte van het aanbieden, verspreiden of bezitten van kinderpornografie (art. 240b, tweede lid, Sr), mensenhandel (art. 273f, eerste lid, Sr), opzettelijke vrijheidsberoving (art. 282 Sr), gijzeling (art. 282a Sr), doodslag (art. 287 Sr) of moord (art. 289 Sr).
De bij algemene maatregel van bestuur aan te wijzen misdrijven zullen misdrijven zijn waarop weliswaar geen gevangenisstraf van acht jaar of meer is gesteld maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Dit betreft misdrijven als het gebruik van een botnet (art. 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b, de verleiding van een minderjarige tot ontucht (art. 248a Sr) en «grooming» (art. 248e Sr). Er is dan vaak geen ander aangrijpingspunt voor de opsporing. Een beperking tot inzet van de bevoegdheid tot heimelijk binnendringen en het verrichten van onderzoekshandelingen tot levensbedreigende en terroristische misdrijven is daarom niet wenselijk. Het voordeel van aanwijzing van de delicten is dat flexibel ingespeeld kan worden op de snelle ontwikkelingen in de computercriminaliteit.
De regering heeft niet gekozen voor een gesloten lijst van delicten omdat de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk in een belangrijk deel van de gevallen dient als basis voor de toepassing van bestaande bijzondere opsporingsbevoegdheden, als het aftappen van communicatie en het afluisteren van vertrouwelijke communicatie. De toepassing van deze opsporingsbevoegdheden is thans niet beperkt tot een lijst van delicten, en de opsporing zou naar het oordeel van de regering ernstig worden belemmerd als een dergelijke lijst wel zou gaan gelden voor het aftappen van telecommunicatie of afluisteren van vertrouwelijke communicatie die door middel van een smartphone wordt afgehandeld, als de software voor het afluisteren op de smartphone is geplaatst. De regering geeft er de voorkeur aan het oordeel over de toepassing van de bevoegdheid in concrete gevallen over te laten aan het oordeel van de rechter. Een soortgelijke systematiek geldt niet alleen bij de toepassing van andere bijzondere opsporingsbevoegdheden, maar ook bij andere dwangmaatregelen als de inbeslagneming en de huiszoeking.

De leden van de D66-fractie hebben erop gewezen dat in de memorie van toelichting wordt gesproken over inzet van de bevoegdheid met het oog op de toepassing van bepaalde doelen op het gebied van de opsporing van strafbare feiten en hebben gevraagd naar welke doelen de regering verwijst.
De regering verwijst hiermee naar de doelen die zijn opgenomen in het voorgestelde artikel 126nba/uba/zpa, eerste lid, onderdelen a tot en met e, Sv. Dit betreft de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, de uitvoering van een bevel tot het direct

afluisteren of het aftappen van communicatie, de uitvoering van een bevel tot stelselmatige observatie, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en de ontoegankelijkmaking van gegevens.

De leden van de D66-fractie hebben een punt van zorg ten aanzien van de kring van personen die kunnen worden getroffen door deze bevoegdheid, te weten de verschoningsgerechtigden, en hebben gevraagd op grond waarvan de regering voldoende waarborgen aanwezig acht in het licht van de bevoegdheid die zij voorstelt. De informatie is dan immers al door de handen van de politie gegaan. Zij hebben tevens gevraagd of op enig moment minstens een registratie van de kennisneming van gegevens en de vernietiging daarvan dient plaats te vinden, alsmede achteraf een notificatie jegens de verschoningsgerechtigde.
Zoals eerder, naar aanleiding van vragen van de leden van de CDA-fractie is opgemerkt, is voor de bescherming van het verschoningsrecht bij de toepassing van de bevoegdheid tot het op afstand binnendringen in een geautomatiseerd werk aangesloten bij de bestaande regeling van artikel 126aa, tweede lid, Sv. Als bij de uitoefening van een bijzondere opsporingsbevoegdheid een proces-verbaal of een ander voorwerp mededelingen bevat door of aan een verschoningsgerechtigde dan worden het betreffende proces-verbaal of voorwerp vernietigd. Indien de officier van justitie vaststelt dat de mededelingen onder de bescherming van het verschoningsrecht vallen, dan beveelt hij terstond de vernietiging van de processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen. Aan de toepassing van de onderzoekshandelingen is inherent dat in een later stadium, nadat de gegevens zijn verzameld, blijkt dat gegevens betrekking hebben op mededelingen door of aan een verschoningsgerechtigde. Dit is thans ook aan de orde bij het toepassing van de bevoegdheid tot het aftappen van communicatie of het opnemen van vertrouwelijke communicatie. Het EHRM heeft het Nederlandse systeem van artikel 126aa Sv voldoende precies en begrijpelijk geacht en geoordeeld dat dit systeem voldoende waarborgen biedt om te kunnen worden aangemerkt als «recht» in de zin van artikel 8, tweede lid, EVRM (EHRM 25 november 2004, appl. no. 16269/92 Aalmoes vs. Nederland). Het bevel van de officier van justitie tot vernietiging is schriftelijk. Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt gezonden aan de officier van justitie. Dit is uitgewerkt in de OM-Instructie Vernietiging geïntercepteerde gesprekken met geheimhouders. In deze instructie is de te volgen procedure, indien de opsporingsambtenaar bij de uitwerking van geïntercepteerde communicatie meent een communicatie met een geheimhouder te constateren, stapsgewijs uitgewerkt. Er vindt geen notificatie plaats jegens de verschoningsgerechtigde maar wel aan de persoon tegen wie de bijzondere opsporingsbevoegdheid is ingezet.

De leden van de D66-fractie hebben opgemerkt dat voor de positie van journalisten wordt verwezen naar het wetsvoorstel bronbescherming in strafzaken en hebben gevraagd of die verwijzing betekent dat journalisten niet beschermd zijn tegen inbreuken, zoals in onderhavig wetsvoorstel voorgesteld, totdat de Wet bronbescherming in strafzaken in werking is getreden.
Journalisten hebben op dit moment geen wettelijk verschoningsrecht vanwege hun stand, beroep of ambt, als bedoeld in artikel 218 Sv. Inmiddels is het wetsvoorstel bronbescherming in strafzaken bij Uw Kamer ingediend (Kamerstukken II 2014/15, 34 032, nr.1) dat voorziet in wettelijke verankering van een recht op bronbescherming. Gelet op de stand van zaken van de parlementaire behandeling ligt het in de lijn der verwachting dat dit wetsvoorstel eerder tot wet wordt verheven dan het voorliggende wetsvoorstel computercriminaliteit III. In afwachting van de afronding van de parlementaire behandeling en de inwerkingtreding van

het wetsvoorstel bronbescherming in strafzaken is het geldend recht is vastgelegd in een Aanwijzing van het College van procureurs-generaal (Strct. 2012, 3656). In het arrest Goodwin van 27 maart 1996 (NJ 1996, 577) heeft het EHRM geoordeeld dat aan journalisten geen volledig verschoningsrecht toekomt, maar dat zij vanwege het belang van de vrijheid van meningsuiting en de persvrijheid in een democratische samenleving onder omstandigheden wel aanspraak kunnen maken een recht op bronbescherming. Dit recht is niet absoluut maar kan door een zwaarderwegend belang op zich worden gezet. Op basis van dit arrest heeft de Hoge Raad het recht op bronbescherming voor de journalist nader ingekaderd. Hiervoor kan worden gewezen op het arrest van 10 mei 1996 (NJ 1996, 578). De Aanwijzing van het College van procureurs-generaal bevat het geldende beleid voor justitieel optreden tegen journalisten met in begrip van de toepassing van dwangmiddelen tegen journalisten, zoals het thans wordt uitgevoerd. Zoals eerder, in antwoord op vragen van de leden van de SP-fractie, is opgemerkt wordt daarbij grote terughoudendheid betracht. Bronbescherming kan worden doorbroken als, uitgaande van het grote belang van de vrijheid van meningsuiting en nieuwsgaring, een nog zwaarderwegend belang bronbescherming niet meer mogelijk maakt. In aanvulling hierop voorziet het wetsvoorstel bronbescherming in strafzaken in een voorafgaande toetsing van bepaalde dwangmiddelen jegens journalisten door een rechter-commissaris.

De leden van de D66-fractie hebben gevraagd of het klopt het dat DDoS-aanvallen uitgevoerd worden door gebruik te maken van botnets, die zijn opgezet door gebruik te maken van fouten in software van computers, mobieltjes, tablets en andere apparaten. De leden van deze fractie hebben tevens gevraagd of het klopt dat de regering door middel van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk gebruik maakt van fouten in de software en of het klopt dat de fouten in die software dezelfde fouten zouden kunnen zijn als de fouten die criminelen gebruiken om botnets op te zetten. Deze leden hebben gevraagd of de regering de tegenstrijdigheid van deze benadering ziet. De leden van de D66-fractie hebben gevraagd of het niet beter is om ervoor te zorgen dat fouten gedicht worden zodat het überhaupt moeilijker wordt om botnets op te zetten. De leden van deze fractie hebben tevens gevraagd of de regering de mening deelt dat dat een grotere impact zal hebben op het aantal DDoS-aanvallen.

Er zijn verschillende technieken beschikbaar die het binnendringen mogelijk maken. Er zijn vele soorten geautomatiseerde werken en de beveiliging kan vele vormen hebben. Bij de keuze van een methode zijn, naast proportionaliteit en subsidiariteit, aspecten als de effectiviteit van de inzet, de kans op onderkenning en het risico op gevolgschade van belang. Het gebruik van een kwetsbaarheid is vaak niet de meest aangewezen methode. Voor een uitgebreide afweging over het gebruik van kwetsbaarheden kan worden verwezen naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden. Overigens kan de voorgestelde bevoegdheid de aanpak van botnets in de toekomst juist versterken.

De leden van de D66-fractie hebben gelezen dat de procedure van nummerherkenning ook wordt gewaarborgd bij het onderzoek in een geautomatiseerd werk en hebben gevraagd of de regering kan toelichten hoe dit in de praktijk werkt. De leden van deze fractie hebben tevens gevraagd hoe, als er een «keylogger» op een smartphone wordt geïnstalleerd, de «logging» wordt stilgezet zodra de verdachte een whatsapp bericht verstuurt naar zijn advocaat. Deze leden hebben voorts gevraagd

of de regering kan toelichten hoe omgegaan wordt met een concept e-mailbericht van een verdachte aan een advocaat.
De regeling rond de toepassing van bijzondere opsporingsbevoegdheden voorziet in een speciale procedure voor mededelingen gedaan door of aan een verschoningsgerechtigde. Dit betreft de regeling van het bestaande artikel 126aa, tweede lid, Sv. Deze regeling is ook van toepassing op het onderzoek in een geautomatiseerd werk. Dit ligt ook daarom voor de hand, omdat na het op afstand binnendringen van een geautomatiseerd werk bestaande opsporingsbevoegdheden kunnen wordt uitgeoefend, zoals het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie. Met behulp van het technische hulpmiddel kunnen de afgetapte of opgenomen gegevens worden verzameld en opgeslagen. Hiervoor kan gebruik worden gemaakt van een keylogger. Ook kunnen gegevens die in het geautomatiseerde werk zijn opgeslagen worden overgenomen en vervolgens worden opgeslagen die in dat werk zijn opgeslagen. Dit kan een concept e-mailbericht aan een advocaat betreffen. Zodra de opsporingsambtenaar bij het onderzoek van de opgeslagen gegevens kennisneemt van mededelingen waarvan hij weet of redelijkerwijs kan vermoeden dat deze zijn gedaan door of aan een geheimhouder, stelt hij de officier van justitie hiervan onverwijld in kennis. Als de officier van justitie vaststelt dat de mededelingen, bedoeld in het eerste lid, mededelingen zijn door of aan een geheimhouder dan beveelt hij terstond de vernietiging van de processen-verbaal en andere voorwerpen, voor zover zij deze mededelingen behelzen. Het bevel tot vernietiging is schriftelijk. Van de vernietiging wordt proces-verbaal opgemaakt, dat wordt gezonden aan de officier van justitie. In de gevallen waarin de geheimhouder verdachte is, wordt het oordeel van een gezaghebbend lid van de betreffende beroepsgroep ingewonnen over de vraag welke gegevens dergelijke mededelingen behelzen.
Het is op dit moment technisch niet mogelijk de logging van de keylogger uit te schakelen zodra de verdachte een bericht verstuurt aan zijn advocaat. Daarvoor is het nodig dat het mailadres van de advocaat door de keylogger wordt herkend waarna de vastlegging van de gegevens kan worden afgebroken. Wel mogelijk is dat het aftappen van telecommunicatie wordt afgebroken als een nummer is betrokken dat door de NOvA bij de politie is aangemeld. Dit betreft het systeem van nummerherkenning. Alsdan wordt het opnemen van de communicatie onmiddellijk beëindigd; als communicatie is opgenomen voordat het nummer is herkend, worden de gegevens van de communicatie onmiddellijk langs geautomatiseerde weg vernietigd.

De leden van de D66-fractie hebben geconstateerd dat het begrip geautomatiseerd werk zeer breed is gedefinieerd en gevraagd of de regering kan toelichten waarom voor deze brede definitie is gekozen en niet voor een beperkte lijst van apparaten zoals smartphones, tablets en pc's.
De brede definitie vormt onderdeel van het Cybercrimeverdrag, dat door de Nederlandse regering is ondertekend. De Nederlandse regering is gehouden dit verdrag te implementeren. De definitie van geautomatiseerd werk, zoals deze in de EU-regelgeving wordt gebruikt, is nog ruimer omdat daarin ook de computergegevens zijn betrokken die met dat apparaat of groep van apparaten worden opgeslagen, verwerkt of verzonden met het oog op de verwerking, het gebruik, de beveiliging en het onderhoud daarvan (Kaderbesluit 2013/40/EU over aanvallen op informatiesystemen). De Nederlandse regering is eveneens gehouden dit kaderbesluit te implementeren. Mede gelet op het advies van de Afdeling advisering geeft de regering de voorkeur aan de definitie van het Cybercrimeverdrag, waarbij opgemerkt kan worden dat het begrip «gegevens» reeds in de Nederlandse wetgeving is geïmplementeerd (art. 80 quinquies Sr). Voor het antwoord op de vraag waarom niet is gekozen

voor een beperkte lijst van apparaten wordt overigens verwezen naar de beantwoording van een eerdere, soortgelijke vraag van de leden van de SP-fractie.

De leden van de fractie van GroenLinks hebben gevraagd of de toepassing van de hackbevoegdheid niet nauwkeuriger moet worden afgebakend. Het komt deze leden voor dat een breed scala van delicten onder de reikwijdte van de voorgestelde bevoegdheid valt, en zij hebben gevraagd of het niet meer voor de hand ligt om de inzet van de bevoegdheid expliciet tot een aantal specifieke delicten te beperken.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de D66-fractie waarom niet is gekozen voor een gesloten lijst van delicten.

De leden van de GroenLinks-fractie hebben voorts gevraagd wat onder geautomatiseerd werk wordt verstaan en of daaronder bijvoorbeeld ook motorvoertuigenhard- en software, geavanceerde medische hulpmiddelen en domotica onder valt. Tevens hebben deze leden gevraagd of de regering een afbakening kan geven welke geautomatiseerde werken wel en welke niet voor toepassing van de hackbevoegdheid in aanmerking komen.
Voor het antwoord op deze vragen wordt verwezen naar de eerdere beantwoording van vragen van de leden van de PvdA-fractie of tot een geautomatiseerd werk ook een «connected car» of connecties infotainment/navigatiesysteem met de daarbij behorende servers behoren.

2.3 De doelen van het onderzoek in een geautomatiseerd werk

2.3.1 De vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan
De leden van de D66-fractie hebben gelezen dat er bij de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker sprake is van een virtuele plaatsopneming of inkijkoperatie en hebben gevraagd of zij het goed begrijpen dat ook in de volgende fase, wanneer verder wordt opgetreden ten aanzien van het geautomatiseerde werk, dat nog steeds heimelijk plaatsvindt en dus buiten de wetenschap van de onderzochte persoon om. De leden van deze fractie hebben tevens gevraagd of de regering in dit kader kan toelichten waar precies de overgang ligt tussen technisch optreden en tactisch optreden ten aanzien van geautomatiseerde werken.
Afhankelijk van hoe het onderzoek plaatsvindt zal de grens tussen het technisch optreden en het tactisch optreden verschillen. Het doel zal echter altijd zijn dat het tactisch personeel geen enkele invloed kan uitoefenen op het binnendringen in het geautomatiseerde werk en de plaatsing, inzet en verwijdering van een technisch hulpmiddel De gegevens die omschreven zijn in het bevel en door het technische team zijn verzameld, komen beschikbaar voor het tactisch personeel met het oog op het gebruik in het opsporingsonderzoek. Als voorbeeld kan de inhoud van het mailverkeer worden gegeven. Wanneer naar de correspondentie tussen de verdachte en een andere verdachte gevraagd wordt in het bevel, zal het tactisch team die gevraagde correspondentie te zien krijgen, en niet eventuele andere correspondentie vanuit hetzelfde email adres.

De leden van de D66-fractie hebben opgemerkt dat de beperking tot een geautomatiseerd werk dat bij de verdachte in gebruik is niet hetzelfde is als diens eigendom en hebben gevraagd of zij het goed hebben begrepen dat het dus ook om geleende of gestolen apparaten kan gaan waarop zich

informatie van anderen kan bevinden. Tevens hebben zij gevraagd wat dit betekent voor de bewijsvoering waarbij aangetoond moet worden dat de gegevens toebehoren aan de verdachte als gebruiker en niet als de persoon aan wie het apparaat toebehoort.
Het vereiste dat het geautomatiseerde werk bij de verdachte in gebruik is betekent dat het op grond van feiten of omstandigheden aannemelijk dient te zijn dat de verdachte gebruik maakt van het geautomatiseerde werk. Het is daarvoor niet vereist dat de verdachte de enige gebruiker is. De leden van de D66-fractie hebben het goed begrepen dat het ook om geleende of gestolen apparaten kan gaan waarop zich informatie van anderen kan bevinden. Hierbij roep ik in herinnering, zoals in de eerdere beantwoording van vragen van de leden van de PvdD-fractie aan de orde is gekomen, dat de inzet van bijzondere opsporingsbevoegdheden niet is beperkt tot de verdachte. Deze bevoegdheden kunnen ook jegens anderen worden ingezet als dit van belang is voor de waarheidsvinding. Met het vereiste dat het geautomatiseerde werk bij de verdachte in gebruik is, wordt voorkomen dat de bevoegdheid wordt ingezet jegens anderen dan de verdachte. Dat gegevens van derden in het kader van de toepassing van bijzondere opsporingsbevoegdheden ter kennis komen van de opsporingsambtenaren is overigens niet nieuw. Bij de toepassing van een opsporingsbevoegdheid van het aftappen van telecommunicatie komt de communicatie van de personen met wie het gesprek wordt gevoerd uit de aard der zaak ter kennis van de opsporingsambtenaren die zijn belast met het uitluisteren van deze communicatie. Ditzelfde geldt bij het gebruik van de internettap, alsdan komt alle informatie die via een IP-adres wordt gecommuniceerd, ter kennis van de opsporing, ook de gegevens van gebruikers van andere geautomatiseerde werken die gebruik maken van dezelfde router en daarmee van ditzelfde IP-adres. Voor de toepassing van bepaalde bijzondere opsporingsbevoegdheden in het kader waarvan gegevens van derden ter kennis kunnen komen van de politie, gelden specifieke verplichtingen rond het verdere gebruik van de verzamelde gegevens. Dit betreft de observatie met behulp van een technisch hulpmiddel dat signalen registreert, het aftappen van telecommunicatie, het direct afluisteren van vertrouwelijke communicatie en het vorderen van gegevens. De officier van justitie kan bepalen dat de gegevens worden gebruikt voor een ander strafrechtelijk onderzoek, anders worden de gegevens vernietigd zodra twee maanden verstreken zijn nadat de zaak is geëindigd (art. 126cc, tweede lid, en 126dd, eerste lid, Sv). Daartoe zullen doorgaans geen gegevens van derden behoren, omdat zij niet als verdachte zijn aangemerkt. Deze verplichtingen zijn onverkort van toepassing voor de toepassing van het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie, nadat op afstand een geautomatiseerd werk is binnengedrongen.
Vereist is dat het geautomatiseerde werk bij de verdachte in gebruik is. Niet is vereist dat de verdachte eigenaar is van het geautomatiseerde werk. Voor de bewijsvoering geldt dat de officier van justitie bewijsmateriaal dient aan te dragen op grond waarvan wettig en overtuigend bewezen kan worden dat een verdachte een strafbaar feit heeft gepleegd. Niet vereist is dat aangetoond wordt dat de gegevens aan de verdachte als gebruiker toebehoren. Als de verdachte het verweer voert dat hij niets te maken heeft met de vastgelegde gegevens dan is het aan de officier van justitie om met feiten en omstandigheden dit verweer te weerleggen.

De leden van de VVD-fractie hebben gevraagd of er bewaartermijnen zijn verbonden aan de vastgelegde gegevens die in het geautomatiseerde werk zijn of worden opgeslagen en zo ja, hoe deze bewaartermijnen er uit zien.
De gegevens die worden vastgelegd in het kader van een onderzoek in een geautomatiseerd werk vallen onder het regime van de Wet politiegegevens (Wpg). De Wpg kent regels over de bewaartermijnen van

politiegegevens. De gegevens die worden verwerkt met het oog op de schending van de rechtsorde in een bepaald geval kunnen worden verwerkt voor zover dat noodzakelijk is voor het doel van het onderzoek. Dit betekent dat de gegevens kunnen worden bewaard totdat de verdachte onherroepelijk is veroordeeld (Kamerstukken II 2005/06, 30 327, nr. 3, blz. 46).

De VVD-fractie heeft gevraagd wat er gebeurt met gegevens of informatie die tijdens het onderzoek worden ingezien die geen betrekking hebben op het specifieke doel van het onderzoek. Deze leden hebben tevens gevraagd wat er in dit kader wordt bedoeld met gegevens die «redelijkerwijs» nodig zijn om de waarheid aan de dag te brengen. Zij hebben voorts gevraagd hoe wordt voorkomen dat bij het verrichten van onderzoek in een geautomatiseerd werk de gegevens, en daarmee de privacy, van anderen dan de verdachte tegen wie het onderzoek gericht is, wordt geschonden.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de D66-fractie.

De leden van de CDA-fractie hebben gevraagd of het meekijken met emailverkeer tevens behelst dat niet alleen verzonden informatie kan worden bekeken maar eveneens de praktijk dat berichten in een concept-box worden geplaatst en aldaar door meerdere personen bekeken kunnen worden via het delen van inloggegevens.
Wanneer berichten in een concept-inbox worden geplaatst kan sprake zijn van stromende gegevens, indien de gegevens bijvoorbeeld vanuit een locatie worden bekeken en daarmee (tijdelijk) worden opgehaald vanaf de server van de aanbieder van de emaildienst. In de huidige situatie zou daarvoor de bevoegdheid van het aftappen en opnemen van telecommunicatie (art. 126m/t Sv) kunnen worden ingezet. Verschillende aanbieders werken echter met een https-verbinding (zoals Google) waardoor de inhoudelijke gegevens niet inzichtelijk zijn nadat deze zijn afgetapt. In de praktijk kunnen de inhoudelijke berichten van mails die geraadpleegd worden in een concept-box veelal dus niet in leesbare vorm worden verkregen.
Wanneer berichten in een concept-inbox op het geautomatiseerde werk worden bewaard, dan is er sprake van vaste gegevens. Het wetsvoorstel biedt de mogelijkheid van het op afstand binnendringen in een geautomatiseerd werk met het oog op het overnemen van gegevens die in dat werk zijn opgeslagen. Daarvoor gelden andere voorwaarden met betrekking tot het te onderzoeken strafbaar feit; er moet dan sprake zijn van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

De leden van de CDA-fractie hebben ook gevraagd in hoeverre toegang mogelijk is tot reeds verwijderde bestanden in het geheugensysteem van het desbetreffende apparaat, vergelijkbaar met de wijze waarop deze door de gebruiker zelf of door een systeembeheerder kunnen worden teruggevonden.
Verwijderde bestanden zijn in bepaalde omstandigheden technisch nog geheel of gedeeltelijk aanwezig op het geautomatiseerde werk. Of het technisch mogelijk is dergelijke bestanden alsnog over te nemen, en welke handelingen hiervoor nodig zijn, zal per geval verschillen. Dit is mede afhankelijk van de (technische) wijze waarop de bestanden zijn verwijderd.

De leden van de D66-fractie hebben gevraagd of er in het bevel een bepaald termijn staat waarbinnen gegevens moeten worden vastgelegd of

dat de politie jarenlang de hacksoftware op het apparaat kan houden, wachtend op mogelijke strafbare feiten.
In het bevel dient de officier van justitie het tijdstip waarop, of de periode waarbinnen, aan het bevel uitvoering wordt gegeven te vermelden. Dit is vastgelegd in de voorgestelde artikelen 126nba/uba, tweede lid, onderdeel g, respectievelijk 126zpa, tweede lid, onderdeel e., Sv. Een bevel tot het binnendringen van een geautomatiseerd werk wordt gegeven voor een periode van ten hoogste vier weken. Het bevel kan telkens voor een periode van ten hoogste vier weken worden verlengd. Dit is vastgelegd in het voorgestelde artikelen 126nba, derde lid, respectievelijk 126uba/zpa, derde lid, Sv. Na afloop van het onderzoek wordt de software verwijderd.

De leden van de D66-fractie hebben opgemerkt dat de regering stelt dat met speciale software het internetgebruik van een verdachte kan worden gevolgd en hebben gevraagd welke software de regering precies bedoelt, en welke software de regering gaat gebruiken om invulling te geven aan de «keylogger»-functie. Zij hebben tevens gevraagd hoe de «keylogger» op de computer of smartphone wordt aangebracht.
Onder verwijzing naar onder meer de antwoorden op Kamervragen van de leden Schouw en Berndsen (D66) over het gebruik van spysoftware (Kamerstukken II 2011/12, Aanhangselnummer 1374) vormt het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken en hoe ze worden toegepast een onaanvaardbaar risico voor de inzetbaarheid van die middelen. Ik kan hierover dan ook geen mededelingen doen.

2.3.3 De ontoegankelijkmaking van gegevens

De leden van de CDA-fractie hebben gevraagd of de beoordeling van de keuze welke maatregel het meest gewenst is, tevens behelst de afweging om gegevens bewust intact te laten in plaats van te verwijderen. Legitieme redenen hiervoor zouden kunnen zijn dat hiermee uiteindelijk (ernstige) strafbare feiten kunnen worden ontdekt en/of worden opgespoord. Een andere reden zou ook kunnen zijn de afweging om de verdachte niet wakker te schudden met (onbewust) achtergelaten sporen. Graag vernemen zij hierop een reactie van de regering.
Het ontoegankelijk maken van gegevens is een bevoegdheid die kan worden ingezet ten behoeve van het voorkomen of beëindigen van een strafbaar feit. De bevoegdheid van het vastleggen van gegevens biedt de mogelijkheid om gegevens over te nemen, waarbij deze beschikbaar blijven voor de gebruiker. De gebruiker blijft dan in het belang van het onderzoek tijdelijk onkundig van de interesse van de opsporing in zijn handelen. Er kan echter ook voor worden gekozen om af te zien van de inzet van een bijzondere opsporingsbevoegdheid, bijvoorbeeld met het oog op de absolute geheimhouding van het opsporingsonderzoek of de opsporing van ernstiger strafbare feiten. De officier van justitie besluit in voorkomend geval welke bevoegdheid in het opsporingsonderzoek wordt ingezet.

De leden van de D66-fractie hebben gevraagd aan welke strafbare feiten de regering denkt voor het ontoegankelijk maken van gegevens en hoe het ontoegankelijk maken zich verhoudt tot het doel juist heimelijk een geautomatiseerd werk binnen te dringen zonder dat de desbetreffende persoon daar weet van heeft.
De bevoegdheid van het ontoegankelijk maken van gegevens laat zich op hoofdlijnen vergelijken met de bevoegdheid tot de inbeslagneming met het oog op de onttrekking aan het verkeer van een voorwerp. Voor deze beide bevoegdheden geldt dat het gaat om een maatregel ter bescherming van de maatschappij. Bij voorwerpen kan worden gedacht aan drugs of vuurwapens, bij gegevens kan worden gedacht aan kinderpornografie of aan de gegevens van een botnet die belangrijke

maatschappelijke diensten belemmeren, zoals de dienstverlening door banken of andere financiële instellingen. Deze bevoegdheid is geregeld in het voorgestelde artikel 126cc Sv., waarin wordt aangesloten bij de regeling van artikel 125o Sv. De uitoefening van de bevoegdheid kan in beginsel tot gevolg hebben dat de betrokkene ervan op de hoogte kan raken dat jegens hem een bijzondere opsporingsbevoegdheid is uitgeoefend. Voortzetting van een vrije beschikbaarheid van de gegevens in het maatschappelijk verkeer kan echter als zodanig schadelijk worden geacht dat het belang van de ontoegankelijkmaking prevaleert boven het belang van de afscherming van de toepassing van de bevoegdheid jegens de betrokkene. Te dien aanzien is de situatie vergelijkbaar met de verplichting, op grond van artikel 126ff Sv, tot inbeslagneming van voorwerpen waarvan het aanwezig hebben of voorhanden hebben op grond van de wet verboden is vanwege hun schadelijkheid voor de volksgezondheid of hun gevaar voor de veiligheid, zoals drugs of explosieven (verbod op doorlaten). Door de inbeslagneming kan de betrokken persoon op de hoogte raken van de toepassing van een bijzondere opsporingsbevoegdheid. Het belang van het voorkomen dat illegale goederen op de markt komen weegt echter zwaarder dan het belang van afscherming van de inzet van een bijzondere opsporingsbevoegdheid.

De leden van de D66-fractie hebben gevraagd over welke te verwijderen gegevens de regering het heeft als zij stelt dat onder ontoegankelijkmaking tevens wordt verstaan het verwijderen van gegevens uit het geautomatiseerde werk, maar met behoud van gegevens ten behoeve van strafvordering.
Hiermee wordt gedoeld op gegevens waarvan de voortzetting van de beschikbaarheid voor het publiek zodanig schadelijk is voor de bescherming van de maatschappelijke waarden dat de gegevens dienen te worden onttrokken aan de beschikkingsmacht van de betrokken persoon, maar die tevens van belang zijn voor het bewijs van de betrokkenheid van die persoon bij het beramen of plegen van een strafbare feit. Als het uitsluitend gaat om gegevens die van belang zijn voor de bewijsvoering, dan kunnen de gegevens worden vastgelegd, zonder dat de beschikkingsmacht van de betrokkene wordt beperkt. In het geval van de ontoegankelijkmaking van gegevens ligt dit in zoverre anders, dat de gegevens tevens buiten de beschikkingsmacht van de betrokkene worden gebracht.

De leden van de D66-fractie hebben gevraagd door wie wordt bepaald welke maatregel het meest effectief, proportioneel en subsidiair is en hoe lang het ontoegankelijk maken van gegevens kan duren. Ook hebben zij gevraagd hoe de toegankelijkheid wordt hersteld als de gegevens zijn gewist voorafgaand aan de einduitspraak van de rechter.
De ontoegankelijkmaking van gegevens strekt ertoe dat maatregelen worden getroffen om te voorkomen dat de beheerder van het geautomatiseerde werk of derden verder van die gegevens kennis nemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Dit is vastgelegd in artikel 125o, tweede lid, Sv. In het voorgestelde artikel 126cc, vijfde lid, wordt naar dit lid verwezen. De officier van justitie bepaalt welke specifieke maatregelen worden getroffen om de gegevens ontoegankelijk te maken. Als de gegevens worden verwijderd, dan dienen zij te worden behouden ten behoeve van de strafvordering. In het kader van de ontoegankelijkmaking kunnen de gegevens dan ook niet worden gewist. De ontoegankelijkmaking betreft een voorlopige maatregel, in afwachting van een beslissing van de rechter. De ontoegankelijkmaking van de gegevens duurt in beginsel tot het moment van de rechterlijke beslissing, op grond van de artikelen 354 of 552fa Sv. Echter, zodra het belang van de strafvordering zich niet meer

verzet tegen opheffing van de maatregel bepaalt de officier van justitie dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerde werk worden gesteld.

De leden van de D66-fractie hebben gelezen dat met behulp van hardware een ingang van een computer (tijdelijk) onbruikbaar kan worden gemaakt en hebben gevraagd of de regering dit kan toelichten, evenals wat voor hardware en wat voor ingangen dit betreft.
De manieren waarop toegang tot een geautomatiseerd werk kan worden verkregen, zijn divers. Het is in het belang van effectieve opsporing niet mogelijk om op verschillende opsporingsmethodieken in te gaan.

De leden van de D66-fractie hebben gevraagd of het klopt dat de apparaten die de politie gaat hacken, op basis van de bevoegdheden in dit wetsvoorstel, feitelijk een botnet zullen vormen. De leden van deze fractie hebben tevens gevraagd of het klopt dat de software die geplaatst wordt op de apparaten in contact staat met een server van de maker van de software in plaats van de server van de overheid.
Dit is niet het geval, de geautomatiseerde werken die op afstand worden binnengedrongen zullen feitelijk geen botnet vormen. Een botnet is een grote groep van geautomatiseerde werken, die vanuit een ander geautomatiseerd werk worden aangestuurd, zonder dat de gebruikers van de grote groep werken zich daarvan bewust zijn of daarvoor toestemming hebben verleend, op zodanige wijze dat het functioneren van een ander geautomatiseerd werk (de «target») wordt gehinderd of zelfs onmogelijk gemaakt. Vaak worden botnets gebruikt voor het plegen van andere strafbare feiten. Van het aansturen van een grote groep van geautomatiseerde werken is bij de thans voorgestelde bevoegdheid geen sprake, deze bevoegdheid is beperkt tot het geautomatiseerde werk dat bij de verdachte in gebruik is. De voorgestelde bevoegdheid voorziet in de mogelijkheid dat op afstand wordt binnengedrongen in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen. Dit kan de server zijn van waaruit het botnet wordt aangestuurd (de command and control server). In het kader van het onderzoek met behulp van een technisch hulpmiddel, een softwareapplicatie, wordt uitsluitend een verbinding tot stand gebracht tussen het binnengedrongen geautomatiseerd werk en de server van de politie. Er wordt geen verbinding tot stand gebracht met de server van de maker van de softwareapplicatie.

De leden van de D66-fractie hebben gevraagd of het in dit geval alleen gaat om botnets waarbij aansturing vanuit een centrale server geschied of ook om peer-to-peer botnets. De leden van deze fractie hebben tevens gevraagd of dit in het laatste geval betekent dat de politie ook computers die onderdeel zijn van een botnet mogen hacken. Deze leden hebben tenslotte gevraagd in hoeverre het overnemen van de servers van een centraal aangestuurde botnet een structurele oplossing is.
Voor een opsporingsonderzoek kan het noodzakelijk zijn een botnet binnen te dringen met als doel de daders van het strafbare feit te achterhalen. In een dergelijk geval is het niet proportioneel in het geautomatiseerd werk meer gegevens te verzamelen dan noodzakelijk voor het onderzoek naar het desbetreffende strafbaar feit. Dat betekent dat slechts het deel van het botnet op afstand wordt binnengedrongen dat nodig voor het onderzoek naar het botnet en de aansturing ervan. Dit zal doorgaans de server zijn van waaruit het botnet wordt aangestuurd maar het is niet uitgesloten dat andere geautomatiseerde werken, die onderdeel vormen van het botnet, moeten worden binnengedrongen, bijvoorbeeld om de centrale server te kunnen identificeren. Het overnemen van servers van een botnet is geen structurele oplossing. Burgers en bedrijven dragen zelf verantwoordelijkheid voor een adequate beveiliging van de geauto-

matiseerde werken die zij gebruiken. Niettemin kan het in een strafrechtelijk onderzoek aangewezen zijn dat opsporingsonderzoek wordt verricht naar een botnet.

De leden van de D66-fractie hebben gevraagd of het niet beter is om te investeren in het veiliger maken van apparaten en goede cyber hygiëne, zodat zij überhaupt geen onderdeel uit gaan maken van een botnet. Deze vraag wordt in beginsel bevestigend beantwoord. Als uitgangspunt verdient het zeker de voorkeur te investeren in de veiligheid van apparaten en de hygiëne op het internet. Dit is een ideaal dat slechts op langere termijn en in samenwerking op supranationaal niveau te realiseren is. In het licht van het open karakter van het internet is hier een lange weg te gaan. Hiervoor zijn inspanningen nodig op mondiaal niveau omdat, vanwege het karakter van de markt, de veiligheid van apparaten en een goede cyberhygiëne niet met enkel nationale inspanningen te bereiken is. Nederland neemt actief deel aan internationale initiatieven die er zijn om het internet veiliger te maken. Dit neemt niet weg dat de botnets thans ook in Nederland een grote bedreiging vormen voor het functioneren van geautomatiseerde werken, waardoor de dienstverlening van bedrijven en overheidsinstellingen ernstig kan worden gehinderd en burgers zich in hun veiligheid aangetast voelen. De voorgestelde bevoegdheid biedt de mogelijkheid om hiertegen op te treden, bijvoorbeeld door de server binnen te dringen van waaruit het botnet wordt aangestuurd (de command and control server) en de gegevens zodanig te bewerken dat de aansturing wordt beëindigd, zodat het aangevallen geautomatiseerde werk weer kan functioneren. Dit is overigens lang niet bij alle botnets mogelijk. Voor het bestrijden van botnets blijven investeringen in de veiligheid van geautomatiseerde werken en samenwerking met andere partijen in binnen- en buitenland van belang.

2.3.4 De uitvoering van een bevel tot het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie

De leden van de SP-fractie hebben gevraagd of de het aangepaste Besluit technische hulpmiddelen strafvordering zal worden voorgehangen voordat het in werking treedt. De leden van de SP-fractie hebben tevens gevraagd of het besluit in aanmerking komt voor internetconsultatie.
Het wetsvoorstel bevat de hoofdelementen van de regeling met betrekking tot het binnendringen en het onderzoek in een geautomatiseerd werk. De overige elementen, zoals de eisen die gesteld worden aan technische hulpmiddelen, betreffen de uitwerking van technische normen en worden geregeld op het niveau van een algemene maatregel van bestuur. Artikel 126ee Sv, zoals aangepast door het wetsvoorstel, bevat een grondslag om bij (of krachtens) algemene maatregel van bestuur regels te stellen over het doen van onderzoek in een geautomatiseerd werk met behulp van een technisch hulpmiddel. In het bijzonder kunnen eisen gesteld worden ten aanzien van de opslag, verstrekking, plaatsing en verwijdering van technische hulpmiddelen, de onschendbaarheid van de vastlegging van gegevens en het voorkomen van misbruik door derden. Ook geeft het wetsvoorstel in artikel 126nba, zevende lid, Sv een grondslag om bij of krachtens algemene maatregel van bestuur regels te stellen over de autorisatie en deskundigheid van de opsporingsambtenaren die kunnen worden belast met het onderzoek in een geautomatiseerd werk, de samenwerking met andere opsporingsambtenaren en de geautomatiseerde vastlegging van gegevens ter uitvoering van het bevel tijdens het onderzoek.
Omwille van de overzichtelijkheid worden voornoemde onderwerpen uitgewerkt in een afzonderlijk besluit en niet, zoals eerder in de memorie van toelichting vermeld, via een wijziging van het Besluit technische hulpmiddelen strafvordering. Net als het Besluit technische hulpmiddelen strafvordering zal dit nieuwe besluit gebaseerd zijn op het uitgangspunt

dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, voor derden toetsbaar en niet manipuleerbaar dienen te zijn. Het wetsvoorstel bevat geen voorhangbepaling. Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen (Aanwijzingen voor de regelgeving, Aanwijzing 35).
Het besluit zal ter consultatie worden aangeboden op www.internetconsultatie.nl.

De leden van de SP-fractie hebben gevraagd of het klopt dat het Besluit technische hulpmiddelen strafvordering op dit moment niet voldoet aan de eisen van digitale opsporingsbevoegdheden
In antwoord op Kamervragen over het gebruik van software door de politie (Aanhangsel Handelingen II 2014/15, nr. 202 en Aanhangsel Handelingen II 2014/15, nr. 3199) is aangegeven dat de politie beschikt over software die fysiek geïnstalleerd kan worden op de computer van een verdachte, waarmee ten behoeve van opsporingsdiensten toegang kan worden verkregen tot die computer en waarmee gegevens daarvan kunnen worden overgenomen. De inzet van dit middel beperkt zich tot het opnemen van vertrouwelijke communicatie (op basis van art. 126l Sv).

De leden van de SP-fractie hebben gevraagd of de regering het standpunt deelt dat het van belang is dat het Besluit technische hulpmiddelen tijdig wordt gewijzigd, zodat parlement en praktijk hierover kunnen oordelen.
De regering deelt het standpunt van de SP-fractie in die zin dat zij alles in het werk stelt om het besluit ter uitvoering van het wetsvoorstel tijdig ter consultatie aan te bieden.

De leden van de CDA-fractie hebben gevraagd of het de opsporingspraktijk niet belemmert dat door middel van een apart bevel toestemming moet worden gevraagd teneinde een ander land te verzoeken instemming te verlenen een gebruiker af te tappen. Zij hebben tevens gevraagd of de regering niet verwacht dat juist digitale criminaliteit zich in veel gevallen zal uitstrekken tot andere landen en of het in dat kader niet wenselijk is om de toestemming aan een ander land direct te koppelen aan de voorgestelde bevoegdheden tot aftappen en opnemen.
Als het gaat om het aftappen van telecommunicatie dan voorziet het Wetboek van Strafvordering in een verplichting om, indien bekend is dat een gebruiker zich op het grondgebied van een andere staat bevindt, voor zover een verdrag dit voorschrijft en met toepassing van dat verdrag, die andere staat in kennis te stellen van het voornemen tot aftappen en het verwerven van de instemming van die staat voordat het bevel ten uitvoer wordt gelegd (art. 126ma/ta Sv). Deze regeling is in het wetboek opgenomen om uitvoering te geven aan het Europees rechtshulpverdrag 2000. De regering verwacht inderdaad dat juist digitale criminaliteit zich in veel gevallen zal uitstrekken tot andere landen en heeft om die reden in de memorie van toelichting een afzonderlijke paragraaf opgenomen, waarin nader wordt ingegaan op het onderzoek in een geautomatiseerd werk en rechtsmacht (paragraaf 2.8). De toestemming van een ander land zal in de praktijk direct kunnen worden gekoppeld aan de voorgestelde bevoegdheden tot aftappen en opnemen, maar deze mogelijkheid is in de eerste plaats beperkt tot andere EU-lidstaten en in de tweede plaats tot de betreffende bevoegdheden.

De leden van de CDA-fractie hebben geconstateerd dat de regering verwijst naar het Cybercrimeverdrag op basis waarvan het aftappen ook zonder de medewerking van de aanbieder kan plaatsvinden en hebben gevraagd of het Cybercrimeverdrag daarmee ook ruimte laat om zonder toestemming van de gebruiker zijn geautomatiseerde werken heimelijk binnen te dringen en zo ja, op grond van welk artikel.

In het Cybercrimeverdrag is vastgelegd dat iedere partij de wetgevende en andere maatregelen neemt die nodig zijn om aan haar bevoegde autoriteiten de bevoegdheid te verlenen tot het op haar grondgebied doorzoeken van of zich op vergelijkbare wijze toegang verschaffen tot een computersysteem of onderdeel daarvan en de daarin opgeslagen computergegevens, en een opslagmedium voor computergegevens waarop computergegevens kunnen worden opgeslagen (artikel 19, eerste lid, Cybercrimeverdrag). Uit het toelichtend rapport («Explanatory report») kan worden afgeleid dat deze bepaling betrekking heeft op de doorzoeking van plaatsen ter vastlegging van gegevens die op een geautomatiseerd werk of een gegevensdrager zijn opgeslagen. Dit is in het Wetboek van Strafvordering geregeld in artikel 125i Sv. Artikel 19, eerste lid, van het Cybercrimeverdrag heeft dus geen betrekking op het zonder toestemming van de gebruiker een geautomatiseerd werk heimelijk binnen te dringen, maar staat daar anderzijds ook niet aan in de weg. Aldus laat dit verdrag ruimte om zonder toestemming van de gebruiker zijn geautomatiseerde werk heimelijk binnen te dringen.

De leden van de D66-fractie hebben opgemerkt dat indien de gebruiker van het nummer dat zal worden afgetapt zich op het grondgebied van een ander land bevindt, toestemming zal moeten worden verkregen van dat land voor toepassing van de bevoegdheid, en hebben gevraagd of dat tot toepassingsknelpunten kan leiden bij landen die minder bereidwillig zijn mee te werken aan aftappen dan wel technisch niet zo ver zijn dan wel wetgeving hebben die zich daartegen verzet. Deze leden hebben tevens gevraagd welke landen eventueel problematisch zouden zijn bij de uitvoering hiervan.
De bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk zal met zich mee brengen dat wanneer het werk zich in het buitenland bevindt het in beginsel noodzakelijk is om in overleg te treden met het desbetreffende land. Elk land heeft eigen wettelijke bevoegdheden en capaciteiten voor de opsporing. Per geval wordt bezien wat de mogelijkheden zijn om het onderzoek effectief voort te zetten.

De leden van de D66-fractie hebben gevraagd of de algemene maatregel van bestuur, waarin eisen worden gesteld aan het technisch hulpmiddel dat voor het opnemen gebruikt kan worden, wordt voorgehangen zodat de Kamer kan kennisnemen van de gestelde eisen aan het technische hulpmiddel.
Voor het antwoord op deze vraag kan worden verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de SP-fractie.

2.3.5 De uitvoering van een bevel tot stelselmatige observatie

De leden van de PvdA-fractie hebben gevraagd of zij het goed begrijpen dat het wetsvoorstel ertoe strekt dat een op zichzelf staand hulpmiddel kan worden aangebracht om een persoon te volgen, zoals een peilzender, zo ja, wat dat te maken heeft met het op afstand binnendringen van een geautomatiseerd werk en zo nee, wat dan bedoeld wordt.
Het binnendringen van een geautomatiseerd werk met als doel het uitvoeren van een bevel tot stelselmatige observatie biedt de mogelijkheid om via de plaatsing van software de GPS-functie van het geautomatiseerde werk in te schakelen. Hiermee kan de locatie zeer nauwkeurig worden bepaald. Als het geautomatiseerde werk een mobiel apparaat is, zoals een smartphone, die de gebruiker bij zich draagt, dan kan via de locatie van de smartphone de locatie van de gebruiker vastgesteld worden en kunnen diens bewegingen worden gevolgd. De smartphone vervult dan een peilzenderfunctie. Plaatsbepaling op basis van GPS-gegevens kan nuttig zijn in die gevallen waarin andere observatiemethoden niet of onvoldoende tot resultaat leiden of wanneer de verblijfplaats van de verdachte onbekend is.

De leden van de SP-fractie hebben te kennen gegeven de opvatting van de Afdeling advisering te delen, dat het permanent waarnemen wat zich in een woning afspeelt niet veel anders is dan het via software volgen van gegevensstromen. Het stelselmatig observeren in de woning is niet toegestaan, terwijl met de bevoegdheid tot binnendringen tot veel meer gegevens toegang kan worden verkregen en de inbreuk op de privacy nog groter wordt, aldus deze leden. Zij hebben gevraagd waarom dit minder ernstig is dan stelselmatige observatie in de woning door middel van plaatsing van camera's.
De Afdeling advisering onderschrijft dat bij de bestrijding van ernstige misdrijven ook van nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt en acht het wetsvoorstel in zoverre noodzakelijk. Wel behoeft naar het oordeel van de Afdeling de bevoegdheid tot het op afstand binnendringen differentiatie, afhankelijk van de ingrijpendheid van de inbreuk op de persoonlijke levenssfeer die hiermee wordt gemaakt. Anders dan de leden van de SP-fractie lijken te veronderstellen, maakt de Afdeling qua ingrijpendheid van de bevoegdheid tot het doorzoeken en overnemen van gegevens niet de vergelijking met de observatie in de woning, maar met de bestaande opsporingsbevoegdheid waarbij heimelijk wordt binnengetreden in een woning met het oog op opnemen van vertrouwelijke communicatie (art. 126l Sv). De Afdeling wijst erop dat de toepassing van deze opsporingsbevoegdheid is beperkt tot gevallen waarbij een verdenking bestaat van misdrijven waarop gevangenisstraf van acht jaren of meer is gesteld.
Naar aanleiding van het advies van de Afdeling advisering is het wetsvoorstel aangescherpt wat betreft de voorwaarden voor inzet van de bevoegdheid tot het heimelijk binnendringen van een geautomatiseerd werk voor de toepassing van onderzoekshandelingen met het oog op het vastleggen of ontoegankelijk maken van gegevens. Voor het verrichten van deze onderzoekshandelingen is verdenking van een misdrijf vereist dat een ernstige inbreuk op de rechtsorde oplevert en waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaar of meer is gesteld, of een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

De leden van de CDA-fractie hebben gevraagd hoe technisch kan worden voorkomen dat de gebruiker merkt dat zijn GPS is aangezet en/of bepaalde software-applicaties op zijn smartphone worden geïnstalleerd. Het prijsgeven van informatie over de vraag hoe kan worden voorkomen dat de verdachte merkt dat zijn GPS is aangezet en/of bepaalde software-applicaties op zijn smartphone worden geïnstalleerd belemmert de toekomstige inzetbaarheid van die middelen. Op deze vraag kan ik daarom geen antwoord geven.

De leden van de D66-fractie hebben opgemerkt dat in de toelichting een voorbeeld wordt aangehaald van een verdachte met een smartphone met een prepaid-abonnement waarbij via de GPS-locatie kan worden nagegaan waar de verdachte zich bevindt en hebben gevraagd of alleen kan worden binnengedrongen op mobiele telefoons die voorzien zijn van een data-abonnement bij een provider of dat dat ook op prepaid telefoons kan.
Het is mogelijk om op afstand software op een smartphone te installeren waardoor de GPS locatie kan worden geactiveerd. De abonnementsvorm die bij het toestel hoort maakt daarvoor niet uit. Het probleem met een anonieme prepaid abonnement betreft het vaststellen of de verdachte van het feit waarvoor het op afstand binnendringen van het geautomatiseerde werk noodzakelijk is, bijvoorbeeld in het kader van een bevel tot stelselmatige observatie, ook de gebruiker is van het desbetreffende prepaid abonnement. Dit vanwege de wettelijke voorwaarde dat het op afstand

binnendringen van een geautomatiseerd werk een geautomatiseerd werk betreft dat bij de verdachte in gebruik is.

De leden van de D66-fractie hebben gevraagd of de regering de mening deelt dat het op afstand heimelijk aanzetten van een webcam ingrijpender is dan het betreden van een woning, omdat het heimelijk gebeurt en omdat dit het vertrouwen van mensen in digitale technologieën erodeert. De uitvoering van een bevel tot stelselmatige observatie dient, ongeacht de wijze van observatie, plaats te vinden binnen de kaders van artikel 126g Sv. Het heimelijk aanzetten van een webcam in een woning is, evenals heimelijke betreding van een woning, bij toepassing van die bevoegdheid niet toegestaan.

De leden van de D66-fractie hebben gevraagd of de regering de wijzigingen in het Besluit technische hulpmiddelen strafvordering zal voorhangen bij beide Kamers.
Het wetsvoorstel bevat geen voorhangbepaling. Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen.
Tevens hebben deze leden gevraagd om een toelichting op de eisen die de regering in het besluit wil opnemen. Ten slotte hebben zij gevraagd of de regering de mening deelt dat al bij de behandeling van dit wetsvoorstel duidelijk moet zijn welke eisen worden gesteld aan de software.
Het onderzoek in een geautomatiseerd werk met behulp van een technisch hulpmiddel, vindt, anders dan het onderzoek met de traditionele technische hulpmiddelen, plaats in een volledig digitale omgeving. Omwille van de overzichtelijkheid zullen de eisen die aan technische hulpmiddelen voor het doen van onderzoek in een geautomatiseerd werk worden gesteld neergelegd worden in een nieuw besluit, dat wordt toegesneden op het doen van onderzoek in een digitale context. De in de memorie van toelichting aangekondigde aanpassing van het Besluit technische hulpmiddelen strafvordering wordt niet langer voorzien.
Het besluit ter uitvoering van het wetsvoorstel wordt gebaseerd op het uitgangspunt dat de gegevens die met een technisch hulpmiddel worden vastgelegd betrouwbaar, voor derden toetsbaar en niet manipuleerbaar dienen te zijn. In het besluit eisen zullen eisen worden gesteld aan de inrichting en werking van het technische hulpmiddel. Een belangrijke inrichtingseis zal zijn dat de instelling van de software kan worden gedifferentieerd naar het gebruik van verschillende functionaliteiten. Verder zal vereist worden dat de inhoud van de geregistreerde gegevens identiek zijn aan de inhoud van de gedetecteerde gegevens. Ook zullen eisen worden gesteld over de automatische opslag van geregistreerde gegevens op – uitsluitend – de politieserver. Om de onschendbaarheid van de waarnemingen te kunnen waarborgen en manipulatie door derden te voorkomen, zal als eis gesteld worden dat het transport van de signalen vanuit het geautomatiseerde werk naar de server van de politie plaatsvindt via een versleuteld bestand. Bij de keuring zal getoetst worden of de software aan de eisen voldoet. Alleen wanneer de software is goedgekeurd, mag deze worden ingezet voor het doen van onderzoek in een geautomatiseerd werk. Het besluit zal verder als voorwaarde stellen dat de technische handelingen die worden verricht tijdens het onderzoek doorlopend en automatisch op de politieserver worden vastgelegd (logging), zodat controle op de uitvoering van het bevel van de officier van justitie te allen tijde, zowel tijdens het onderzoek als achteraf, mogelijk is.

De leden van de D66 fractie hebben gevraagd of de regering bereid is in het besluit op te nemen dat hacksoftware op apparaten niet in contact mag staan met servers van de maker van de software. Ook hebben deze leden gevraagd of de regering bereid is in het besluit op te nemen dat

hacksoftware geen gebruik mag maken van fouten in software. Zij hebben voorts gevraagd welke software de regering gaat aanschaffen om uitvoering te geven aan de hackbevoegdheid, wat het budget voor de aan te schaffen software is en of de regering software van het HackingTeam gaat aanschaffen.
De software die als technisch hulpmiddel wordt geïnstalleerd zal tijdens de inzet niet in contact staan met de producent van de software. Er zijn diverse technieken beschikbaar voor het binnendringen in een geautomatiseerd werk. Zoals betoogd in de brief over het gebruik van kwetsbaarheden die tegelijk met deze antwoorden aan de Kamer is gezonden, beoogt de regering geen verbod op software die gebruik maakt van kwetsbaarheden, hiervoor kan ook worden verwezen naar de eerdergenoemde brief over het gebruik van kwetsbaarheden. Zodra in het geautomatiseerde is werk binnengedrongen kan met behulp van een technisch hulpmiddel, een softwareapplicatie, onderzoek worden verricht in het geautomatiseerde werk. In het besluit ter uitvoering van het wetsvoorstel zal de technische eis worden gesteld dat door een technisch hulpmiddel geregistreerde gegevens uitsluitend worden opgeslagen op de politieserver. Het gebruik van de software tijdens de onderzoeksfase zal dus plaatsvinden zonder dat de politieserver in contact staat met de leverancier van de software. Over welke software gebruikt gaat worden kunnen in het belang van de opsporing geen uitspraken worden gedaan.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten waarom er niet voor gekozen is de rechter-commissaris aanwezig te laten zijn tijdens het hacken, aangezien bij een huiszoeking de rechter-commissaris wel aanwezig is.
Zoals in de memorie van toelichting is uiteen gezet, vereist het op afstand binnendringen van een geautomatiseerd werk een gedegen voorbereiding, waarbij de eigenschappen van dat werk en de risico's van het binnentreden vooraf in beeld worden gebracht. Zodra het bevel tot het binnendringen door de officier van justitie is opgesteld en de rechter-commissaris een machtiging heeft verleend, kan worden overgaan tot het daadwerkelijk binnendringen van het geautomatiseerde werk. Het bevel wordt in beginsel gegeven voor een periode van ten hoogste vier weken. Het binnendringen in een geautomatiseerd werk betreft echter een handeling waarvan het tijdstip van uitvoering van tevoren niet duidelijk vastligt. Ook kan de duur van de uitoefening van de bevoegdheid binnen de periode van geldigheid van het bevel verschillen, afhankelijk van de aard van de uit te voeren handelingen. Aanwezigheid van de rechter-commissaris tijdens het binnendringen stuit op de bovengenoemde praktische uitvoeringsproblemen. Dit staat er overigens niet aan in de weg dat de rechter-commissaris in een concreet geval kan bepalen dat het binnendringen van een geautomatiseerd werk en/of het verrichten van bepaalde onderzoekshandelingen in zijn aanwezigheid worden verricht. Tenslotte kan er nog op worden gewezen dat de rechter-commissaris niet altijd aanwezig is bij de doorzoeking van een woning. In het geval van dringende noodzaak en indien het optreden van de rechter-commissaris niet kan worden afgewacht, kan de officier van justitie of hulpofficier van justitie een woning doorzoeken (art. 97, eerste en derde lid, Sv). Verder is de rechter-commissaris tijdens de doorzoeking niet altijd permanent aanwezig, bijvoorbeeld in het geval van het gelijktijdig doorzoeken van verschillende plaatsen.

De leden van de D66-fractie hebben gevraagd of het praktisch mogelijk is voor de opsporingsambtenaren om de automatische logging uit te zetten en door te gaan met hacken. De leden van deze fractie hebben tevens de vraag opgeworpen of daarmee een situatie in theorie mogelijk is dat de opsporingsambtenaar gegevens op een apparaat kan zetten die de verdachte niet zelf op het apparaat heeft geplaatst.

Het loggingsproces is zo ingericht dat de loggingsinformatie tijdens de fase van bewijsvergaring te allen tijde blijft functioneren en niet valt te manipuleren, te wijzigen of te verwijderen. De software wordt hierop gecontroleerd alvorens deze kan worden ingezet. Het is praktisch mogelijk de logging uit te schakelen. Echter, dit is altijd zichtbaar in de logginsgegevens, aangezien er dan een verschil zichtbaar zal zijn in de geregistreerde tijd. Een dergelijke onregelmatigheid zal de integriteit en betrouwbaarheid van het bewijsmateriaal aantasten hetgeen aan de bruikbaarheid van het materiaal in de weg staat.
Daarnaast is een duidelijke taakscheiding tussen de technische en de tactische opsporingsambtenaren voorzien. Alleen de technische, daartoe aangewezen ambtenaren hebben toegang tot het systeem van waaruit het op afstand binnendringen van het geautomatiseerde werk wordt uitgevoerd. De tactische opsporingsambtenaren, die feitelijk met de bewijsvergaring het opsporingsonderzoek bezig zijn, hebben daartoe geen toegang. Zij worden voorzien van de gegevens die in het bevel zijn aangeduid waar specifiek om gevraagd is in het bevel en die via bijvoorbeeld de geplaatste software door het technische team worden aangeleverd. Zij hebben zelf geen toegang tot de technische voorzieningen.
In theorie is het mogelijk dat een opsporingsambtenaar gegevens op een apparaat zet die de verdachte niet zelf op het apparaat heeft gezet. Op dit punt wijkt de situatie in de digitale wereld niet af van het analoge domein. Tijdens een huiszoeking kunnen verdovende middelen in een kast worden gelegd en tijdens de doorzoeking van een voertuig kunnen wapens in de kofferbak worden gelegd.
Omdat het onderzoek in een geautomatiseerd werk in een volledig digitale omgeving plaatsvindt, kunnen de handelingen die verricht worden ter uitvoering van het bevel van de officier van justitie doorlopend en geautomatiseerd worden vastgelegd op de politieserver. Het loggingproces is zo ingericht dat deze te allen tijde blijft functioneren, waardoor zowel tijdens het onderzoek als achteraf controle kan plaatsvinden. Als er sprake zou zijn van manipulatie kan dit dus altijd worden achterhaald. De opsporingsambtenaren die lid zijn van een technisch team en belast zijn met de plaatsing, inzet en verwijdering van een technisch hulpmiddel hebben geen toegang tot de server waarop de logging plaatsvindt. Deze is uitsluitend toegankelijk voor daartoe aangewezen deskundige ambtenaren.

De leden van de D66-fractie hebben geconstateerd dat de ontwikkeling van de techniek ertoe leidt dat de reikwijdte van het verbod om een technisch hulpmiddel op een persoon te bevestigen minder strikt dient te worden uitgelegd dan voorheen en hebben gevraagd of dit betekent dat de politie ook de mogelijkheid krijgt «wearables» en «pacemakers» of andere medische apparatuur te hacken. Zij hebben tevens gevraagd of de regering dit wenselijk vindt gezien de gevoelige informatie en het feit dat de apparaten onveilig blijven doordat fouten in de software in stand gehouden worden.
Thans is in de wet bepaald dat een technisch hulpmiddel niet op een persoon wordt bevestigd, tenzij met diens toestemming (artikelen 126g, derde lid, en 126o, derde lid, Sv). Uit de wetsgeschiedenis blijkt dat bevestiging op een persoon inhoudt: op of aan het lichaam of de kleding. Voorgesteld wordt om de bevestiging van een technisch hulpmiddel op een persoon mogelijk te maken in het kader van de stelselmatige observatie van een geautomatiseerd werk. In verband met het stelselmatige karakter dient de officier van justitie in het bevel tot het op afstand binnendringen van een geautomatiseerd werk melding te maken van het voornemen om gebruik te maken van een technisch hulpmiddel dat zich op een persoon of in de kleding van een persoon bevindt. Dit kan een technisch hulpmiddel betreffen dat reeds op de persoon aanwezig is (zoals een mobiele telefoon in de kleding) of dat op de persoon wordt

bevestigd (zoals een peilzender in de kleding). Op grond van de voorgestelde aanpassing van de regeling rond het bevestigen van een technisch hulpmiddel op een persoon of in diens kleding kan ook een «wearable» worden gebruikt, voor zover deze onder het begrip «geautomatiseerd werk» valt. Hoewel een pacemaker onder de definitie van geautomatiseerd werk valt, zullen hierin naar verwachting geen gegevens te vinden zijn die bijdragen aan plaatsbepaling van een persoon. In de praktijk is het tevens moeilijk denkbaar dat er zich een zo zwaar wegend belang voordoet dat het door de leden van deze fractie gesuggereerde binnentreden van een pacemaker proportioneel zou worden geacht. Voor het oordeel van de regering over het in stand houden van fouten in de software wordt verwezen naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de D66-fractie hebben gevraagd of de regering bereid is om de bevoegdheid tot het binnendringen en onderzoek doen in een geautomatiseerd werk niet te laten gelden voor geautomatiseerde werken die zich op (of in) een persoon bevinden.
De huidige techniek maakt het mogelijk om via plaatsing van software op een geautomatiseerd werk een locatiebepaling van dat geautomatiseerd werk te krijgen. Het geautomatiseerde werk functioneert dan als peilzender. Als het geautomatiseerde werk een mobiel apparaat is, zoals een smartphone, wordt het tevens mogelijk om de locatie van de bezitter te bepalen. Omdat plaatsbepaling op basis van GPS-gegevens nuttig kan zijn in die gevallen waarin andere observatiemogelijkheden niet of onvoldoende tot resultaat leiden of wanneer de verblijfplaats van de verdachte onbekend is, wil de regering deze observatiemethode, waarbij een mobiele telefoon fungeert als peilzender, mogelijk maken. Hierdoor kan het voorkomen dat het technisch hulpmiddel, zoals de peilzender in de mobiele telefoon, zich op of aan het lichaam of de kleding bevindt. Een waarborg voor de inzet van dit middel vormt de wettelijke eis van melding door de officier van justitie van het voornemen om tot de inzet hiervan over te gaan in het bevel. Hierdoor is voorafgaande rechterlijke toetsing verzekerd.

2.4 De juridische voorwaarden voor de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie hebben gevraagd hoe de rechterlijke toets voorafgaand mogelijk is nu niet op voorhand duidelijk is of in een geautomatiseerd werk privégegevens zijn opgeslagen. Zij hebben gevraagd of er altijd vanuit dient te worden gegaan dat er mogelijk gestuit wordt op privégegevens en er dus altijd een rechterlijke toets aan vooraf dient te gaan.
Het onderzoek in een geautomatiseerd werk kan meebrengen dat inzage wordt verkregen in communicatie die in elektronische vorm is opgeslagen of vastgelegd. Dit kan aan de orde zijn bij het vaststellen van de aanwezigheid van gegevens, het vastleggen van gegevens die in het geautomatiseerde werk zijn opgeslagen of vastgelegd of de ontoegankelijkmaking van gegevens. Dat niet op voorhand duidelijk is of in een geautomatiseerd werk privégegevens zijn opgeslagen doet hieraan niet af, omdat ernstig rekening moet worden gehouden met de kans dat dit wel het geval is. Met het vereiste van een rechterlijke machtiging is voorzien in rechterlijke tussenkomst voordat de bevoegdheid wordt toegepast. In dit opzicht worden met dit wetsvoorstel gelijke waarborgen geboden ter bescherming van elektronische communicatie als voor de communicatie die met behulp van brief of telefoon wordt overgebracht. Het vereiste van de voorafgaande toetsing door de rechter-commissaris dient aldus ter

bescherming van de burger in zijn grondrechten, ongeacht of daadwerkelijk privégegevens in het geautomatiseerde werk zijn opgeslagen.

De leden van de CDA-fractie hebben gevraagd of de regering de mening deelt dat het verzoek tot machtiging, en dus ook de verlening, zo zorgvuldig maar tegelijkertijd ook zo volledig mogelijk ingekleed dient te worden door politie en justitie.
De regering deelt de mening van de CDA-fractie dat het verzoek tot machtiging, en dus ook de verlening, zo zorgvuldig maar tegelijkertijd ook zo volledig mogelijk ingekleed dient te worden. Een zorgvuldige en volledige administratieve voorbereiding is van essentieel belang voor een afgewogen en zorgvuldige oordeelsvorming in het kader van een strafzaak en voor een transparant strafproces.

De leden van de CDA-fractie hebben gevraagd of rekening wordt gehouden met het aantreffen van mogelijk nieuwe strafbare feiten en zo ja, op welke wijze. Tevens hebben zij gevraagd of ook altijd rekening wordt gehouden met de mogelijkheid dat meerdere personen gebruik kunnen maken van het betreffende apparaat, ook al is deze kring van personen niet precies duidelijk. Tevens hebben zij gevraagd of in dat laatste geval een nieuw bevel dient te worden afgegeven.
Voor de inzet van de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk is een verdenking vereist van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Indien aan de overige wettelijke voorwaarden is voldaan kan worden binnengedrongen in een geautomatiseerd werk dat bij de verdachte in gebruik is. Als in het kader van het onderzoek in het geautomatiseerde werk gegevens rond andere strafbare feiten worden aangetroffen dan die welke aanleiding vormde voor het binnendringen, dan kunnen deze gegevens niet zonder meer worden vastgelegd, omdat de bevoegdheid van het ontoegankelijkmaken van gegevens is beperkt tot de gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd. Als het gaat om gegevens die betrekking hebben op een ander strafbaar feit dan is een aanvullend bevel van de officier van justitie, evenals een aanvullende machtiging van de rechter-commissaris, noodzakelijk. Voor het op afstand binnendringen is vereist dat het geautomatiseerde werk bij de verdachte (art. 126nba Sv), dan wel de persoon jegens wie de bevoegdheid wordt toegepast (art. 126uba/zpa Sv), in gebruik is. Als de verdenking is gericht jegens andere personen bij wie dat werk in gebruik is, dan moet een nieuw bevel worden afgegeven. In dat bevel wordt het misdrijf en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte vermeldt. In het geval het een onderzoek betreft naar georganiseerde criminaliteit dan kunnen de bevoegdheden van Titel V van het Wetboek van Strafvordering worden toegepast. Vereist is dat het bevel een omschrijving van het georganiseerd verband vermeldt, dit is vastgelegd in het voorgestelde artikel 126uba, tweede lid, onderdeel a, Sv. Gelet op de systematiek van de wet ligt het in de rede dat in het bevel tevens wordt vermeld, indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven. Dit vereiste geldt eveneens bij de toepassing van andere bijzondere opsporingsbevoegdheden op grond van deze titel, hiervoor kan worden gewezen op de regeling van de stelselmatige observatie (art. 126o, vierde lid, onderdeel c, Sv), de stelselmatige inwinning van informatie (art. 126qa, derde lid, onderdeel c, Sv), het opnemen van vertrouwelijke communicatie (art. 126s, derde lid, onderdeel c, Sv) en het aftappen van telecommunicatie (art. 126t, tweede lid, onderdeel c, Sv). Naar analogie van deze bepalingen wordt voorge-

steld de tekst van het voorgestelde artikel 126nba, tweede lid, onderdeel a, aan te passen zodat in het bevel tevens wordt opgenomen indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven. Daartoe zal een nota van wijziging worden opgesteld.

De leden van de CDA-fractie hebben gevraagd of het gegeven dat onbekend of juist al duidelijk is dat de gegevens niet in Nederland zijn opgeslagen of vastgelegd, een legitieme grond kan vormen voor de rechter-commissaris om geen machtiging af te geven. Zij hebben tevens gevraagd of de regering de mening deelt dat een gebrek aan informatie op dit punt geen belemmering mag vormen voor het inzetten van de bevoegdheden wanneer de verdenking van strafbare feiten voldoende is aangetoond.
De rechter-commissaris toetst of het bevel van de officier van justitie aan de wettelijke voorwaarden voldoet. Op grond van artikel 539a Sv kunnen opsporingsbevoegdheden buiten het rechtsgebied van een rechtbank worden uitgeoefend, voor zover het volkenrecht dit toelaat. Op grond van de jurisprudentie van de Hoge Raad kan worden aangenomen dat de vraag of 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. Dit komt verderop, naar aanleiding van vragen van de PvdA-fractie over het onderzoek in een geautomatiseerd werk en rechtsmacht, nader aan de orde. Het is echter aan de rechter-commissaris zelf om in een concreet geval de omvang en reikwijdte van de toetsing van het bevel van de officier van justitie te bepalen. In het licht daarvan is het niet bij voorbaat uitgesloten dat de rechter-commissaris in het kader van de toetsing van de rechtmatigheid van de voorgenomen inzet van de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk ook de verhouding met het volkenrechtelijke beschermde soevereiniteitsbeginsel in de beoordeling betrekt. Ook de vraag of een gebrek aan informatie op dit punt een belemmering mag vormen voor het inzetten van de bevoegdheden is aan de rechter-commissaris ter beoordeling, de regering onthoudt zich van een oordeel daarover.

De leden van de CDA-fractie hebben gevraagd of de regering de mening deelt dat het in het belang van de veiligheid van andere landen is indien opsporingsbevoegdheden (aldaar) kunnen worden ingezet. Ook hebben zij gevraagd hoe de regering de wijziging die zij naar aanleiding van het advies van de Raad van State heeft doorgevoerd, uitlegt en of dat niet een afzwakking vormt van de inzet van de voorgestelde bevoegdheid door de opsporingsdiensten.
De mening van de CDA-fractie, dat het in het belang van de veiligheid van andere landen is indien opsporingsbevoegdheden aldaar kunnen worden ingezet, raakt aan zowel praktische als theoretische aspecten rond de toepassing van de uitvoerende rechtsmacht. Het is bij vormen van grensoverschrijdende criminaliteit, waarbij gebruik wordt gemaakt van informatie- en communicatietechnologie, niet bij voorbaat gegeven dat het land van waaruit die criminaliteit wordt gepleegd in eenzelfde mate betrokken is dan het land of de landen waar de gevolgen van die criminaliteit zich voordoen. In die gevallen waarin het land van waaruit die criminaliteit wordt gepleegd niet of in mindere mate door die criminaliteit wordt geraakt, is het eveneens niet of in mindere mate in het belang van de veiligheid van dat land als opsporingsbevoegdheden aldaar kunnen

worden ingezet. Vanuit meer theoretisch perspectief moet worden opgemerkt dat het uitvoeren van een opsporingsbevoegdheid door een land in een ander land raakt aan het volkenrechtelijke beginsel van de soevereiniteit over het eigen grondgebied. Als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden dan is een verzoek om rechtshulp aangewezen. Een rechtshulpverzoek heeft betrekking op het respecteren van de soevereiniteit en de territoriale integriteit van de andere staat en de toepasselijkheid van de eigen wetgeving op dat grondgebied, evenals de bevoegdheid van de andere staat om zelf op te treden tegen inbreuken op de rechtsorde die op het eigen grondgebied worden beraamd of gepleegd.
De Afdeling advisering heeft gewezen op het aanmerkelijke risico dat opsporingshandelingen worden verricht buiten het territorium van Nederland zonder dat hiervoor een grondslag in het volkenrecht bestaat en dat de voorzichtigheid die past bij het zelfstandig optreden ter handhaving tot uitdrukking zou moeten komen in de regelgeving. Naar aanleiding van dit advies is het wetsvoorstel aangepast en dient de officier van justitie, indien daarover wetenschap bestaat, in het bevel te vermelden dat de gegevens niet in Nederland zijn opgeslagen. Hiermee wordt verzekerd dat het aspect van de inbreuk op de soevereiniteit van een andere staat onderwerp vormt van een expliciete afweging door de officier van justitie en de rechter-commissaris. Naar het oordeel van de regering moet deze aanpassing worden gezien als een extra waarborg voor een zorgvuldige voorbereiding van de inzet van de bevoegdheid en niet als een afzwakking van de inzet van de voorgestelde bevoegdheid door de opsporingsdiensten.

De leden van de CDA-fractie hebben de strikte scheiding begrepen die de regering beoogt tussen het opsporingsteam enerzijds en het technische team de bevoegdheden toepast anderzijds. Tegelijkertijd hebben de leden van deze fractie gevraagd of de regering de mening deelt dat in de praktijk juist van belang is dat deze teams goed met elkaar communiceren en geen verdere belemmeringen op dit punt worden opgelegd, ook niet in lagere regelgeving.
De regering acht de hierboven in het antwoord aangegeven scheiding van taken tussen het tactische team en het technische team noodzakelijk. Deze scheiding van functies behoeft de communicatie tussen de teams niet te belemmeren. De gegevens, die op grond van het bevel van de officier van justitie worden verzameld, komen beschikbaar voor de opsporingsambtenaren van het tactische team. Bij het traditionele aftappen van telecommunicatie wordt een soortgelijke werkwijze gevolgd; de tap wordt geplaatst door de Unit Landelijke Interceptie en de opgenomen telecommunicatie is beschikbaar voor de opsporingsambtenaren die zijn verbonden aan het tactische team dat is belast met het opsporingsonderzoek.

De leden van de D66-fractie hebben gevraagd waarom ervoor wordt gekozen om bij algemene maatregel van bestuur te voorzien in de reikwijdte van het wetsvoorstel en deze niet volledig in het Wetboek van Strafvordering te regelen. Voorts wensen deze leden te vernemen wat dit betekent voor de strafvorderlijke waarborgen, die juist noodzakelijk zijn bij het toepassen van een zeer ingrijpende opsporingsbevoegdheid.
Hiervoor heb ik aangegeven, eveneens in antwoord op vragen van de D66-fractie, dat door de aanwijzing bij algemene maatregel van bestuur van de delicten waarvoor de bevoegdheid mag worden ingezet flexibeler ingespeeld kan worden op ontwikkelingen in de computercriminaliteit. De strafvorderlijke waarborgen voor de inzet van de bevoegdheid voor deze delicten zijn identiek aan de waarborgen die gelden bij de inzet voor de opsporing van delicten die bij wet aangewezen zijn. Voor een uitgebreid

overzicht van de juridische voorwaarden die gelden voor de inzet van de bevoegdheid wordt verwezen naar paragraaf 2.4. van de memorie van toelichting. Een belangrijke voorwaarde is dat de officier van justitie pas een bevel kan geven voor onderzoek in een geautomatiseerd werk na voorafgaande toetsing door de rechter-commissaris. Het vereiste van een dringend onderzoeksbelang geldt onverkort: de rechter-commissaris moet op basis van het bevel kunnen vaststellen dat de gegevens niet op een minder ingrijpende wijze kunnen worden verkregen.

De leden van de fractie van D66 hebben gevraagd of de regering voornemens is om de algemene maatregel van bestuur aan de Kamer te doen toekomen in het kader van de verdere behandeling van het wetsvoorstel.
Zoals hiervoor in antwoord op vergelijkbare vragen van deze leden is aangegeven bevat het wetsvoorstel geen voorhangbepaling. Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen.

De leden van de D66 fractie hebben gevraagd hoe de regering meent te gaan voorzien in voldoende specialistische kennis bij de rechterlijke macht, en rechter-commissarissen in het bijzonder, van de technische aspecten die met de toepassing van de bevoegdheid gepaard gaan en de ingrijpendheid van de bevoegdheid bepalen.
De rechtspraak kent sinds 2009 een landelijk opererend Kenniscentrum Cybercrime, dat is ondergebracht bij het Gerechtshof te Den Haag. Het centrum voorziet rechters, raadsheren en gerechtsambtenaren in Nederland van zowel juridische als praktische kennis over computercriminaliteit, zoals computervredebreuk of spam-aanvallen, digitale opsporing en digitaal bewijs.
Het kenniscentrum heeft via intranet een website opgezet waarop onder andere relevante regelgeving, jurisprudentie en wetenschappelijke artikelen uit (vooral) binnen- en buitenland te vinden zijn. Elk kwartaal brengt het kenniscentrum een digitale nieuwsbrief uit met actuele ontwikkelingen over de verslagperiode. Daarnaast verzorgt het kenniscentrum cursussen en presentaties, al dan niet in samenwerking met SSR en al naar gelang de behoefte van de gerechten. Bij sommige gerechten maakt de presentatie van kenniscentrum inmiddels deel uit van het jaarlijkse opleidingscurriculum. Ook fungeert het kenniscentrum als helpdesk voor vragen van justitiële medewerkers in het hele land. De vaste medewerkers worden bijgestaan door een externe begeleidingsgroep met specifieke kennis van cybercrime. Verder organiseert het Kenniscentrum een jaarlijkse Themadag over relevante en actuele thema's uit de digitale wereld. Tot slot fungeert het kenniscentrum als aanspreekpunt voor externe partijen, zoals het NFI, universiteiten, het NCSC, EC3 en de Raad van Europa, en onderhoudt het kenniscentrum contacten met ketenpartners, zoals het openbaar ministerie en de politie, in het bijzonder het Team High Tech Crime van de politie. Aldus blijft het kenniscentrum op de hoogte van relevante ontwikkelingen die vervolgens kunnen worden omgezet in cursussen en presentaties.

De leden van de D66-fractie hebben gevraagd hoe de regering meent te voorzien in voldoende specialistische kennis bij de daartoe aangewezen officieren van justitie die een dergelijk bevel kunnen afgeven. De leden van deze fractie hebben tevens gevraagd of in deze gevallen alleen een rol is toebedacht aan de officier van justitie of dat ook de hulpofficier van justitie hier enige rol heeft en zo ja, welke.
Het openbaar ministerie zorgt binnen het reguliere opleidingsaanbod, zoals via het reguliere opleidingsaanbod Strafrecht van SSR, voor passende kennis en vaardigheden. De hulpofficier van justitie heeft hierin

geen rol, wel kan de hulpofficier van justitie als opsporingsambtenaar zijn betrokken bij de uitvoering van het bevel van de officier van justitie.

De leden van de D66-fractie hebben gevraagd of de regering kan toelichten wat voor soort routers zullen worden binnengedrongen, en of het hier vooral om thuisnetwerken of Wi-Fi-hotspots gaat of ook om zogenaamde enterprise routers die netwerken van internetaanbieders (ISP's) met elkaar verbinden.
Zoals hiervoor reeds aan de orde is gekomen, geschiedt de inzet van de voorgestelde bevoegdheid onder vooraf bepaalde voorwaarden en met passende waarborgen omkleed. In het algemeen is het niet wenselijk specifieke apparaten van de bevoegdheid uit te sluiten. Eén van de doelen van de wet is het verbeteren van de mogelijkheden om cybercriminelen op te sporen en bewijs te vergaren. Het aanwijzen van een specifieke categorie apparaten waar de bevoegdheid niet voor kan worden toegepast, zou betekenen dat cybercriminelen die deze apparaten voor criminele doeleinden gebruiken niet effectief kunnen worden aangepakt en het strafbaar feit onvoldoende kan worden onderzocht. Wel kan de aard van het geautomatiseerde werk reden zijn voor grote terughoudendheid bij de inzet, of bepalend zijn voor besluit tot inzet of het afzien daarvan. Overigens kunnen in het belang van de effectiviteit van de opsporing geen nadere mededelingen worden gedaan over het type router dat op afstand kan worden binnengedrongen.

De leden van de D66-fractie hebben gevraagd of bij het binnendringen van de routers ook de software, de zogeheten firmware, wordt aangepast. De leden van deze fractie hebben tevens gevraagd welke software wordt het binnendringen wordt gebruikt. Deze leden hebben verder gevraagd wat er wordt gedaan met de datapakketjes die de router moet doorgeven, of er aanpassingen worden gedaan aan het routingprotocol en of de datapakketjes worden ingezien door middel van «deep-packet-inspection» of dat alleen de «header» wordt gelezen. Zij hebben tenslotte gevraagd wat er wordt gedaan met de lijsten van IP-adressen die door het binnendringen van een router verkregen worden.
Er kunnen geen uitspraken worden gedaan over de methoden en technieken die opsporingsinstanties gebruiken zodat de opsporingsinstanties hun werkzaamheden goed kunnen blijven uitvoeren. Het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken vormt een onaanvaardbaar risico voor de inzetbaarheid van die middelen. In het belang van de effectiviteit van de opsporing kunnen dan ook geen mededelingen worden gedaan over welke software wordt gebruikt en de mogelijkheid tot aanpassing van de software in het geautomatiseerde werk.
Op de gegevens, die zijn verzameld ten behoeve van de opsporing, is de Wet politiegegevens van toepassing. De gegevens die niet relevant zijn voor de opsporing, zullen conform die wet worden verwijderd. Indien bij het op afstand binnendringen van een router IP-adressen worden aangetroffen dan is het eventuele verdere gebruik van de gegevens afhankelijk van de informatie waar in het bevel specifiek toestemming voor gegeven is.

De leden van de D66-fractie hebben opgemerkt dat het wetsvoorstel spreekt over het afgeven van een bevel en vervolgens een machtiging, en hebben gevraagd wie tijdens de uitvoering van de bevoegdheid toezicht houdt op de toepassing ervan. De leden van deze fractie hebben tevens gevraagd of zij het voorstel juist begrijpen als zij constateren dat alleen wordt voorzien in de zogeheten logging waarin de verrichtte handelingen worden vastgelegd. Indien dat laatste het geval is, dan zouden deze leden graag vernemen wie de logging op juistheid controleert.

Tijdens de uitvoering van het bevel tot het op afstand binnendringen van een geautomatiseerd wordt toezicht uitgeoefend door de leidinggevende functionarissen binnen de opsporingsdienst en door de betrokken officier van justitie. Tevens wordt toezicht uitgeoefend door de rechter-commissaris, in het kader van de afgifte van een machtiging voor de toepassing van de bevoegdheid. Dit is voor de uitvoering van deze bevoegdheid niet anders dan bij het toepassen van andere bijzondere opsporingsbevoegdheden en dwangmiddelen, die zijn onderworpen aan voorafgaande rechterlijke toetsing.
Door de scheiding tussen de werkzaamheden van de technische en de tactische medewerkers is er geen mogelijkheid voor de tactische medewerkers om eigenstandig de werking van de software te beïnvloeden. De logging is een proces dat niet uitgezet of veranderd kan worden zonder dat dit achteraf zichtbaar is. De server waarop de logging plaatsvindt is uitsluitend toegankelijk voor daartoe aangewezen deskundige ambtenaren. De medewerkers van een technisch team die belast zijn met de plaatsing, inzet en verwijdering van een technisch hulpmiddel hebben geen toegang tot de server. Ingeval er tijdens de strafzaak twijfels zouden rijzen over de onderzoekshandelingen die zijn verricht of over de betrouwbaarheid of kwaliteit van het met een technisch hulpmiddel verzamelde gegevens dan kan de rechter, al dan niet op verzoek van de verdachte of diens raadsman, beslissen tot nader onderzoek van de tijdens het onderzoek vergaarde bewijs aan de hand van de gelogde gegevens.

De leden van de D66-fractie hebben gevraagd of de regering de mening deelt dat de definitie van strafbare feiten die bij algemene maatregel van bestuur aangewezen kunnen worden zeer breed is of de regering een overzicht kan geven om welke misdrijven het gaat.
De regering deelt de mening van de leden van de D66-fractie dat de definitie van strafbare feiten die bij algemene maatregel aangewezen kunnen worden zeer breed is, maar meent dat deze mening nuancering behoeft, nu het oordeel hierover afhangt van de strafbare feiten die uiteindelijk worden aangewezen. Dit betreft misdrijven die worden gepleegd met behulp van een geautomatiseerd werk, die een ernstige inbreuk op de rechtsorde opleveren en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders. Het betreft misdrijven als het gebruik van een botnet (art. 138ab, derde lid, Sr), het aanbieden, verspreiden of bezitten van kinderpornografie (art. 240b Sr), de verleiding van een minderjarige tot ontucht (art. 248a Sr) en «grooming» (art. 248e Sr), die veelal met behulp van een geautomatiseerd werk worden gepleegd en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is. In dergelijke gevallen is er vaak geen ander aangrijpingspunt voor de opsporing dan onderzoek doen in het geautomatiseerde werk zelf.

De leden van de ChristenUnie-fractie hebben opgemerkt dat in het Wetboek van Strafvordering vaker gebruik wordt gemaakt van een machtiging van de rechter-commissaris en gevraagd hoe vaak een tapverzoek door de rechter-commissaris wordt afgewezen en hoe vaak de machtiging wordt verleend. Zij hebben tevens gevraagd of daarin ook categorieën van gronden voor afwijzing kunnen worden gelezen.
Er zijn geen cijfers beschikbaar hoe vaak een rechter-commissaris een verzoek tot het verlenen van een machtiging heeft afgewezen. Wel is bekend dat de bevoegdheid tot het tappen van telefoons wordt getoetst door de rechters die niet tevens de strafzaak later behandelen. Er zijn slechts zeer weinig zaken bekend waarin rechtbanken tot het oordeel komen dat de bevoegdheid tot het afluisteren van de telefoon onrechtmatig is toegepast.

De leden van de D66-fractie hebben geconstateerd dat de regering niet geheel gevolg heeft gegeven aan het advies van de Afdeling advisering van de Raad van State om de binnendringingsbevoegdheid meer in lijn te brengen met de proportionaliteits- en subsidiariteitsvereisten in artikel 8 van het EVRM. Deze leden hebben gevraagd of de regering desondanks van mening is dat de juridische risico's met dit wetsvoorstel zijn ondervangen op dit punt.
Aan het advies van de Afdeling advisering op dit punt is deels gevolg gegeven. Met de Afdeling advisering ben ik 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 verdergaande inbreuk op de privacy van de betrokkene oplevert dan wanneer het binnendringen wordt gevolgd door het aftappen van communicatie of de stelselmatige observatie. Beperking van de toepassing van deze onderzoeksbevoegdheden tot zeer ernstige misdrijven, waarop gevangenisstraf van acht jaar of meer is gesteld, zoals de Afdeling advisering voorstelt, is evenwel te beperkend. Dit zou tot gevolg hebben dat de bevoegdheid niet zou kunnen worden ingezet voor een opsporing van een aantal strafbare feiten waarbij het geautomatiseerde werk instrumenteel is maar een lagere wettelijke strafbedreiging kennen. In dergelijke gevallen zijn er echter dikwijls geen andere aanknopingspunten voor de opsporing dan het op afstand heimelijk binnendringen in het geautomatiseerde werk. Ook voor deze gevallen zijn strenge voorwaarden gesteld. Zo is wettelijk vereist dat het gaat om een misdrijf dat bij algemene maatregel van bestuur is aangewezen, dat het misdrijf een ernstige inbreuk op de rechtsorde oplevert en dat er een dringend onderzoeksbelang aanwezig is. Hiermee wordt naar het oordeel van regering voldaan aan de eisen die gesteld worden door artikel 8 van het EVRM. Hierdoor wordt voldoende geborgd dat de inzet van de bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit plaatsvindt.

2.5. De inzet van de bevoegdheid

De leden van de VVD-fractie vragen of toegelicht kan worden op basis van welke informatie een inschatting wordt gemaakt van de barrières voor het onderzoek in een geautomatiseerd werk, in het bijzonder op het gebied van de beveiliging.
De inschatting van de barrières voor het op afstand binnendringen van een geautomatiseerd werk wordt gemaakt op basis van de informatie die is verkregen door het gebruik van openbaar beschikbare gegevens, zoals de vastlegging van IP-adressen in de database van de beheerders, en gegevens die gedurende het opsporingsonderzoek zijn verkregen, bijvoorbeeld door middel van het gebruik van bijzondere opsporingsbevoegdheden zoals het vorderen van gegevens bij derden of het aftappen van telecommunicatie met behulp van een IP-tap. Niet uitgesloten is ook dat eerst wordt binnengedrongen met het oog op de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, waarna de verkregen informatie ten grondslag kan liggen aan beslissingen over het verdere handelen met betrekking tot dat werk. Er is dan sprake van een meer stapsgewijze aanpak, waarbij het handelen voortdurend wordt afgewogen tegen de risico's.

De leden van de VVD-fractie lezen dat de risico's voor het functioneren van het geautomatiseerde werk bij de voorbereiding niet altijd volledig in te schatten zijn en dat de risico's soms volledig(er) in beeld komen nadat er is binnengedrongen. Deze leden vragen of hier nog iets tegenover wordt gesteld en of er een waarborg is die dit probleem ondervangt.
Voor het op afstand binnendringen van een geautomatiseerd werk is een bevel van de officier van justitie vereist. De officier van justitie zal zich

door de betrokken opsporingsambtenaren zorgvuldig laten informeren over de noodzaak van de inzet van de bevoegdheid, en de risico's die daaraan zijn verbonden. Dit is ook van belang voor de afgifte van de machtiging door de rechter-commissaris. Hierboven is reeds aangegeven dat hierbij ook gekozen kan worden voor een meer stapsgewijze aanpak, waarbij op basis van de informatie die is verkregen in het kader van de vaststelling van bepaalde kenmerken van het geautomatiseerde werk beslissingen worden genomen over de verdere aanpak. Voor de inschatting, beheersing en beperking van de risico's voor het systeem is de deskundigheid van de opsporingsambtenaren van het technische team belast met het binnendringen van essentieel belang. Op grond van het voorgestelde artikel 126nba, zevende lid, Sv worden bij of krachtens algemene maatregel van bestuur eisen gesteld aan het deskundigheidsniveau dat van deze opsporingsambtenaren mag worden verwacht.

De leden van de VVD-fractie hebben voorts gelezen dat de officier van justitie en de rechter-commissaris niet bij uitstek deskundig zouden zijn om de technische risico's te beoordelen. Deze leden vragen of zij hun oordeel dienen te baseren op de deskundigheid van de opsporingsambtenaren en zo ja, of er dan nog in voldoende mate is van een onafhankelijke beoordeling.
Het is van belang dat het openbaar ministerie en de zittende magistratuur over voldoende ICT-kennis beschikken om de inzet van de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk adequaat te kunnen toetsen. Het openbaar ministerie heeft de expertise over computercriminaliteit centraal ondergebracht bij het landelijk parket. Voor de zittende magistratuur is een Kenniscentrum Cybercrime opgericht bij het Gerechtshof in Den Haag.
Het opsporingsonderzoek vindt plaats onder verantwoordelijkheid van de officier van justitie. In een opsporingsonderzoek is het, voorafgaand aan de inzet van de bevoegdheid tot het doen van onderzoek in een geautomatiseerd werk, nodig om een beeld te krijgen van de toegang tot het geautomatiseerde werk en de risico's daarbij. Voor het beoordelen van de risico's is het van belang dat de kenmerken van het geautomatiseerde werk zo goed mogelijk in kaart worden gebracht, zodat zeker kan worden gesteld dat de bevoegdheid wordt uitgeoefend ten aanzien van het juiste geautomatiseerd werk en de juiste persoon. Deze informatie wordt door de officier van justitie gebruikt in zijn afweging over de afgifte van een bevel tot onderzoek in het geautomatiseerde werk. De technische risico's komen aan de orde in het kader van de proportionaliteits- en subsidiariteitsafweging die de officier van justitie maakt bij de inzet van de bevoegdheid. Voor de inschatting hiervan is de deskundigheid van de technisch zeer gespecialiseerde opsporingsambtenaren van het technische team van groot belang. Zij beschikken bij uitstek over de technische expertise en dienen de officier van justitie in staat te stellen een afweging te maken. Net als bij andere afwegingen zal de officier van justitie daarom voor de informatie op basis waarvan de afweging gemaakt wordt steunen op de expertise van de opsporingsambtenaren. Indien wenselijk, kan de officier van justitie een stapsgewijze aanpak hanteren en bepalen dat een bevel wordt afgegeven voor het bepalen van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker. Als gedurende het onderzoek blijkt dat verdergaande handelingen nodig en verantwoord zijn, kan de officier van justitie het bevel stapsgewijs uitbreiden. De officier van justitie behoeft voor de afgifte het bevel een schriftelijke machtiging van de rechter-commissaris. Het bevel dient voldoende informatie te bevatten voor de rechter-commissaris om de reikwijdte van het onderzoek te toetsen en een proportionaliteits- en subsidiariteittoets te verrichten met betrekking tot de inzet van de bevoegdheid.

De leden van de VVD-fractie hebben gevraagd of in de Contourennota Rijksrecherche en het opleidingsaanbod bij de politieacademie rekening wordt gehouden met de steeds grotere vraag bij de politie naar deskundige (technische) opsporingsambtenaren. Zij hebben tevens gevraagd of zowel voor de tactische als voor de technische opsporingsdiensten dezelfde screening geldt.
De vraag naar voldoende gekwalificeerd personeel op het gebied van cybercriminaliteit wordt onderkend. De aankomende jaren wordt hier middels door- en zijinstroom van medewerkers invulling aan gegeven (zie het Inrichtingsplan Nationale Politie). Het opleidingsaanbod bij de Politieacademie biedt tal van (verplichte) opleidingen, modules en trainingen aan op het gebied van cybercrime en digitale expertise, zoals Recherchekundige Master Digitaal, digitale opsporing, internet en opsporing, en forensic scripting. De verwachting is dat er voor het verzekeren van voldoende kennis op het gebied van cybercriminaliteit behoefte zal zijn aan specifieke (nieuwe) opleidingen. Gezamenlijk met de Politie Academie zal worden bezien hoe dit in het onderwijsaanbod kan worden opgenomen.
Iedere politieambtenaar wordt gescreend. De zwaarte van de screening hangt af van de te vervullen functie. Dit kan dus verschillend zijn voor de tactiek en/of de techniek.

De leden van de VVD-fractie hebben opgemerkt dat voor de inzet van softwareapplicaties een voorafgaande keuring van het technische hulpmiddel is vereist. De leden van deze fractie hebben gevraagd wie een dergelijke keuring uitvoert.
De keuring van de huidige technische hulpmiddelen die worden gebruikt bij de opsporing wordt uitgevoerd door een gespecialiseerde afdeling van de landelijke eenheid van het landelijk politiekorps politie. Het ligt in de rede om deze keuringsdienst ook aan te wijzen voor de keuring van technische hulpmiddelen voor het doen van onderzoek in een geautomatiseerd werk. Het besluit dat ter uitvoering van het wetsvoorstel wordt opgesteld zal de mogelijkheid bevatten om ook andere organisaties aan te wijzen.

De leden van de VVD-fractie hebben gevraagd of mensen achteraf op de hoogte worden gesteld als hun geautomatiseerde werk, achteraf onterecht, heimelijk is binnengedrongen en zo nee, wat de overwegingen zijn om dit niet te doen.
Net als bij de inzet van andere bijzondere opsporingsbevoegdheden waarbij inbreuk wordt gemaakt op de persoonlijke levenssfeer van de betrokkenen geldt een verplichting tot schriftelijke mededeling (notificatie) aan de betrokkene, zodra het belang van het onderzoek dat toelaat. Dit betreft artikel 126bb van het Wetboek van Strafvordering. De mededeling blijft achterwege indien uitreiking van de mededeling redelijkerwijs niet mogelijk is.

De leden van de VVD-fractie hebben geconstateerd dat het decryptiebevel niet langer in het wetsvoorstel staat en hebben gevraagd welke instrumenten de politie in plaats daarvan ter beschikking staan. Ook hebben zij gevraagd bij de beantwoording eveneens in te gaan op de discussie over zwakheden in het systeem, de zogeheten zero days discussie.
Met het voorstel voor het decryptiebevel aan de verdachte werd beoogd een extra mogelijkheid op te nemen om versleutelde gegevens, die door de opsporingsinstanties redelijkerwijs niet ontsleuteld kunnen worden, te laten ontsleutelen zodat kennis kan worden genomen van de inhoud van die gegevens met het oog op de waarheidsvinding. Hierbij moest echter rekening worden gehouden met de kans dat de verdachte zou weigeren aan het decryptiebevel te voldoen, zodat de gegevens ontoegankelijk zouden blijven voor de opsporing. Met het op afstand binnendringen in

een geautomatiseerd werk kan daadwerkelijk toegang worden verkregen tot de versleutelde gegevens omdat met de toepassing van deze bevoegdheid de gegevens op afstand heimelijk overgenomen en vastgelegd kunnen worden zodat de versleuteling ongedaan gemaakt kan worden. Aldus biedt de inzet van deze bevoegdheid de meeste kans op het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing.
Voor het antwoord op de vraag over het gebruik van kwetsbaarheden verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de PvdA-fractie hebben gevraagd of het voor de verkenning van een geautomatiseerd werk meteen nodig is om op afstand in dat geautomatiseerde systeem binnen te dringen en onderzoek te doen of dat met behulp van andere opsporingsbevoegdheden deze informatie ook verkregen kan worden.
Het is niet altijd nodig om voor de verkenning van een geautomatiseerd systeem op afstand in dat systeem binnen te dringen. Soms kan waardevolle informatie over het systeem worden verkregen door publiek beschikbare gegevens op het internet of door het inzetten van andere bijzondere opsporingsbevoegdheden. Voor het identificeren van het geautomatiseerde werk of van de gebruiker kan de bevoegdheid tot het vorderen van verkeersgegevens (artikelen 126n/u en 126zh Sv) of van de bevoegdheid tot het opvragen van gebruikersgegevens (artikelen 126na/ua en 126zi Sv) worden gebruikt. De bevoegdheid tot het aftappen 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 leden van de PvdA-fractie hebben gevraagd of er een verschil is tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem en zo ja, of daar dan ook verschillende bevoegdheden voor nodig zijn.
In de memorie van toelichting wordt met de term onderzoek in een geautomatiseerd werk gedoeld op het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen. Het binnendringen omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel met behulp waarvan gegevens kunnen worden vastgelegd. Het verrichten van onderzoekshandelingen heeft betrekking op de verschillende bevoegdheden die zijn aangeduid in het voorgestelde artikel nba/uba/zpa, eerste lid, onderdelen a. tot en met e. Deze onderzoekshandelingen betreffen de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of van de gebruiker en de vastlegging daarvan, de vastlegging van gegevens die in het geautomatiseerde werk zijn of worden opgeslagen, de ontoegankelijkmaking van gegevens, de uitvoering van een bevel tot het aftappen van telecommunicatie of opnemen van vertrouwelijke communicatie en de uitvoering van een bevel tot stelselmatige observatie. Voor het binnendringen van een geautomatiseerd werk zijn een bevel nodig van de officier van justitie en een machtiging van de rechter-commissaris. Ditzelfde geldt voor ieder van de afzonderlijke onderzoekshandelingen. Wel kan een bevel of machtiging voor het binnendringen worden gecombineerd met het bevel of machtiging voor de toepassing van een of meer onderzoekshandelingen, zodat één bevel nodig is voor de toepassing van deze bevoegdheden in het geval van onderzoek in een geautomatiseerd werk.

De leden van de PvdA-fractie hebben gevraagd of een computer of afstand kan worden binnengedrongen zonder een machtiging van de

rechter-commissaris voor het op afstand heimelijk onderzoeken van een geautomatiseerd werk.
Voor het op afstand heimelijk binnendringen van een geautomatiseerd werk is, op grond van het voorgestelde artikel 126nba Sv, altijd een machtiging van de rechter-commissaris vereist.

De leden van de PvdA-fractie hebben gevraagd wat er met verdachte informatie gebeurt die al tijdens de verkennende fase in een geautomatiseerde werk wordt gevonden, zoals een map met de naam «kinderporno». Tijdens de verkennende fase wordt het onderzoek in een geautomatiseerd werk voorbereid, geprobeerd wordt een goed beeld te verkrijgen van de mogelijkheden om daadwerkelijk toegang te krijgen tot het geautomatiseerde werk en de daaraan verbonden risico's. Tijdens die fase wordt echter niet binnengedrongen in het geautomatiseerde werk, er kan dan evenmin verdachte informatie in dat werk worden gevonden.

De leden van de PvdA-fractie hebben gevraagd of er technisch gezien andere mogelijkheden dan via systeemzwakten om een geautomatiseerd werk binnen te dringen zijn en zo ja, welke mogelijkheden dat zijn. De leden van deze fractie hebben tevens gevraagd of de politie zelf op afstand zwakten in een systeem kan aanbrengen. Deze leden hebben voorts gevraagd in welke mate systeemzwakten van belang zijn voor de politie om een geautomatiseerd systeem binnen te dringen en of via het lek dat de politie zelf creëert of waar het gebruik van maakt ook anderen dat systeem kunnen binnendringen. Tenslotte hebben zij gevraagd waarom «exploits» als kwetsbaarheid wel snel opgelost kunnen worden en de andere manieren die de politie gebruikt om een systeem binnen te dringen niet onschadelijk kunnen worden gemaakt.
Om binnen te dringen in een geautomatiseerd werk zijn verschillende technieken mogelijk. Er kan bijvoorbeeld worden binnengedrongen door het verkrijgen van inloggegevens door zogenoemde social engineering, door inlichtingenwerk, of door in overleg met beheerders toegang tot een systeem of gegevens te verkrijgen. Deze opties zijn echter niet in elke casus bruikbaar of succesvol. Bijvoorbeeld wanneer het gaat om technisch capabele criminelen die zich bewust zijn van het feit dat de politie naar hen op zoek is, en daarom alles in het werk stellen toegang tot informatie over strafbare feiten voor de politie verborgen te houden.
Voor de vragen over het gebruik van kwetsbaarheden door de politie verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden. Overigens wordt opgemerkt dat de politie gedurende de bevoegdheidsuitoefening wel een duidelijk belang kan hebben de beveiliging van een systeem van een verdachte niet verder te verzwakken in verband met attributie van hetgeen daar wordt aangetroffen aan een verdachte. Indien derden onbeperkte toegang zouden hebben levert dit mogelijk problemen op met bewijsgaring of verweren.

De leden van de PvdA-fractie hebben gevraagd wie de voorafgaande keuring van het technische hulpmiddel uitvoert van de softwareapplicaties.
Voor het antwoord op deze vraag wordt verwezen naar het antwoord op een eerdere, soortgelijke vraag van de leden van VVD-fractie.

De leden van de PvdA-fractie zouden niet graag zien dat door de politie aangetroffen zwakheden in een systeem verhuld blijven omdat de politie die zwakheden voor opsporingsdoeleinden wil blijven gebruiken en hebben gevraagd hoe de bevoegdheid om op afstand heimelijk een geautomatiseerd werk te onderzoeken zich verhoudt tot de plicht om datalekken te melden. De leden van deze fractie hebben tevens gevraagd of ook de politie aan die meldplicht gehouden is.

De Wet meldplicht datalekken voorziet in een verplichting voor de verantwoordelijke om de Autoriteit Persoonsgegevens onverwijld in kennis te stellen van een inbreuk op de beveiliging waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens die door hem worden verwerkt (art. 34, eerste lid, Wbp). De politie is echter geen verantwoordelijke voor de gegevens, waarin op afstand wordt binnengedrongen, als bedoeld in de Wet bescherming persoonsgegevens. De politie is dan ook niet gehouden om een datalek, dat is aangetroffen in het kader van de toepassing van de voorgestelde bevoegdheid van artikel 126nba/uba Sv aan de Autoriteit Persoonsgegevens te melden. In daarvoor in aanmerking komende gevallen zal de politie de verantwoordelijke in kennis stellen van het feit dat de beveiliging van het systeem zodanig tekort schiet dat dit kan leiden tot nadelige gevolgen voor de bescherming van persoonsgegevens. Op grond van de wettelijke meldplicht kan de verantwoordelijke gehouden zijn die inbreuk ter kennis te brengen van de AP. Voor de vragen over het gebruik van kwetsbaarheden door de politie verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden. Overigens kan nog worden opgemerkt dat de richtlijn gegevensbescherming opsporing en vervolging, die dit voorjaar door de Raad en het Europees parlement is goedgekeurd[3], voorziet in een verplichting voor opsporingsinstanties om een datalek te melden aan de toezichthoudende autoriteit (artikel 30). Dit betreft echter een datalek bij de opsporingsinstantie zelf. De richtlijn gegevensbescherming opsporing en vervolging moet binnen twee jaar in de Nederlandse wetgeving worden geïmplementeerd.

De leden van de PvdA-fractie hebben gevraagd in hoeverre het doel van de bescherming van de cybersecurity, daaronder de integriteit en veiligheid van het internet begrepen, kan botsen met het doel van het voorkomen van cybercrime waaronder het onderzoeken van geautomatiseerde werken.
Voor het antwoord op deze vragen verwijs ik naar de brief over het gebruik van kwetsbaarheden die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de PvdA-fractie hebben gevraagd of een eigenaar van een geautomatiseerd werk die merkt dat derden zijn werk binnendringen gerechtigd is om daar maatregelen tegen te nemen, ook al gebeurt dat binnendringen door een daartoe bevoegde opsporingsambtenaar. Ook hebben deze leden gevraagd of die eigenaar onderscheid kan maken tussen iemand die het geautomatiseerde werk met verkeerde bedoelingen binnendringt en een opsporingsambtenaar. Vergelijkbare vragen worden gesteld over de eigenaar van een server die niet zelf verdachte is. Meer specifiek wensten deze leden te vernemen of het uitmaakt of de eigenaar van de server specifieke maatregelen neemt gericht tegen de aanval van buitenaf of dat hij generieke maatregelen neemt om de beveiliging van zijn hard- en software beter te beveiligen.
Er zijn verschillende technieken beschikbaar die het mogelijk maken in een geautomatiseerd werk van een verdachte of dat bij een verdachte in gebruik is, zoals serverruimte, binnen te dringen, daarbij eventuele beveiligingen te omzeilen en software te installeren met behulp waarvan bepaalde onderzoekshandelingen kunnen worden verricht. De eigenaar

[3] Richtlijn 2016/1680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

van een geautomatiseerd werk is te allen tijde gerechtigd om maatregelen te nemen om zijn computer te beschermen tegen aanvallen van buitenaf, bijvoorbeeld door het installeren van een virusscanner. Als hierdoor het opsporingsonderzoek wordt verstoord, dan zal een andere methode moeten worden gezocht om in het geautomatiseerde werk binnen te dringen. De eigenaar mag bij de bescherming van een geautomatiseerd werk echter niet zover gaan dat hij een strafbaar feit pleegt. Het wederrechtelijk binnendringen in een geautomatiseerd werk is als computervredebreuk strafbaar gesteld (art. 138ab Sr), handelingen zijn aan te merken als «terughacken» zijn derhalve niet toegestaan. De eigenaar van een geautomatiseerd werk kan, als hij de software zou ontdekken, in beginsel geen onderscheid maken tussen iemand die het geautomatiseerde werk met verkeerde bedoelingen binnendringt en een opsporingsambtenaar. Ditzelfde geldt voor de eigenaar van een server die niet zelf verdachte is. Het maakt daarbij niet uit of de eigenaar van de server specifieke maatregelen neemt gericht tegen de aanval van buitenaf of dat hij generieke maatregelen neemt om de beveiliging van zijn hard- en software beter te beveiligen.

De leden van de SP-fractie hebben gevraagd of het van belang kan zijn voor de overheid om lekken in software niet te dichten, en in hoeverre een softwarefabrikant, eindgebruiker of het Nationaal Cyber Security Centrum (NCSC) op de hoogte wordt gesteld van een kwetsbaarheid als deze is geconstateerd door opsporings- instanties, vooral waar het gaat om fouten of lekken die ondanks updates blijven bestaan. De leden van deze fractie hebben tevens gevraagd of deze aan hen worden gemeld zodat deze kunnen worden opgelost.
Voor het antwoord op deze vragen verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de SP-fractie hebben opgemerkt dat de regering stelt dat de politie geen baat heeft bij instandhouding van onbeveiligde systemen vanwege de maatschappelijke kosten en hebben gevraagd of de regering dit nader kan toelichten. De leden van deze fractie hebben tevens gevraagd of politie en Openbaar Ministerie (OM) ook heimelijk kunnen binnendringen zonder gebruik te maken van «zero days», of dat er per definitie kwetsbaarheden nodig zijn.
Voor het antwoord op deze vraag verwijs ik naar het eerdere antwoord op een eerdere vraag van de leden van de PvdA fractie over andere mogelijkheden om een geautomatiseerd werk binnen te dringen dan via systeemzwakten, en naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de SP-fractie hebben gevraagd hoe de conclusie van het in april 2015 verschenen rapport van de WRR («De publieke kern van het internet») dat het functioneren en de integriteit van de publieke kern van het internet veilig gesteld moet worden en beschermd moet worden tegen oneigenlijke interventies door staten en andere partijen, in verhouding staat tot de hackbevoegdheid voor opsporingsdiensten.
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. De AIV spreekt van het internet als een «mare liberum», waarbinnen de staat zich dient te beperken tot het borgen van de juridische kaders van de rechtsstaat en het beschermen van de burgerlijke vrijheden. 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. De «mare liberum»-vergelijking biedt goede aanknopingspunten, maar gaat niet volledig op omdat veiligheid en het respecteren van mensenrechten 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 en tegen deze bedreigingen op te treden 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 het kabinet 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.

De leden van de SP-fractie hebben gevraagd hoe wordt voorkomen dat het heimelijk binnendringen uiteindelijk meer standaard wordt dan uitzondering.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een vraag van de leden van de PvdA-fractie over hoe wordt voorkomen dat de nieuwe bevoegdheid te gemakkelijk wordt ingezet omdat bestaande bevoegdheden, zoals het plaatsen van een technisch hulpmiddel om gegevens te tappen of het in beslag nemen van gegevensdragers, wellicht moeilijker in te zetten zijn (paragraaf 2.1).

De leden van de SP-fractie lazen over «social engineering» en het verleiden van personen om te reageren op bijvoorbeeld een emailbericht teneinde inloggegevens te verkrijgen en hebben gevraagd waarom deze opsporingsmethodes niet voldoende zijn.
De «social engineering» en het verleiden van personen om te reageren op bijvoorbeeld een emailbericht zijn methoden om de inloggegevens te verkrijgen zodat een geautomatiseerd werk op afstand heimelijk kan worden binnengedrongen. Thans bestaat er echter geen bevoegdheid om een geautomatiseerd werk op afstand heimelijk binnen te dringen, deze bevoegdheid wordt in dit wetsvoorstel voorgesteld.

De leden van de SP-fractie vinden het opvallend dat Duitsland en Frankrijk hebben afgezien van het gebruik van spyware, omdat oneigenlijk gebruik van derden niet viel uit te sluiten, en hebben gevraagd waarom dit argument niet voor Nederland geldt. Ook hebben zij gevraagd hoe groot dit risico is.
Het is de regering niet bekend of Duitsland en Frankrijk afzien van het gebruik van spyware, noch welke redenen hieraan ten grondslag zouden liggen. Voor wat betreft de afwegingen die aan de keuze van de Nederlandse regering ten grondslag liggen kan het volgende worden toegelicht. Zodra sprake is van een technische kwetsbaarheid in een geautomatiseerd werk bestaat per definitie de kans dat derden van die kwetsbaarheid gebruik maken. De regering is er echter van overtuigd dat voldoende maatregelen zijn genomen om misbruik van derden te voorkomen, zoals de keuring van het technisch hulpmiddel. Bovendien neemt de politie maatregelen om te voorkómen dat anderen bij de inzet van de bevoegdheid van dezelfde kwetsbaarheid gebruik kunnen maken. Hierbij kan worden gedacht aan het vooraf analyseren van het werk, het direct na

het binnendringen eerst nader analyseren ten behoeve van een verbeterde risico-inschatting, het sterk beperken van de tijd van het contact tussen het te onderzoeken systeem en het systeem van de politie, en het monitoren van activiteiten van het betrokken deel van het te onderzoeken systeem. Dergelijke maatregelen zijn niet alleen van belang voor het beperken van de kans dat derden van dezelfde kwetsbaarheid gebruik maken, maar ook om het risico op onderkenning van de opsporingsactiviteiten te beperken en de integriteit van het bewijs zeker te stellen.

De leden van de SP-fractie hebben opgemerkt dat in de memorie van toelichting wordt gesproken over het belang van goede keuring. Het is deze leden niet duidelijk waarom Duitsland en Frankrijk dit niet voldoende hebben geacht om alsnog gebruik te maken van spyware.
Het is mij niet bekend door welke feiten de keuzes, die door de Franse en Duitse autoriteiten zijn gemaakt, zijn ingegeven.

De leden van de CDA-fractie hebben gevraagd hoe van tevoren kan worden vastgesteld welke programma's zijn geïnstalleerd, wat voor bestandsmappen er zijn, wat het besturings- systeem is, wie er allemaal gebruik van maakt, en of dit niet juist allemaal onderdelen zijn die door toepassing van de bevoegdheid inzichtelijk moeten worden voor politie en justitie.
De elementen die door de leden van de CDA-fractie zijn genoemd betreft gegevens die nodig zijn om vast te stellen hoe het geautomatiseerde werk functioneert en hoe het door de gebruiker wordt gebruikt. Dit is behulpzaam om de juiste afweging te kunnen maken hoe het werk het beste benaderd kan worden, gericht op zowel het voorkomen dat de gebruiker het binnendringen opmerkt als op het verzamelen van gegevens waar de politie en het openbaar ministerie naar op zoek zijn. In bepaalde gevallen is het mogelijk dat deze informatie inderdaad pas te verkrijgen is nadat de bevoegdheid is toegepast. Alsdan kan, in overleg met de rechter-commissaris, worden gekozen voor een meer stapsgewijze aanpak, waarbij de onderzoeksbevindingen aanleiding kunnen geven tot een aanvullend bevel van de officier van justitie en een aanvullende machtiging van de rechter-commissaris voor het verrichten van nadere onderzoekshandelingen in het geautomatiseerde werk.

De leden van de CDA-fractie hebben gevraagd wat precies de formele voorwaarden zijn in de praktijk. Juist omdat niet duidelijk is wat kan worden aangetroffen, zal nooit een volledige inschatting te maken zijn van de inbreuk op de persoonlijke levenssfeer of de schade die optreedt aan de software van de gebruiker, en deze leden hebben daarom gevraagd of met een «uitgebreide» afweging in dit kader niet vooral een «zorgvuldige» afweging wordt bedoeld. Deze leden zijn van mening dat een globale risico-inschatting gewenst is, maar meenden dat voorkomen moet worden dat opsporingsambtenaren in de praktijk per casus een volledig boekwerk moeten opstellen over de details van het apparaat dat zij op het oog hebben en de omvang van de operatie die met het inzetten van de bevoegdheid gepaard gaat. Zij hebben gevraagd of de regering dat ook zo ziet en hoe dit vorm krijgt in onderhavig wetsvoorstel en/of lagere regelgeving.
Hoe uitgebreid vooraf onderzoek en documentatie nodig zijn, is zeer afhankelijk van het geval en de bekendheid met het type geautomatiseerd werk. Indien de aard van het geautomatiseerde werk bekend is, en hier na verloop van tijd meer ervaring mee is opgedaan, zal de inzet die nodig is voor een goede risico-inschatting kleiner zijn. Hierboven is, naar aanleiding van vragen van de leden van andere fracties, reeds de mogelijkheid van een stapsgewijze benadering aan de orde gekomen, waarbij op basis van de verkregen informatie beslissingen worden genomen over het verdere handelen rond het geautomatiseerde werk. De

risico's van de inzet worden mondeling besproken met de officier van justitie in het zogenaamde «juridisch-operationeel overleg». Deze werkwijze wordt nu al gevolgd als het gaat om bijzondere operaties voor bijvoorbeeld de inzet van de bevoegdheid tot het opnemen van vertrouwelijke communicatie. Deelnemers aan het overleg zijn de officier van justitie, de teamleider, een jurist en een technisch opsporingsambtenaar. Tijdens het overleg wordt mondeling uitleg gegeven over eventuele gevaarzettende situaties. In de praktijk is er sprake van voortdurend overleg tijdens de inzet. Ter illustratie kan worden opgemerkt dat het bij de inzet van het direct afluisteren thans voor komt dat dagelijks meer dan twintig keer telefonisch contact is met de officier van justitie.

De leden van de CDA-fractie hebben gevraagd hoe kan worden aangetoond dat bepaalde apparatuur en/of software daadwerkelijk is beschadigd door ingrijpen van de politie of dat het niet gewoon ouderdom van het apparaat betreft dan wel fouten in de oorspronkelijke software.
Indien een betrokkene meent dat bepaalde apparatuur en/of software is beschadigd door ingrijpen van de politie, dan kan hij zich bij de burgerlijke rechter vervoegen met een beroep op de onrechtmatige (overheids)daad (art. 6:162 BW). Daarbij geldt als hoofdregel dat degene die schade claimt, (zo nodig) moet bewijzen dat de schade is veroorzaakt door degene die daarop in rechte wordt aangesproken («wie eist bewijst»). Het is dan ook in eerste instantie aan de gebruiker om aan te tonen dat de apparatuur en/of software daadwerkelijk is beschadigd door het ingrijpen van de politie. Zo zou deze een deskundigenrapport kunnen overleggen waarin de schade, de oorzaak en het causale verband worden omschreven. Op basis van die inbreng kan de rechter de politie opdragen om aan te tonen dat de beschadiging niet is veroorzaakt vanwege het optreden van de politie. De logging van de gegevens door de politie zal dan helderheid kunnen bieden over de technische handelingen die hebben plaatsgevonden ter uitvoering van het bevel van de officier van justitie. Het is uiteindelijk aan de rechter om te bepalen of en in hoeverre er aanleiding bestaat om schadevergoeding toe te kennen.

Deze leden vernamen graag of de regering nog meer voorbeelden en/of uitzonderingen in gedachten heeft en hoe zij dit verwerkt in de aangekondigde regeling voor schadevergoeding.
Dit is niet het geval. Uitgangspunt voor het onderzoek naar de mogelijkheid van een algemene regeling voor schadevergoeding naar aanleiding van strafvorderlijk overheidsoptreden is dat de civielrechtelijke regels voor de verdeling van de bewijslast niet worden gewijzigd.

Ook hebben deze leden de regering gevraagd heel expliciet de bewijslast voor eventueel ontstane schade neer te leggen bij de gebruiker, gelet op de administratieve en juridische lasten die dit met zich mee zou brengen voor de politie, maar ook in het licht van het voorkomen van een claimcultuur.
Zoals hierboven is aangegeven ligt de bewijslast op grond van het civiele recht in eerste instantie bij de gebruiker van het geautomatiseerde werk en bestaat er geen aanleiding om dit te wijzigen. Het nader expliciteren van de bewijslastregel is evenmin nodig, aangezien deze regel reeds onderdeel is van de grondbeginselen van het burgerlijk recht.

Deze leden hebben de regering voorts gevraagd om aan te geven of zij maximumbedragen aan de vergoedingen in gedachten heeft bij de voorgestelde regeling. Dit bijvoorbeeld gelet op de mogelijkheid dat iemand die onherroepelijk is veroordeeld voor het vervaardigen en verspreiden van kinderpornografie, vervolgens met duizenden euro's door de Staat gecompenseerd wordt voor eventuele schade aan diens apparaat

of software. Ook hebben zij gevraagd of de regering de mening deelt dat dit laatste niet is uit te leggen aan slachtoffers en/of nabestaanden van ernstige misdrijven.
De regering heeft thans geen gedachten over eventuele maximumbedragen. De jurisprudentie geeft daartoe ook geen aanleiding omdat de civiele rechter in beginsel geen grondslag ziet voor de vergoeding van strafvorderlijke schade indien de betrokkene onherroepelijk is veroordeeld. Dat is slechts anders indien er voor het strafvorderlijk optreden vanaf de aanvang een rechtvaardiging heeft ontbroken doordat dit optreden, beoordeeld naar het tijdstip waarop het plaatsvond, in strijd was met het geschreven of ongeschreven recht. Dat is bijvoorbeeld het geval indien er geen sprake was van een redelijk vermoeden van schuld als bedoeld in artikel 27 Sv of bij het toepassen van bepaalde bevoegdheden zonder de daartoe vereiste machtiging van de rechter-commissaris. In de situatie die door de leden van de CDA-fractie wordt geschetst, is het niet waarschijnlijk dat een dergelijke omstandigheid zich voordoet. Bovendien wordt door de strafrechter in de strafzaak al rekening gehouden met eventuele vormverzuimen (art. 359a Sv), waardoor de rol van de civiele rechter op dit punt tot een minimum beperkt zal blijven.

De leden van de D66-fractie hebben opgemerkt dat vier fasen worden beschreven die plaatsvinden bij toepassing van de bevoegdheden en hebben gevraagd of voor iedere afzonderlijke fase een bevel door de officier van justitie en een machtiging door de rechter commissaris wordt afgegeven.
In paragraaf 2.5 van de memorie van toelichting worden drie fasen beschreven rond de inzet van de voorgestelde bevoegdheid, te weten de verkennende fase (fase I), het onderzoek in een geautomatiseerd werk (fase II) en de afsluiting van een onderzoek in een geautomatiseerd werk (fase III). Zoals hierboven, naar aanleiding van vragen van de leden van de PvdA-fractie over het verschil tussen het binnendringen in een geautomatiseerd systeem en het onderzoeken van een dergelijk systeem aan de orde is gekomen (paragraaf 2.5), wordt met de term onderzoek in een geautomatiseerd werk gedoeld op het op afstand heimelijk binnendringen in een geautomatiseerd werk en het verrichten van bepaalde onderzoekshandelingen. Het binnendringen omvat veelal het plaatsen en verwijderen van een technisch hulpmiddel met behulp waarvan gegevens kunnen worden vastgelegd. Het verrichten van onderzoekshandelingen heeft betrekking op de verschillende bevoegdheden die zijn aangeduid in het voorgestelde artikel nba/uba/zpa, eerste lid, onderdelen a. tot en met e. Voor het binnendringen van een geautomatiseerd werk is een bevel nodig van de officier van justitie en een machtiging van de rechter-commissaris. Ditzelfde geldt voor ieder van de afzonderlijke onderzoekshandelingen. In alle gevallen betreft dit fase II rond de inzet van de voorgestelde bevoegdheid.

De leden van de D66-fractie hebben gelezen dat in de fase van het onderzoek van het geautomatiseerd werk eventueel een technische hulpmiddel wordt geplaatst, en hebben de regering gevraagd aan te geven in welke gevallen het niet nodig is een technisch hulpmiddel te plaatsen en toch een geautomatiseerd werk binnengedrongen kan worden.
In bepaalde gevallen kan het plaatsen van een technisch hulpmiddel achterwege blijven. Dit is bijvoorbeeld het geval als de benodigde gegevens direct na het binnendringen kunnen worden ingezien of overgenomen ten behoeve van het vaststellen van de identiteit van het geautomatiseerde werk op basis van het voorgestelde art. 126nba lid 1 sub a. De vraag of een technisch hulpmiddel noodzakelijk is, is onder meer afhankelijk van de aard van de inzet, de aard van het geautomati-

seerde werk en de vraag of de gegevens zonder technisch hulpmiddel als rechtmatig bewijs kunnen worden vergaard.

De leden van de D66-fractie hebben de regering gevraagd aan te geven op wat voor manier, zonder de hackbevoegdheid te gebruiken, vastgesteld kan worden welke programma's zijn geïnstalleerd en welke bestandsmappen aanwezig zijn op het geautomatiseerde werk. De leden van deze fractie hebben tevens gevraagd welke open bronnen bedoeld worden en welke bijzondere opsporingsbevoegdheden kunnen worden ingezet om inloggegevens te achterhalen. Deze leden hebben verder gevraagd of het klopt dat in de praktijk al in de verkennende fase routers gehackt moeten worden om al deze informatie van geautomatiseerde werken te verzamelen. De leden van deze fractie hebben voorts gevraagd wat er met de informatie van geautomatiseerde werken van niet-verdachten gebeurt en of de regering kan aangeven welke software in de verkennende fase wordt gebruikt om de benodigde informatie te verzamelen.
In de memorie van toelichting is aangegeven dat voor het verkrijgen van een beeld van het functioneren van het geautomatiseerde werk gebruik kan worden gemaakt van informatie uit zowel open als gesloten bronnen. Met open bronnen worden alle gegevens bedoeld die openbaar toegankelijk zijn, dit laat zich in zijn algemeenheid moeilijk omschrijven maar hiervoor kan worden gedacht aan informatie op sociale websites. Daarbij kunnen ook bijzondere opsporingsbevoegdheden worden ingezet. Voorbeelden van de bijzondere opsporingsbevoegdheden die kunnen worden ingezet om inloggegevens te achterhalen zijn het vorderen van gegevens bij derden (art. 126nd Sv) en het afluisteren van vertrouwelijke communicatie (art. 126l Sv) door het plaatsen van een keylogger op het toetsenbord. Indien het ten behoeve van het binnendringen in een geautomatiseerd werk noodzakelijk is eerst in een router binnen te dringen, dan geldt ook dit als de inzet van de bevoegdheid tot het op afstand binnendringen van een geautomatiseerd werk. Voor het op afstand binnendringen van die router is dan een bevel van de officier van justitie en voorafgaande machtiging van de rechter-commissaris vereist. Het kan voorkomen dat bij voorbaat vast staat dat een router en een daaraan gekoppeld apparaat beide moeten worden binnengedrongen te behoeve van de opsporing. Het bevel en de machtiging kunnen dan voor die beide apparaten worden afgegeven, uiteraard mits het bevel voldoet aan de daaraan te stellen eisen en de inzet proportioneel wordt geacht. De vraag van de leden van deze fractie wat er gebeurt met de informatie van geautomatiseerde werken van niet-verdachten laat zich niet goed beantwoorden, omdat de voorgestelde bevoegdheid is gericht tot een geautomatiseerd werk dat bij de verdachte in gebruik is. Het is niet uitgesloten dat in het kader van de uitvoering van de voorgestelde bevoegdheid ook gegevens van anderen ter kennis komen van de politie, op dat punt verschilt de situatie niet van die bij de toepassing van andere Bob-bevoegdheden zoals het aftappen van communicatie of het afluisteren van vertrouwelijke communicatie. De verzamelde gegevens kunnen voor het opsporingsonderzoek worden gebruikt; als de gegevens daarvoor niet van belang zijn dan moeten ze worden vernietigd. Over het gebruik van de software in de verkennende fase kunnen geen uitspraken worden gedaan, om te voorkomen dat de taakuitvoering van de opsporingsdiensten wordt belemmerd.

De leden van de D66-fractie hebben gevraagd wat de regering bedoelt met verhullingstechnieken, en of de regering bedoelt dat het kwetsbaarheden in bijvoorbeeld VPN-diensten wil gebruiken.
Criminelen gebruiken vaak geavanceerde technieken om buiten het bereik van de opsporingsdiensten te blijven. Hierbij kan gedacht worden aan anonimiseringstechnieken als TOR en IP-spoofing. Dataverkeer lijkt door deze technieken afkomstig van een ander IP-adres dan in werkelijkheid het

geval is, waardoor de gebruiker niet meer te identificeren is. Juist deze omstandigheid leidt ertoe dat het soms nodig is om in het geautomatiseerd werk van de verdachte te komen, zodat ondanks dergelijke technieken de nodige gegevens kunnen worden verkregen.

De leden van de D66-fractie hebben gevraagd of de regering op de hoogte is van de zogeheten ASML-hack, waar een fout in de software van een VPN-dienst leidde tot economische schade voor het bedrijf. De leden vragen hoe de regering aankijkt tegen de economische consequenties van het gebruiken in plaats van dichten van dergelijke kwetsbaarheden.
Voor het antwoord op de vraag hoe de regering aankijkt tegen het gebruik van kwetsbaarheden verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de D66 fractie hebben een toelichting gevraagd op de vraag waarom hacken via «social engineering» of «phishing» niet voldoende is om de problemen in de opsporing naar cybercrime te overkomen.
Naar aanleiding van de vraag van deze leden wordt opgemerkt dat «social engineering» en «phishing» enkele methoden uit een breder scala zijn om toegang te krijgen tot gegevens die in het kader van de opsporing en de bewijsvoering van belang zijn. Social engineering kan er op gericht zijn de verdachte te bewegen handelingen te verrichten zodat software wordt geplaatst op het geautomatiseerde werk dat hij gebruikt, met behulp waarvan verbinding met een andere computer mogelijk wordt gemaakt of met behulp waarvan inloggegevens kunnen worden meegelezen. Met phishing wordt geprobeerd de verdachte ertoe te bewegen bepaalde vertrouwelijke gegevens prijs te geven, zoals identificerende gegevens of inloggegevens. Bij de toepassing van deze methoden wordt dus uitgegaan van de – veelal onwetende – medewerking van de verdachte of van een derde die het geautomatiseerde werk gebruikt waarvan de verdachte ook gebruik maakt. Deze middelen kunnen uitkomst bieden in bepaalde gevallen, waarin toegang tot gegevens niet mogelijk is zonder dat op afstand wordt binnengedrongen in een geautomatiseerd werk. In andere gevallen zal de verdachte geen medewerking verlenen, gaat het om een geval waarbij een verdachte in het geheel geen communicatiesoftware gebruikt, of gaat het om technisch capabele criminelen die zich bewust zijn van het feit dat de politie naar hen op zoek is, en daarom alles in het werk stellen toegang tot informatie over strafbare feiten voor de politie verborgen te houden. Dan zijn andere middelen nodig om het onderzoek voort te kunnen zetten.

De leden van de D66-fractie hebben erop gewezen dat de regering stelt dat inloggegevens via kunstmatige intelligentie verkregen kunnen worden, en gevraagd of de regering deze techniek nader kan toelichten.
Zonder volledig in te willen gaan op de verschillende methoden en technieken die opsporingsinstanties gebruiken kan wel een voorbeeld gegeven worden van een techniek die gebruik maakt van kunstmatige intelligentie. De opsporingsinstanties kunnen bijvoorbeeld gebruik maken van zogenaamde «brute force», ofwel brute kracht. Dit betreft het gebruik van de rekenkracht van een computer om een probleem op te lossen zonder dat gebruik wordt gemaakt van algoritmen of heuristieken om de berekening te versnellen. Brute force wordt gebruikt als er geen algoritme bekend is dat sneller of efficiënter tot een oplossing leidt. De methode bestaat uit het botweg uitproberen van alle mogelijke opties, net zo lang tot er een gevonden is die overeenkomt met de gewenste invoer. Deze methode wordt ook door criminelen ingezet om wachtwoorden te achterhalen.

De leden van de D66-fractie hebben opgemerkt dat de regering stelt dat «in de derde plaats kwetsbaarheden in een computer kunnen worden geëxploiteerd, zoals het gebruik van fouten of lekken in de software. Hierbij worden in beginsel geen nieuwe kwetsbaarheden gecreëerd». De leden van deze fractie hebben de regering gevraagd nader toelichten wat zij met «in beginsel» bedoelt, en of de mogelijk bestaat dat de regering bedrijven zal dwingen of vragen om kwetsbaarheden in software in te bouwen. Deze leden hebben tevens gevraagd of de regering kan bevestigen dat antivirusbedrijven niet gevraagd zullen worden bepaalde aanvallen door te laten.
De regering zal bedrijven niet dwingen om kwetsbaarheden in software in te bouwen. Het is evenmin voorzien dat antivirusbedrijven wordt gevraagd bepaalde aanvallen door te laten. Het kan echter niet bij voorbaat worden uitgesloten dat een dergelijke keuze in een uitzonderlijk geval in een opsporingsonderzoek aan de orde is. Een dergelijke keuze zal de toets van proportionaliteit en subsidiariteit niet snel doorstaan. In een dergelijk uitzonderlijk geval zullen de directe en maatschappelijke gevolgen van de aanval, de kans op succes in het opsporingsonderzoek en de mogelijkheid de schade te herstellen bij die afweging van belang zijn.

De leden van D66 hebben gewezen op de mogelijkheden van oneigenlijk gebruik door derden van kwetsbaarheden die de politie introduceert en hebben gevraagd of de politie dat succesvol kan voorkomen.
Indien de politie bij de inzet van de bevoegdheid gebruik maakt van een bepaalde kwetsbaarheid, dan neemt de politie maatregelen om te voorkómen dat anderen daar tegelijk gebruik van maken. Hierbij kan worden gedacht aan het vooraf analyseren van het werk, het direct na het binnendringen eerst nader analyseren ten behoeve van een verbeterde risico-inschatting, het sterk beperken van de tijd van het contact tussen het te onderzoeken systeem en het systeem van de politie, en het monitoren van activiteiten van het betrokken deel van het te onderzoeken systeem. Dergelijke maatregelen zijn niet alleen van belang voor het beperken van de kans dat derden van dezelfde kwetsbaarheid gebruik maken, maar ook om het risico op onderkenning van de opsporingsactiviteiten te beperken en de integriteit van het bewijs zeker te stellen. Echter, voor geen enkel systeem dat met internet is verbonden is bij voorbaat volledig uit te sluiten dat dit op een bepaald moment wordt binnengedrongen door bijvoorbeeld criminelen of buitenlandse mogendheden.

De leden van de D66-fractie hebben gevraagd hoe de regering de proportionaliteit van haar voorstel beschouwt om gebruik te gaan maken van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten.
Over de proportionaliteit van het gebruik van technische kwetsbaarheden is geen algemeen antwoord mogelijk. Zodra sprake is van een technische kwetsbaarheid in een geautomatiseerd werk, bestaat per definitie de kans dat derden van die kwetsbaarheid gebruik maken. Het is daarvoor niet van belang of de opsporingsdiensten van die kwetsbaarheid gebruik maken. In beginsel is het de verantwoordelijkheid van de gebruiker om afdoende maatregelen te treffen teneinde te voorkomen dat derden toegang kunnen verkrijgen tot het geautomatiseerde werk. Wel zullen de opsporingsdiensten, zodra zij tijdens het onderzoek in een geautomatiseerd werk merken dat derden gebruik maken van dezelfde kwetsbaarheid om gegevens in het geautomatiseerde werk te manipuleren, maatregelen treffen om te voorkomen dat de integriteit van het bewijsmateriaal wordt aangetast. Dit is hierboven, naar aanleiding van soortgelijke vragen van de leden van de leden van deze fractie en van de leden van de fractie van de SP, reeds aan de orde gekomen.

De leden van de D66-fractie hebben gevraagd of het klopt dat de malware die geïnstalleerd wordt op geautomatiseerde werken in contact staat met een server van de leverancier. De leden van deze fractie hebben tevens gevraagd of het klopt dat de leverancier de mogelijkheid heeft om zelfstandige updates in de malware uit te voeren en zelf de controle over de geautomatiseerde werken over te nemen. Tenslotte hebben zij gevraagd of het klopt dat andere klanten van de leverancier ook toegang kunnen krijgen tot de geautomatiseerde werken die geïnfecteerd zijn met de malware van de leverancier.
Het besluit dat ter uitvoering van het wetsvoorstel wordt opgesteld zal technische eisen stellen aan de softwareapplicaties die voor het onderzoek in een geautomatiseerd werk wordt gebruikt, waaronder de eis uitsluitend gegevens worden opgeslagen op de politieserver. De software zal dus niet in contact staan met de server van de leverancier. De leverancier heeft geen mogelijkheid om zelfstandig updates uit te voeren en zelf de controle over het geautomatiseerde werk over te nemen. Evenmin kunnen andere klanten van de leverancier toegang krijgen tot het geautomatiseerde werk.

De leden van de D66-fractie hebben gevraagd of het klopt dat de mogelijkheid bestaat dat de server van de leverancier die in contact staat met alle geïnfecteerde geautomatiseerde werken gehackt kan worden en de hackers de controle over alle geïnfecteerde geautomatiseerde werken kunnen overnemen.
Dit is niet juist. De opslag van door een technisch hulpmiddel geregistreerde gegevens vindt plaats op een beveiligde politieserver. Er wordt geen gebruik gemaakt van een server van de leverancier van de software.

De leden van de D66-fractie hebben gelezen dat de politie waar mogelijk zal proberen te voorkomen dat anderen van dezelfde zwakheid gebruik maken, en vragen of dit niet vrijwel onmogelijk is en of de regering concrete voorbeelden kan geven waarin dit wel mogelijk is.
Voor het antwoord op deze vraag verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van deze fractie over het door de politie succesvol voorkomen van oneigenlijk gebruik van kwetsbaarheden door derden en het gebruik van technische kwetsbaarheden waarbij misbruik door derden niet valt uit te sluiten Zoals eerder opgemerkt, valt voor geen enkel systeem dat met internet is verbonden bij voorbaat uit te sluiten dat dit wordt binnengedrongen door derden. De regering kan dan ook geen concrete voorbeelden geven waarin dit wel valt uit te sluiten.

De leden van de D66-fractie hebben gelezen dat de politie geen baat heeft bij de instandhouding van onbeveiligde systemen en menen dat dit een zeer tegenstrijdige positie is gezien de feitelijke afhankelijkheid van fouten in de software als gevolg van de hackbevoegdheid. De leden van deze fractie hebben gevraagd of het klopt dat de politie afhankelijk zal zijn van zowel bekende als onbekende fouten in de software.
Voor het antwoord op deze verwijs ik naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de D66-fractie hebben gevraagd of het klopt dat het zeer onwaarschijnlijk is dat de politie de fouten die de aan te kopen software gebruikt om een geautomatiseerd werk binnen te dringen zal melden bij de fabrikant zodat ze gedicht kunnen worden. Zij hebben voorts gevraagd of dit betekent dat de politie een belang heeft bij de instandhouding van onveilige software, en of de regering de mening deelt dat het actueel houden van programma's geen soelaas biedt tegen het gebruiken van onbekende kwetsbaarheden zoals de politie beoogt te doen.

Voor het antwoord op de vraag over het gebruik van kwetsbaarheden verwijs ik de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de D66-fractie hebben gevraagd of de regering de mening deelt dat de politie niet zowel een belang kan hebben bij onveilige software en tegelijk een belang bij het veiliger maken van software.
Die mening deelt de regering niet. Het is in het belang van alle partijen om kwetsbaarheden op internet te verminderen. Tegelijk is het voor een effectieve opsporing en het waarborgen van de nationale veiligheid noodzakelijk toegang te krijgen tot relevante gegevens. Dergelijke gegevens zijn onder meer nodig voor het onderkennen van specifieke dreigingen voor de nationale veiligheid, het bepalen van de strategie in opsporingsonderzoeken, de bewijsvoering en om criminele activiteiten te kunnen stoppen. Deze gegevens zijn veelal, en steeds vaker alleen maar, digitaal en via internet te benaderen.

De leden van de D66-fractie hebben gevraagd of de regering kan aangeven waarom het toch de moeite waard is voor de politie om te kunnen hacken als het zo kostbaar en riskant is. Deze leden hebben tevens gevraagd hoe kostbaar het gebruik van «exploits» precies is.
De overheid kan ten behoeve van de opsporing software produceren of kopen om de bevoegdheid tot binnendringen in een geautomatiseerd werk uit te voeren. De kostbaarheid van deze technische middelen verschilt sterk en is afhankelijk van de aanbieder. Niettemin acht de regering het van groot belang om op afstand een geautomatiseerd werk te kunnen binnendringen om de criminaliteit te kunnen bestrijden en de samenleving te kunnen beschermen tegen allerlei vormen van cybercrime. Nut en noodzaak van de voorgestelde bevoegdheid zijn in paragraaf 2.1 van deze nota naar aanleiding van het verslag en in de memorie van toelichting reeds aan de orde gekomen. In ieder afzonderlijk geval zal de noodzaak van die inzet moeten worden afgewogen tegen de daaraan verbonden risico's. Daarbij zullen ook de kosten van die inzet kunnen worden betrokken. Het publieke belang van de opsporing en vervolging van strafbare feiten in concrete gevallen laat zich bij voorbaat echter lastig in geld uitdrukken.

De leden van de PvdA-fractie hebben de regering gevraagd nader toe te lichten hoe de keuring van de aan te schaffen software eruit zal zien en welke eisen aan de keuring worden gesteld.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de D66-fractie, over de eisen aan de hacksoftware (paragraaf 2.3.5).

De leden van de D66-fractie hebben gevraagd in hoeverre er sprake is van obstructie van politieonderzoek als een persoon de malware van de politie detecteert en verwijdert.
De politie neemt bij de inzet maatregelen om te voorkomen dat een verdachte detecteert dat wordt binnengedrongen. Mocht een verdachte desondanks toch aanvullende beveiligingsmaatregelen nemen, door bijvoorbeeld een beveiligingsupdate uit te voeren, dan is hij hiertoe gerechtigd. In dat geval zullen de opsporingsambtenaren een nieuwe methode om het geautomatiseerde werk binnen te dringen moeten zoeken. Er kan dan inderdaad sprake zijn van obstructie van het onderzoek.

De leden van de D66-fractie hebben geconstateerd dat bij beëindiging van een onderzoek het technische hulpmiddel, de malware, zoveel mogelijk wordt verwijderd en hebben gevraagd of de regering nader kan toelichten wat zij bedoelt met «zoveel mogelijk». De leden van deze fractie hebben

tevens gevraagd of de regering van plan is om bij het binnendringen van routers de firmware aan te passen. Zij hebben voorts gevraagd op wat voor manier de firmware wordt aangepast bij het beëindigen van het onderzoek en of in een dergelijk geval de laatste versie van de firmware wordt geïnstalleerd, ook als dit betekent dat de politie daarna niet meer de router kan binnendringen.
De politie zal op basis van de wet bepaalde methodes toepassen en het systeem zo veel mogelijk achtergelaten als ware er niet in het systeem binnengedrongen. Er kunnen echter sporen van het technische middel in het geautomatiseerde werk achterblijven, die het gevolg zijn van het geïnstalleerde technische hulpmiddel op het geautomatiseerde werk of van handelingen die door het technische team zijn uitgevoegd om het technisch hulpmiddel te plaatsen of te verwijderen. De achtergebleven sporen hebben als zodanig niet of nauwelijks invloed op het functioneren van het geautomatiseerde werk. Wanneer deze sporen risico's opleveren voor het functioneren van het geautomatiseerde werk, is de officier van justitie gehouden de beheerder van het systeem hiervan in kennis stellen en informatie te verstrekken voor volledige verwijdering van de overgebleven sporen. In het belang van de effectiviteit van de opsporing kunnen geen nadere mededelingen worden gedaan over de mogelijkheden tot aanpassing van de firmware.

De leden van de D66-fractie hebben gevraagd hoe de aansprakelijkheid is geregeld in het geval dat bij het plaatsen of verwijderen van een technisch hulpmiddel het geautomatiseerd werk schade berokkend wordt.
De aansprakelijkheid kan in een dergelijk geval worden vergeleken met schade die tijdens een rechtmatige huiszoeking veroorzaakt wordt. Uit vaste jurisprudentie van de Hoge Raad (zie o.m. arrest d.d. 30 maart 2001, NJ 2003, 615 en arrest d.d. 17 november 2004, NJ 2005, 392) volgt dat schade toegebracht tijdens een (strafrechtelijk) rechtmatige huiszoeking onrechtmatig kan zijn. Het toebrengen van onevenredige schade bij een op zichzelf rechtmatige overheidshandeling/ huiszoeking is jegens de getroffene onrechtmatig. Of sprake is van onevenredige schade, dat wil zeggen of de gevolgen buiten het normale maatschappelijk risico of het normale bedrijfsrisico vallen, volgt enerzijds uit de aard van de overheidshandeling en het gewicht van het daarmee gediende belang en in hoeverre die handeling en de gevolgen daarvan voorzienbaar zijn voor de derde die als gevolg daarvan schade lijdt, en anderzijds uit de aard en de omvang van de toegebrachte schade.
Indien de overheid op deze grond aansprakelijk is, kan de vraag rijzen of de op de overheid rustende vergoedingsplicht op de voet van art. 6:101 BW moet worden verminderd of geheel moet vervallen omdat de schade mede een gevolg is van een omstandigheid die aan de benadeelde kan worden toegerekend.

De leden van de D66-fractie hebben gevraagd hoe er op wordt toegezien dat software die is geplaatst om heimelijk te kunnen binnendringen ook weer tijdig van het apparaat wordt verwijderd wanneer dat niet zelfstandig in de software is ingebouwd.
De technische handelingen ter uitvoering van een bevel van de officier van justitie zullen door een speciale eenheid binnen de politie worden uitgevoerd, waar opsporingsambtenaren werkzaam zijn die beschikken over expertise en kennis op het gebied van informatie- en communicatietechnologie. De opsporingsambtenaren van deze eenheid zijn verantwoordelijk voor de correcte uitvoering van de handelingen die in het kader van de uitvoering van het bevel worden verricht, inclusief het verwijderen van het technisch hulpmiddel. De werkzaamheden worden uitgevoerd onder de verantwoordelijkheid van het openbaar ministerie, dat het gezag heeft over de opsporing van strafbare feiten.

Nadat het onderzoek in het geautomatiseerde werk is afgerond zal het geautomatiseerde werk zo veel mogelijk worden achtergelaten als ware er niet in het systeem binnengedrongen. De opsporingsinstanties hebben zelf belang bij een tijdige verwijdering van de software, omdat anders de kans bestaat dat de verdachte die ontdekt en aldus op de hoogte raakt van het opsporingsonderzoek en vervolgens bewijsmateriaal vernietigt. Indien tijdens de strafzaak twijfel ontstaat over de handelingen van het technische team dan biedt de logging van gegevens de mogelijkheid om alle onderzoekshandelingen in dat werk te controleren en te verantwoorden.

De leden van de D66-fractie hebben gevraagd of, indien software en sporen niet verwijderd kunnen worden maar de verdachte achteraf wel is vrijgesproken, er een recht op vergoeding voor eventuele schade bestaat die is toegebracht aan apparatuur door het heimelijk binnendringen en het plaatsen van software.
Naar geldend recht kan een gewezen verdachte op twee manieren aanspraak maken op een schadevergoeding wegens onrechtmatig strafvorderlijk optreden: (a) indien er voor het strafvorderlijk optreden van de aanvang af een rechtvaardiging heeft ontbroken vanwege strijd met het geschreven of ongeschreven recht, of (b) indien uit de uitspraak van de strafrechter of anderszins uit de stukken betreffende de niet met een bewezenverklaring geëindigde strafzaak blijkt van de onschuld van de verdachte en van het ongefundeerd zijn van de verdenking waarop het optreden van politie of justitie berustte (HR 13 oktober 2006, NJ 2007, 432). Het feit dat de gewezen verdachte is vrijgesproken is voor dat laatste echter onvoldoende, omdat een vrijspraak niet altijd behoeft te betekenen dat een verdachte onschuldig was (zie o.a. HR 29 april 1994, NJ 1995, 727 en HR 23 december 1994, NJ 1995, 512).

De leden van de D66-fractie hebben gelezen over een impact analyse naar een schadevergoedingsregeling die in het wetboek zou moeten komen. Die schadevergoeding wordt gekoppeld aan de modernisering van het Wetboek van Strafvordering. Deze leden vinden het een zeer opmerkelijke keuze dat de regering wel onderhavige bevoegdheid apart en vooruitlopend op de modernisering tracht te regelen, maar voor de schadevergoeding verwijst naar de modernisering. Zij hebben gevraagd wanneer de regering verwacht dat de impact analyse naar de schadevergoeding gereed is, en of de regering bereid is de Kamer de impactanalyse toe te sturen voorafgaande aan de verdere behandeling van onderhavig wetsvoorstel.
Ter voorbereiding van de algemene regeling voor schadevergoeding in het Wetboek van Strafvordering is in 2015 een impactanalyse gemaakt met een tweetal scenario's. Deze impactanalyse primair is bedoeld om inzicht te krijgen in de huidige praktijk van de vergoeding van strafvorderlijke schade en bovendien is verricht op basis van een regeling die in het najaar van 2007 in consultatie is gegaan, maar geen vervolg heeft gekregen. De verdere voorbereiding van deze versie van het wetsvoorstel is aangehouden omdat er te veel onzekerheden waren over de financiële gevolgen, de uitwerking en de uitvoering. Toezending van deze impactanalyse aan Uw Kamer voorafgaande aan de verdere behandeling van het wetsvoorstel lijkt dan ook weinig zinvol. In het kader van de modernisering wordt thans een nieuw voorstel opgesteld dat zich momenteel in de ambtelijke voorbereidingsfase bevindt. Voor het nieuwe conceptwetsvoorstel zal een nieuwe en uitvoeriger impactanalyse worden uitgevoerd. In de memorie van toelichting op de nieuwe regeling, die een plaats moet vinden in boek 6 van het wetboek, zullen ook de uitkomsten van de nieuwe impact analyse worden verantwoord.

De leden van de D66-fractie hebben gevraagd wie er actief op toeziet dat, indien de software niet verwijderd kan worden, het dataverkeer vanuit de server van de politie ook daadwerkelijk wordt stopgezet.
Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van een eerdere, soortgelijke vraag van de leden van deze fractie. Aanvullend kan worden opgemerkt dat sommige programma's de mogelijkheid bieden van een zelfstandige verwijdering na een vooraf ingestelde periode. Na, al dan niet zelfstandige, verwijdering van de software zal de politieserver geen gegevens meer kunnen ontvangen. Wanneer zwaarwegende belangen zich verzetten tegen verwijdering, bijvoorbeeld als verwijdering aanzienlijke risico's meebrengt voor het systeem, wordt vanuit de politieserver het dataverkeer stopgezet. Hier zien de opsporingsambtenaren van het technische team op toe. De onderzoekshandelingen in het geautomatiseerde werk worden elektronisch vastgelegd (logging) en tevens vastgelegd in een proces-verbaal, ten behoeve van de controle en de verantwoording.

De leden van de D66-fractie hebben gevraagd of het klopt dat de geïnfecteerde geautomatiseerde werken tevens in verbinding staan met een server van de leverancier van de hacksoftware.
Zoals in de beantwoording van een eerdere, soortgelijke vraag van de leden van deze fractie eerder aan de orde is gekomen, is dit niet het geval.

De leden van de D66-fractie hebben gevraagd op wat voor manier de politie ervoor gaat zorgen dat de server van de politie die in verbinding staat met geïnfecteerde geautomatiseerde werken niet gehackt wordt. De leden van deze fractie hebben tevens gevraagd of de regering kan uitsluiten dat het bij verlies van controle over de server IP-«hijacking»-technieken moeten worden toegepast om de controle terug te krijgen. Ieder systeem dat verbonden is met het internet kan in potentie gehackt worden. De politie zal haar eigen geautomatiseerde omgeving zo veilig mogelijk inrichten en de gebruikte systemen voortdurend beschermen en bewaken tegen mogelijke aanvallen van buiten. Een honderd procent garantie dat dit te allen tijde kan worden voorkomen is in de digitale wereld niet te geven. Het systeem dat in gebruik is voor het binnendringen van het geautomatiseerde werk van de verdachte is verbonden met andere politiesystemen, ten behoeve van logging, monitoring en de correcte opslag van de verzamelde gegevens. De gegevens kunnen echter uitsluitend vanuit het systeem naar de andere politiesystemen worden verzonden, en niet vanuit die systemen worden geraadpleegd.

De leden van de D66-fractie hebben gevraagd waarom niet gekozen is voor een harde termijn voor het opmaken van een proces-verbaal.
Voor de termijn voor het opmaken van een proces-verbaal is aangesloten is bij de algemene verplichting in artikel 152 Sv op grond waarvan opsporingsambtenaren zo spoedig mogelijk proces-verbaal dienen op te maken van hun opsporingshandelingen. In de praktijk wordt gestreefd naar een zo spoedig mogelijke afronding van het proces-verbaal.

De leden van de D66-fractie vragen hoe de voorgestelde bevoegdheid, die zij zeer ingrijpend achten, voldoende controleerbaar is voor de verdediging en de rechtspraak als de inhoud van de processen-verbaal, zoals regelmatig in de praktijk blijkt, niet op orde is. Deze leden vragen welke garantie de regering biedt dat dit met extra zorgvuldigheid zal gebeuren.
De kwaliteit van de processen-verbaal heeft de aandacht van de organisaties in de strafrechtsketen. De politie en het openbaar ministerie werken in een gezamenlijk programma aan de verbetering van het proces van opsporing en vervolging. Hierbij gaat het in eerste instantie om de kwaliteit van de processen-verbaal. Bij brief van 21 december 2015 (Kamerstukken II 2015/16, 29 279, nr. 295) is de voortgangsrapportage van

het programma Versterking Prestaties Strafrechtketen aan Uw Kamer gezonden. In de bijlage bij de brief wordt ingegaan op de tot nu toe bereikte resultaten van de kwaliteit van de opsporing en vervolging.
Het binnendringen in een geautomatiseerd werk en het onderzoek in dat werk vormen een specialisme. Hiermee wordt een beperkte groep van deskundige opsporingsambtenaren belast, die beschikken over expertise en kennis op het gebied van informatie- en communicatietechnologie en die werkzaam zijn bij een speciale eenheid binnen de politie. In de opleiding van die ambtenaren zal aandacht worden besteed aan de verbaliseringsplicht. Er zullen zogenaamde standaardprocessen-verbaal worden ontwikkeld om deze opsporingsambtenaren hierbij te ondersteunen.

De leden van de ChristenUnie-fractie hebben gevraagd waarom er voor is gekozen binnendringing van een computer eerder gelijk te schakelen met het aftappen van telefoongegevens dan met huiszoeking. Deze leden hebben tevens gevraagd of overwogen is om, net als bij een huiszoeking, de binnendringing onder lopend toezicht van een (gespecialiseerde) rechter-commissaris en een assisterende griffier te stellen.
Inderdaad is overwogen om het binnendringen van een geautomatiseerd werk onder het rechtstreekse toezicht van een rechter-commissaris te laten plaatsvinden, dat wil zeggen dat de rechter-commissaris aanwezig is bij het uitvoeren van de bevoegdheid zoals dit bij de huiszoeking in beginsel ook het geval is. Voor de toelichting hierop wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de D66-fractie. Het binnendringen in een geautomatiseerd werk vertoont essentiële verschillen met de huiszoeking, waaronder het fysiek betreden van de woning. Bij het binnendringen in een geautomatiseerd werk kan de inbreuk op de privacy aanzienlijk worden beperkt door een nauwkeurige omschrijving van de gezochte categorie gegevens in het bevel van de officier van justitie.

De leden van de ChristenUnie-fractie hebben geconstateerd dat met de binnendringingsbevoegdheid een spanning ontstaat tussen het gerichte belang van effectief opsporingsonderzoek en het publieke belang van het dichten van beveiligingslekken en hebben gevraagd hoe wordt voorkomen dat vanwege dat gerichte belang kwetsbaarheden in systemen niet openbaar worden gemaakt of op andere wijze worden geadresseerd.
Voor een antwoord op uw vraag over de afwegingen die zijn gemaakt met betrekking tot effectieve opsporing en het bevorderen van veilige systemen verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de D66-fractie (vraag 36) en naar de brief over het gebruik van kwetsbaarheden, die samen met deze nota naar aanleiding van het verslag aan Uw Kamer is gezonden.

De leden van de Groen Links-fractie veronderstellen dat het binnendringen in een geautomatiseerd werk in principe op dezelfde wijze plaatsvindt als een computerhack. Dit biedt de kans om ook na sluiting van het strafrechtelijk onderzoek het geautomatiseerde werk binnen te dringen. De leden van deze fractie hebben gevraagd hoe wordt verzekerd dat misbruik van dit soort datalekken (bijvoorbeeld het zonder nieuwe machtiging betreden van het werk) uitgesloten is.
De technische handelingen bij de uitvoering van de bevoegdheid zullen door een speciale eenheid binnen de politie worden uitgevoerd, waar opsporingsambtenaren werkzaam zijn die beschikken over expertise en kennis op het gebied van informatie- en communicatietechnologie. De opsporingsambtenaren van de eenheid zijn belast met een correcte uitvoering van het bevel van de officier van justitie, inclusief het verwijderen van het technische hulpmiddel. De werkzaamheden worden uitgevoerd onder de verantwoordelijkheid van het openbaar ministerie,

dat het gezag heeft over de opsporing van strafbare feiten. Nadat het onderzoek in het geautomatiseerde werk is afgerond, wordt het technische hulpmiddel verwijderd, deze voorwaarde zal in het besluit ter uitvoering van het wetsvoorstel worden gesteld In uitzonderingsgevallen kan worden afgezien van de (volledige) verwijdering van het technische hulpmiddel. Hierbij moet worden gedacht aan zwaarwegende belangen die zich verzetten tegen het verwijderen, zoals de situatie dat het verwijderen aanzienlijke risico's met zich mee brengt voor het systeem waarin het technische hulpmiddel is geïnstalleerd. Wanneer de software aanwezig blijft in het geautomatiseerde werk waarin de bevoegdheid is toegepast, wordt vanuit de server van de politie het dataverkeer stopgezet zodat de politie geen gegevens meer kan ontvangen van het geautomatiseerde werk. Deze voorwaarde zal worden neergelegd in het besluit ter uitvoering van het wetsvoorstel. Van de stopzetting van de verbinding dient proces-verbaal te worden opgemaakt. De opsporingsinstanties hebben zelf overigens weinig belang bij een niet-tijdige verwijdering van de software, omdat de kans bestaat dat de software wordt ontdekt en de verdachte aldus op de hoogte raakt van het opsporingsonderzoek en vervolgens bewijsmateriaal vernietigt. Gelet op deze procedures en voorschriften is het niet waarschijnlijk dat een opsporingsambtenaar na afloop van het onderzoek in het geautomatiseerde werk opnieuw zal binnendringen met gebruikmaking van de eerder gemaakte verbinding.

2.6 De toetsing van de inzet van de voorgestelde bevoegdheid

De leden van de VVD-fractie lazen dat met behulp van de verzamelde gegevens de uitvoering van de bevoegdheid in voorkomende gevallen kan worden gecontroleerd en hebben gevraagd of nader toegelicht kan worden wat hier moet worden verstaan onder «op deze wijze» en «in voorkomend geval».
Nadat op afstand heimelijk is binnengedrongen in het geautomatiseerde werk kunnen bepaalde onderzoekshandelingen worden verricht. Over het verrichten van deze handelingen worden geautomatiseerd gegevens vastgelegd, ook wel logging genoemd, zodat achteraf verantwoording kan worden afgelegd over de handelingen die, al dan niet met behulp van een technisch hulpmiddel, in het geautomatiseerde werk zijn verricht. Met de woorden «op deze wijze» wordt gedoeld op de gegevens die met behulp van de onderzoekshandelingen zijn verkregen. Met de woorden «in voorkomend geval» wordt gedoeld op de gevallen waarin twijfel ontstaat over de wijze waarop de gegevens zijn verkregen of over de betrouwbaarheid van de verkregen gegevens, bijvoorbeeld op grond van een verweer van de verdachte of diens raadsman.

De leden van de VVD-fractie hebben gevraagd in hoeverre de officier van justitie, de parketsecretarissen en de zittende magistratuur verplicht zijn zich bij te scholen en cursussen te volgen op het gebied van computercriminaliteit.
Elke officier van justitie, parketsecretaris en zittende magistratuur heeft de mogelijkheid om zich bij te scholen op het gebied van computercriminaliteit. Deze bijscholing vindt intern binnen de organisaties plaats. Het openbaar ministerie zorgt binnen het reguliere opleidingsaanbod, zoals via het reguliere opleidingsaanbod Strafrecht van SSR, voor passende kennis en vaardigheden.

De leden van de PvdA-fractie hebben gelezen dat er een notificatieplicht is voorzien op grond waarvan de betrokkene op de hoogte wordt gesteld dat er een opsporingsambtenaar op afstand in zijn pc of smartphone heeft gekeken en hebben gevraagd of de regering de mening deelt dat het nakomen van de notificatieplicht van belang is om de controle op de inzet van deze bevoegdheid mede te waarborgen en zo ja, waarom en hoe de

regering ervoor gaat zorgen dat die notificatieplicht ook daadwerkelijk nageleefd gaat worden.
De wetgever heeft bij de totstandkoming van de Wet bijzondere opsporingsbevoegdheden (BOB) bepaald dat de officier van justitie aan de betrokkene schriftelijk mededeling doet van de uitoefening van een bijzondere opsporingsbevoegdheid, behoudens als uitreiking van de mededeling redelijkerwijs niet mogelijk is (art. 126bb, eerste lid, Sv). Deze notificatieplicht is bedoeld om betrokkenen te informeren over het feit dat er in het kader van een opsporingsonderzoek een inbreuk op hun privacy is gemaakt, zodat zij daartegen een rechtsmiddel kunnen instellen. In 2012 is door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Veiligheid en Justitie onderzoek verricht naar het gebruik van de telefoon- en internettap tijdens het opsporingsproces. Het rapport van dit onderzoek is aan Uw Kamer aangeboden (Kamerstukken II 2011/12, 30 517, nr, 25). De onderzoekers concludeerden dat de onderzochte parketten zich anno 2011 doorgaans houden aan de notificatieplicht. Uit het rapport werd wel duidelijk dat de administratieve afhandeling van het notificeren per parket verschillend is. In het kader van het actieprogramma «Minder regels, meer op straat», heb ik uw Kamer gemeld dat er enkele trajecten zijn ingezet die een verbetering opleveren ten aanzien van de administratieve processen rondom de inzet van bijzondere opsporingsbevoegdheden. Naast het vereenvoudigen van het aanvragen van bevoegdheden gaat het daarbij om de inrichting van de zogenaamde gemeenschappelijke «BOB-kamer». Deze samenwerking tussen politie en openbaar ministerie moet de kwaliteit, de efficiency en de effectiviteit van het administratief proces rondom de inzet van bijzondere opsporingsbevoegdheden verbeteren, waaronder een meer eenduidige naleving van de notificatieplicht. Op basis van de bevindingen van de onderzoekers en de getroffen maatregelen ga ik er dan ook vanuit dat de notificatieplicht voor de voorgestelde bevoegdheid daadwerkelijk zal worden nageleefd.

De leden van de PvdA-fractie hebben gevraagd of er sancties staan op het niet nakomen van de notificatieplicht en zo ja, welke. Ook hebben zij gevraagd of die sancties in het geval van de bestaande opsporingsbevoegdheden ook al worden opgelegd en zo nee, waarom niet.
In het eerdergenoemde artikel 126bb Sv is vastgelegd dat de officier van justitie aan de betrokkene schriftelijk mededeling doet van de toepassing van een bijzondere opsporingsbevoegdheid, zodra het belang van het onderzoek dat toelaat. Notificatie is niet vereist als het proces-verbaal van de toepassing van een bijzondere opsporingsbevoegdheid bij de processtukken wordt gevoegd. Er zijn geen sancties gesteld op het niet-nakomen van de notificatieplicht, deze worden dus ook in het geval van de bestaande opsporingsbevoegdheden niet opgelegd. Dat notificatie niet heeft plaatsgevonden, zal doorgaans alleen door het betrokken parket worden geconstateerd. Het ligt in die gevallen meer in de rede om alsnog tot notificatie over te gaan dan te zoeken naar wegen om herhaling te voorkomen.

De leden van de PvdA-fractie hebben gevraagd of de regering de mening deelt dat het goed zou zijn indien, ook in het geval van het gebruik van de bevoegdheid tot het onderzoek in een geautomatiseerd werk, dat er een onafhankelijke toezichthouder zou komen die het gebruik van die bevoegdheid in zijn algemeenheid gaat toetsen op proportionaliteit, doelmatigheid en rechtmatigheid en zo ja, hoe de regering dit gaat bewerkstellingen.
De regering deelt de mening van de leden van de fractie van de PvdA-fractie, dat toezicht op het gebruik van de voorgestelde bevoegdheid in zijn algemeenheid wenselijk is. Een dergelijk toezicht is reeds in de wet voorzien. De Inspectie Veiligheid en Justitie (VenJ) is als rijksinspectie

belast met het toezicht op de kwaliteit van de taakuitvoering door organisaties werkzaam op het terrein van veiligheid en justitie. Daartoe behoort het toezicht op de taakuitvoering door de politie (art. 57, eerste lid, onderdeel d, Wet veiligheidsregio's). Het toezicht richt zich op de taakuitvoering van de politie, onverminderd het gezag van de burgemeester en de officier van justitie, en de kwaliteitszorg door de politie (art. 65, eerste lid, onderdelen a, en b., Politiewet 2012). Dit betreft de naleving van de wet- en regelgeving rond de toepassing van die bevoegdheden en de kwaliteit van de uitvoering. Waar nodig signaleert de Inspectie VenJ risico's. Een voorbeeld betreft het onderzoek naar de bevraging van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) door de daartoe bevoegde opsporingsambtenaren.
De Inspectie VenJ is een rijksinspectie. Een rijksinspectie heeft de ruimte om zelf, op basis van een werkprogramma en zijn professionele deskundigheid, informatie te verzamelen, daarover een oordeel te vormen, en daarover te rapporteren en te adviseren. Er zijn rijksbrede regels geformuleerd over de positionering van de rijksinspecties binnen de ministeries, waarmee invulling wordt gegeven aan de onafhankelijkheid in de oordeelsvorming van de rijksinspecties (Regeling van de Minister-President, Minister van Algemene Zaken van 30 september 2015, nr. 3151041, houdende de vaststelling van de Aanwijzingen inzake de rijksinspecties, Stcrt. 2015, nr. 33574). De inspecteurs beschikken over de nodige wettelijke toezichtbevoegdheden, op grond van de Algemene wet bestuursrecht (art. 5:12 tot en met 5:20 Awb). Eenieder is verplicht alle medewerking te verlenen aan de inspecteur bij de uitoefening van zijn bevoegdheden.
Op basis van de in de wet vastgelegde positie en taken 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. 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.
Het toezicht door de Inspectie VenJ zal betrekking hebben op de naleving van de wettelijke regels en voorschriften rond de toepassing van het onderzoek in een geautomatiseerd werk die zijn neergelegd in het Wetboek van Strafvordering en in het Besluit technische hulpmiddelen Strafvordering. Meer concreet heeft het toezicht 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.
Het toezicht van de Inspectie VenJ is aldus gericht op het functioneren van het wettelijke systeem rond het onderzoek in een geautomatiseerd werk (systeemtoezicht). Het kader voor het toezicht wordt gevormd door de grenzen van het bevel en de machtiging voor het onderzoek in een geautomatiseerd werk. De oordeelsvorming door de officier of de rechter-commissaris, zoals deze tot uitdrukking komt in het bevel respectievelijk de machtiging, valt buiten dit kader. Het oordeel over de beslissingen of het handelen van de officier van justitie is voorbehouden aan de procureur-generaal bij de Hoge Raad en de rechter ter terechtzitting.

Het is niet bij voorbaat uitgesloten dat de inspecteurs bij de uitoefening van het toezicht in aanraking komen met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie. In een dergelijk geval kan het hoofd van de Inspectie VenJ de procureur-generaal bij de Hoge Raad informeren. De procureur-generaal bij de Hoge Raad waakt in het bijzonder voor de handhaving en uitvoering van wettelijke voorschriften bij de Hoge Raad, de gerechtshoven en de rechtbanken (art. 121 Wet RO). Indien naar het oordeel van de procureur-generaal bij de Hoge Raad het openbaar ministerie bij de uitoefening van zijn taak de wettelijke voorschriften niet naar behoren handhaaft of uitvoert, kan hij Onze Minister daarvan in kennis stellen (art. 122, eerste lid, Wet RO). Het is evenmin uitgesloten dat de inspecteurs in aanraking komen met mogelijke schendingen van de regels rond de bescherming van persoonsgegevens. In een dergelijk geval kan de Inspecteur VenJ de AP informeren. De AP is belast met het toezicht op de naleving van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens, en beschikt over de nodige wettelijke bevoegdheden ter handhaving.
Tenslotte zijn er door de Inspectie afspraken gemaakt met de Onderzoeksraad voor de Veiligheid en de Rijksinspecties over de afstemming (Afstemmingsprotocol Onderzoeksraad en Veiligheid en Rijksinspecties, ondertekend op 12 december 2010).
De Inspectie VenJ werkt op basis van een werkprogramma dat jaarlijks door het hoofd van de Inspectie VenJ wordt vastgesteld en door de Minister van Veiligheid en Justitie aan de Staten-Generaal wordt aangeboden. Een overzicht van lopende onderzoeken is te vinden op de website van de Inspectie. Na afloop van een onderzoek wordt een rapport opgesteld. Het vastgestelde inspectierapport wordt door het hoofd van de Inspectie aan de Minister van Veiligheid en Justitie aangeboden en door die Minister openbaar gemaakt.
Het hoofd van de Inspectie VenJ stelt jaarlijks een rapport op waarin verslag zal worden gedaan van het toezicht op de uitvoering van de bevoegdheid tot het onderzoek in een geautomatiseerd werk.
De opsporingsambtenaren van de Koninklijke marechaussee die zijn belast met de uitvoering van de politietaak als bedoeld in de artikelen 3 en 4 van de Politiewet 2012, vallen eveneens onder de reikwijdte van de Politiewet 2012 en daarmee onder het toezicht van de Inspectie VenJ. De opsporingsambtenaren die werkzaam zijn bij een bijzondere opsporingsdienst, bedoeld in artikel 1, onderdeel a, van de Wet op de bijzondere opsporingsdiensten, vallen echter niet onder de reikwijdte van de Politiewet 2012. Ditzelfde geldt voor de personen die als buitengewoon opsporingsambtenaar worden ingezet vanwege hun specifieke expertise op het gebied van de informatie- en communicatietechnologie, benodigd voor het onderzoek in een geautomatiseerd werk. Dit betreft de opsporingsambtenaren, bedoeld in artikel 142, eerste lid, onderdeel b, van het Wetboek van Strafvordering. Daarmee valt de taakuitvoering van deze opsporingsambtenaren buiten het toezicht van de Inspectie VenJ. Om hieraan tegemoet te komen is aanpassing van de bepalingen over het onderzoek in een geautomatiseerd werk (artikelen 126nba/uba/zpa) noodzakelijk. De voorgestelde wijziging is opgenomen in een nota van wijziging.

De leden van de SP-fractie hebben gevraagd of het klopt dat alle onderzoekshandelingen met betrekking tot het heimelijk binnendringen in een geautomatiseerd werk worden vastgelegd en ten behoeve waarvan dit wordt vastgelegd. Daarbij hebben zij gevraagd of dit onder andere ook is om toezicht te houden op het correct uitvoeren van het bevel. Zij hebben tevens gevraagd wie toezicht houdt op de correcte uitvoering van een bevel en of het klopt dat dat niet wordt gedaan door de rechter-commissaris en zo nee, waarom niet.

Inderdaad worden geautomatiseerd gegevens vastgelegd (logging) rond het verrichten van de onderzoekshandelingen, zodat achteraf kan worden nagegaan welke handelingen in het geautomatiseerde werk zijn verricht. Dit is van belang voor het verantwoorden van de verrichtingen als hierover in de later stadium vragen zouden rijzen. Dit kan aan de orde komen naar aanleiding van een verweer van de verdachte of zijn raadsman tijdens de strafzaak, of in het kader van het toezicht op de rechtmatige uitvoering van de bevoegdheid, door de Inspectie VenJ. De rechter-commissaris geeft een machtiging voor de uitvoering van een bevel van de officier van justitie tot het binnendringen van een geautomatiseerd werk en tot het verrichten van bepaalde onderzoekshandelingen. De rechter-commissaris houdt in beginsel geen toezicht op de correcte uitvoering van die handelingen. Dit neemt niet weg dat de rechter-commissaris in een concreet geval kan bepalen dat het binnendringen van een geautomatiseerd werk en/of het verrichten van bepaalde onderzoekshandelingen in zijn aanwezigheid worden verricht. Hiervoor kan ook worden verwezen naar de beantwoording van een eerdere vraag van de leden van de D66-fractie. Dit is echter ter beoordeling van de rechter-commissaris zelf.

De leden van de SP-fractie ontvingen graag een uiteenzetting van de wijze waarop onafhankelijke controle plaatsvindt (en eventuele handhaving) van correcte uitvoering van een afgegeven bevel en rechterlijke machtiging zodat toetsing niet alleen vooraf en achteraf plaatsvindt maar ook tijdens de inzet.
Een bevel van de officier van justitie tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt zorgvuldig voorbereid, waarbij een afweging wordt gemaakt tussen de te bereiken doelen, de beschikbare technieken en middelen, de mogelijk alternatieve middelen en de risico's die aan de inzet zijn verbonden. Als de officier van justitie besluit tot de inzet van deze bevoegdheid dan wordt de voorgenomen inzet een de Centrale Toetsingscommissie voorgelegd. Het bevel van de officier van justitie is tevens onderworpen aan rechterlijke toetsing, vanwege het vereiste van de voorafgaande machtiging van de rechter-commissaris. De officier van justitie houdt toezicht op de uitvoering van het bevel en van onderzoekshandelingen die worden verricht worden geautomatiseerd gegevens vastgelegd (logging). Verder geldt de verbaliseringsplicht, die inhoudt dat de opsporingsambtenaar ten spoedigste proces-verbaal opmaakt van de door hem verrichte handelingen (art. 152 Sv), zodat daarover verantwoording kan worden afgelegd. Het toezicht op een rechtmatige toepassing is in handen van de rechter ter terechtzitting. Aanvullend zal de Inspectie VenJ toezicht uitoefenen op de uitvoering van de bevoegdheid. Hiervoor wordt verwezen naar de beantwoording van de vragen van de leden van de PvdA-fractie.

De leden van de SP-fractie wilden weten of bij het voorleggen van een bevel aan de rechter-commissaris ook meegenomen wordt hoe doelgericht wordt gezocht en tot hoeveel gegevens toegang zal worden verkregen en of een machtiging of bevel minder snel zal worden afgegeven naarmate het aantal gegevens dat (ongericht) wordt verzameld toeneemt. Daarbij hebben zij gevraagd hoe zwaar dit weegt bij de belangenafweging.
Voor het afgeven van een machtiging tot het op afstand heimelijk binnendringen van een geautomatiseerd werk vormt de proportionaliteit en subsidiariteit van de voorgestelde inzet van de bevoegdheid onderdeel van de toetsing door de rechter-commissaris. Ook de aard en ernst van de verdenking, hoe specifiek de verdenking is, of er een duidelijk beeld is welke gegevens worden gezocht en hoe waarschijnlijk het is dat die gegevens zich daadwerkelijk in het geautomatiseerde werk bevinden, vormen onderdeel van die toetsing. Het aantal gegevens dat wordt

verzameld betreft geen op zichzelf staand criterium maar kan wel worden betrokken in de proportionaliteitstoetsing. Er valt geen algemene indicatie te geven van het gewicht dat de rechter-commissaris zal toekennen aan het aantal gegevens dat wordt verzameld. Dat zal sterk afhangen van de concrete feiten en omstandigheden van het geval. Overigens is hier geen sprake van een «ongerichte» verzameling van gegevens. In het bevel dienen onder meer het geautomatiseerde werk en de categorie gegevens waar de inzet op is gericht nauwkeurig te worden omschreven.

De leden van de SP-fractie hebben gevraagd of de aangepaste opleidingen niet alleen ingaan op de nieuwe bevoegdheden maar ook op de begrippen proportionaliteit en subsidiariteit.
Begrippen als proportionaliteit en subsidiariteit zijn cruciaal voor het maken van de afweging betreffende een bevel tot het binnendringen in een geautomatiseerd werk en voor het bepalen van de reikwijdte van de inzet in een concreet geval. Deze begrippen worden daarom opgenomen in de desbetreffende opleidingen en cursussen.

De leden van de SP-fractie hebben gevraagd hoe de samenwerking verloopt met en de inzet van ethische hackers.
Nederland was in 2013 het eerste land ter wereld waar sprake was van beleid om de samenwerking met de gemeenschap van ethische hackers te stimuleren via de «leidraad om te komen tot een praktijk van «responsible disclosure». Op 18 december 2014 is uw Kamer geïnformeerd (Kamerstukken II 2014/15, 26 643, 342) over de positieve ervaringen op dit gebied en de wijze waarop ethische hackers middels meldingen aan de overheid over kwetsbaarheden bijdragen aan het verhogen van de digitale veiligheid. Jaarlijks wordt in het Cyber Security Beeld Nederland stilgestaan bij responsible disclosure. Dit beleid is de afgelopen jaren actief uitgedragen op de Global Conference on Cyberspace in 2015 en tijdens het Nederlandse EU voorzitterschap in 2016. Tot slot worden ook regelmatig hackevenementen en andere bijeenkomsten georganiseerd om de kennis van de gemeenschap van ethische hackers actief te ontsluiten.

De leden van de SP-fractie hebben gevraagd of zij het goed begrijpen als zij stellen dat er een notificatieplicht komt aan de betrokkene als het belang van het onderzoek dat toelaat en wanneer daarvan sprake is. Zij hebben tevens gevraagd of dan ook de reden wordt aangegeven van het onderzoek in het geautomatiseerde werk, zodat betrokkene weet waar hij eventueel verweer tegen moet voeren. Ook hebben zij gevraagd hoe om te gaan met de notificatieplicht als het gaat om gegevens op een buitenlands of onbekend geautomatiseerd werk.
Zoals eerder, naar aanleiding van een vraag van de PvdA-fractie is aangegeven, is in artikel 126bb Sv een notificatieplicht vastgelegd voor de toepassing van een bijzondere opsporingsbevoegdheid. Notificatie is vereist zodra het belang van het onderzoek dat toelaat. Degene die aan de toepassing van een bijzondere opsporingsbevoegdheid wordt onderworpen heeft op grond van artikel 13 EVRM het recht om zich hierover te beklagen, indien hij op de hoogte is van de toepassing van de heimelijke bevoegdheid (Kamerstukken II 1996/97, 25 403. nr. 3, blz. 12). Daarbij wordt de reden van het onderzoek in het geautomatiseerde werk niet gegeven, dit is op grond van de wettelijke regeling niet vereist omdat het gaat om notificatie van de inzet van een bevoegdheid. De notificatieplicht geldt onverkort als het gaat om gegevens op een buitenlands geautomatiseerd werk. In dat geval is het echter mogelijk dat de mededeling achterwege blijft omdat de betrokkenen niet getraceerd kunnen worden, zodat uitreiking daarvan redelijkerwijs niet mogelijk is (art. 126bb, eerste lid, Sv).

De leden van de SP-fractie hebben gevraagd hoe, in de gevallen waarin de betrokkene niet op de hoogte wordt gebracht, dan rekening wordt gehouden met artikel 13 EVRM, waarin staat dat mensen eventueel schending van hun grondrechten aan moeten kunnen vechten.
Artikel 13 EVRM garandeert een ieder die beweert dat zijn rechten en vrijheden neergelegd in het EVRM zijn geschonden, het recht op een «effective remedy before a national authority». Deze verdragsbepaling biedt aan degene jegens wie een heimelijke opsporingsbevoegdheid is toegepast, indien hij op de hoogte is van de toepassing van die bevoegdheid, het recht om zich hierover te beklagen. In de zaak Klass heeft het EHRM beslist dat in geval van een telefoontap «*an effective remedy under article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance*» (Klass and Others judgment of 8 September 1978, Series A, nr. 28, AA 1979, 327). Daarom is in artikel 126bb Sv bepaald dat het informeren van de persoon ten aanzien van wie een in dat artikel genoemde bijzondere opsporingsbevoegdheid is uitgeoefend achterwege mag blijven zolang zulks het doel waartoe werd afgeluisterd, in casu het strafrechtelijk onderzoek, kan schaden.

De leden van de CDA-fractie hebben gevraagd naar de snelheid waarmee de toetsing middels de Centrale Toetsingscommissie en het College van procureurs-generaal plaatsvindt, gelet op de spoedeisendheid die kan zijn geboden bij het inzetten van bepaalde bevoegdheden. Deze leden hebben tevens gevraagd of in dit geval ook uitzonderingen mogelijk en wenselijk zijn, bijvoorbeeld toetsing achteraf.
De verantwoordelijke hoofdofficier van justitie die een zaak ter goedkeuring voorlegt aan het College van procureurs-generaal, zendt daartoe de stukken aan de CTC. Iedere week vindt er een vergadering van de CTC plaats. Naar aanleiding van de bespreking ter vergadering wordt een advies opgesteld, dat door tussenkomst van de PG-portefeuillehouder aan het College van procureurs-generaal wordt voorgelegd. Er is tevens voorzien in een spoedprocedure. De CTC toetst de zaak dan zo spoedig mogelijk en legt haar (mondeling) advies voor aan (een lid) van het College. Hierop kan het College een (mondelinge)beslissing nemen. Op grond hiervan kan worden vastgesteld dat de huidige regeling voorziet in voldoende mogelijkheden om te komen tot een snelle afronding van het advies- en besluitvormingstraject binnen het openbaar ministerie.

De leden van de CDA-fractie hebben gevraagd naar de logica van een notificatieplicht, nu de kern van heimelijk binnendringen in beginsel is dat de betrokkene niet op de hoogte wordt gesteld. Zij hebben gevraagd of niet een andere wettelijke constructie wenselijk is, namelijk dat pas achteraf mededeling wordt gedaan van de inbreuk en eventueel een wettelijke uitzondering hierop dat vooraf mededeling wordt gedaan. Voor deze leden rijst dan nog wel de vraag in welke gevallen de regering het wel denkbaar acht dat vooraf de betrokkene op de hoogte wordt gesteld. Zij hebben verzocht deze vragen eveneens te beantwoorden in geval vermoedens zijn dat meerdere personen gebruik maken van het betreffende apparaat.
De mededeling wordt, anders dan de leden van de CDA-fractie kennelijk veronderstellen, altijd achteraf gedaan. De regering acht het niet wenselijk dat de mededeling vooraf wordt gedaan, omdat de betrokkene dan op de hoogte komt dat de politie en justitie in hem zijn geïnteresseerd. Dit is in strijd met de aard van de bevoegdheid, die juist heimelijk wordt toegepast. De mededeling wordt gedaan aan de betrokkenen, dit zijn de personen jegens wie één van de bevoegdheden is uitgeoefend, de houder van de telefoonaansluiting of de rechthebbende van de besloten plaats die is betreden (art. 126bb, tweede lid, Sv). Als meerdere personen gebruik maken van het geautomatiseerde werk dan zullen deze wel zo

nauw met de verdachte verbonden zijn dat zij informeel met de bevoegdheidsuitoefening op de hoogte raken, dat hoeft echter niet. Voor zover gegevens zouden zijn vastgelegd die op hen betrekking hebben dan hebben zij als betrokkene te gelden in de zin van de notificatieplicht.

De leden van de D66-fractie hebben opgemerkt dat wordt voorzien in een Centrale Toetsingscommissie en hebben gevraagd waarom niet is voorzien in systeemtoezicht meer op afstand, zoals door de Autoriteit Persoonsgegevens wordt bepleit.
Er is reeds voorzien in systeemtoezicht meer op afstand, zoals door de AP bepleit. Dit betreft het toezicht door de Inspectie Veiligheid en Justitie, op grond van de Politiewet 2012. Dit is hierboven reeds aan de orde gekomen, naar aanleiding van een vraag van de PvdA-fractie. Voor de nadere toelichting op het toezicht door de Inspectie Veiligheid en Justitie verwijs ik naar de beantwoording van de vraag van die fractie.

Het is de leden van de D66-fractie opgevallen dat hoe hoger in de controleketen hoe minder de inzet op specialistische kennis lijkt te zijn, terwijl de inzet en kennis van weke de controlerende taak dan juist maximaal dient te zijn. De leden van deze fractie hebben gevraagd wat de regering vindt van het voorstel om ten minste te voorzien in specialistische rechter-commissarissen gelijk aan de cybercrime officier van justitie bij ieder regioparket. Deze leden hebben tevens gevraagd wat de regering vindt van het voorstel om een speciale cyberkamer bij de rechtspraak in te richten die zich met dit soort zaken zal bezig houden en waarin kennis en ervaring met cyberzaken is gebundeld.
De rechtspraak zal zorgen voor een adequate implementatie van deze nieuwe wetgeving, inclusief de organisatorische en deskundigheidsvoorzieningen die daarvoor nodig zijn. Als in het kader daarvan enige vorm van specialisatie binnen de gerechten nodig, wenselijk en uitvoerbaar wordt geacht, zal ook dat aspect bij de implementatie worden betrokken. Eerder is reeds melding gemaakt van het landelijk opererend Kenniscentrum Cybercrime, dat is ondergebracht bij het Gerechtshof te Den Haag. Een vergelijking met een landelijke gespecialiseerde en geconcentreerde kamer als de Ondernemingskamer lijkt niet voor de hand te liggen. Dit in verband met het ontbreken van een scherpe scheiding tussen cybercrime en commune criminaliteit.

De leden van de ChristenUnie-fractie hebben gevraagd naar de positie van private en publieke onderzoekers die op het «darkweb» meekijken en daar strafbare feiten tegenkomen. Deze leden vragen voorts of de regering heeft overwogen om voor deze groep nadere voorzieningen te treffen, of de regering een beeld heeft van de juridische risico's van dergelijk onderzoek en of overwogen is hiernaar onderzoek te doen.
Een ieder is bevoegd om aangifte te doen van een strafbaar feit dat hem of haar ter kennis komt (art. 161 Sv). Op grond van artikel 160 Sv geldt een aangifteplicht voor de misdrijven die in dat artikel genoemd worden, waaronder moord en doodslag, hulp bij zelfdoding, verkrachting, schending van staatsgeheimen en bepaalde misdrijven in tijden van oorlog. Er bestaat geen aangifteplicht voor degene die door de aangifte het risico loopt zelf te worden vervolgd. Nadere voorzieningen voor onderzoekers die onderzoek doen op het «darkweb» worden niet overwogen.

De leden van de ChristenUnie hebben gevraagd wat de regering vindt van het door verschillende organisaties en experts gedane voorstel als extra waarborg via een onafhankelijke commissie van toezicht binnendringing binnen opsporingsonderzoeken te laten monitoren.
Met de leden van de fractie van de ChristenUnie is de regering doordrongen van het belang van toezicht op de uitoefening van de

bevoegdheid van het binnendringen van een geautomatiseerd werk. In dit toezicht is reeds voorzien. Dit betreft het toezicht door de Inspectie Veiligheid en Justitie, op grond van de Politiewet 2012. Dit is hierboven reeds aan de orde gekomen, naar aanleiding van een soortgelijke vraag van de leden van de PvdA-fractie.

De leden van de ChristenUnie-fractie hebben gevraagd of de regering bereid is het Besluit technische hulpmiddelen strafvordering te herzien voordat de Kamer zich over het wetsvoorstel uitspreekt.
Het wetsvoorstel bevat geen voorhangbepaling. Het is regeringsbeleid om in beginsel geen formele betrokkenheid van het parlement bij gedelegeerde regelgeving te regelen.

De leden van de PvdD-fractie zijn van mening dat er een onafhankelijke commissie voor toezicht op de opsporingsdiensten moet komen en hebben gevraagd of de regering bereid is hierover met een voorstel te komen alvorens de Kamer over het wetsvoorstel zal stemmen.
Met de leden van de PvdD-fractie is de regering van oordeel dat toezicht op de opsporingsdiensten wenselijk is. In dit toezicht is reeds voorzien. Dit betreft het toezicht door de Inspectie Veiligheid en Justitie, op grond van de Politiewet 2012. Dit is hierboven reeds aan de orde gekomen, naar aanleiding van een soortgelijke vraag van de leden van de PvdA-fractie. In het licht van de bestaande situatie acht de regering een voorstel om te komen tot een onafhankelijke commissie voor toezicht op de opsporingsdiensten niet nodig.

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

De leden van de SP-fractie waren benieuwd op grond waarvan het Duitse Bundesverfassungsgericht heeft geoordeeld dat een heimelijke infiltratie van een computersysteem alleen is toegestaan als er aanwijzingen zijn van een concreet gevaar voor een belangrijk rechtsgoed, zoals gevaar voor leven of de vrijheid van een persoon of het staatsbelang en hebben gevraagd in hoeverre onderhavig wetsvoorstel aan deze eisen voldoet. Tevens hebben zij gevraagd of het klopt dat onderhavig wetsvoorstel sneller leidt tot inzet van de hackbevoegdheid.
In de uitspraak van 27 februari 2008 heeft het Duitse Bundesverfassungsgericht (BVerfG) zich uitgesproken over een wet van de deelstaat Noordrijn-Westfalen, die de inlichtingendienst («Verfassungsschutzbehörde») van die deelstaat de bevoegdheid gaf tot het op afstand heimelijk doorzoeken van geautomatiseerde werken. Deze bevoegdheid was dus, anders dan in de memorie van toelichting gemeld, niet aan de opsporingsautoriteiten toegekend. Het BVerfG achtte deze wet in strijd met de artikelen 10 en 13 van de Duitse Grondwet, die het recht op privacy beschermen. Het Hof oordeelde dat de bewuste bepaling ongeldig was omdat deze niet voldeed aan de eisen die daaraan, op grond van eerdergenoemde artikelen 10 en 13 van de Duitse Grondwet, moesten worden gesteld. Dit betrof het beginsel van de duidelijkheid van de wetgeving («Normenklarheit»), de vereisten van de proportionaliteit en de waarborgen voor een zorgvuldige toepassing ter bescherming van het recht op bescherming van de persoonlijke levenssfeer. Deze toets vertoont overeenkomsten met die van het EHRM, op basis van artikel 8 EVRM. Daarbij hecht het BVerfG aan het beginsel van de passendheid (»Gebot der Angemessenheit»), waaruit voortvloeit dat de wetgeving die inbreuk maakt op fundamentele rechten een balans moet houden tussen de aard en intensiteit van de inbreuk op die rechten en de feitelijke omstandigheden die een dergelijke inbreuk kunnen rechtvaardigen. De vereisten voor de mate van waarschijnlijkheid en de feitelijke basis van de verwachting moeten proportioneel zijn ten opzichte van de aard en intensiteit van de inbreuk op fundamentele rechten (punt 245). Het Hof

heeft vervolgens overwogen dat een dergelijke inbreuk uitsluitend toegestaan is bij feitelijke indicaties van een concreet gevaar voor een belangrijk rechtsgoed («überragend wichtiges Rechtsgut»). Dit betreft allereerst het lichaam, leven en de vrijheid van de persoon. Ook kan dit betreffen een bedreiging van de grondvesten of het voortbestaan van de staat of van de mensheid. De levering van publieke voorzieningen kan hieronder ook worden begrepen (punt 247).
Het criterium dat door het BVerfG is geformuleerd is in de Nederlandse wetgeving niet bekend en is geformuleerd naar aanleiding van de wetgeving in Noordrijn-Westfalen, die voorzag in een heimelijk binnendringen in een geautomatiseerd werk teneinde gegevens te doorzoeken. Niettemin is ook in het conceptwetsvoorstel gekozen voor strikte voorwaarden voor de toepassing van de bevoegdheid, namelijk dat het moet gaan om een ernstig strafbaar feit, waarvoor voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op de rechtsorde oplevert. Voor bepaalde onderzoekshandelingen geldt daarenboven het vereiste van een zeer ernstig misdrijf, waarvoor een gevangenisstraf van ten minste acht jaar of meer is gesteld, kan worden opgelegd. Dit criterium is ingevoegd naar aanleiding van het advies van de Afdeling advisering van de Raad van State. Overigens zal het onderscheid in de praktijk niet heel groot zijn, omdat ernstige vormen van criminaliteit, zoals de handel in verdovende middelen, mensen of kinderpornografie, terroristische activiteiten, een bedreiging vormen voor het lichaam, het leven of de vrijheid van personen. Echter, ook in de gevallen waarin geen direct risico bestaat voor het leven of de vrijheid van personen kan aanleiding bestaan tot de toepassing van de voorgestelde bevoegdheid. Dit betreft allereerst situaties waarin de infrastructuur, bijvoorbeeld de financiële dienstverlening, ernstig wordt belemmerd door vormen van cybercrime als DDOS-aanvallen of het gebruik van botnets. Dit betreft tevens situaties waarin het op afstand binnendringen van een geautomatiseerd werk noodzakelijk is voor het toepassen van de bestaande bevoegdheden op het gebied van het aftappen en direct afluisteren. De inbreuk op de persoonlijke levenssfeer van de betrokkene is dan minder groot, omdat het binnendringen voorwaardelijk is voor het plaatsen van het technische hulpmiddel voor het aftappen of direct afluisteren en er geen sprake is van het doorzoeken van het geautomatiseerde werk met het oog op het overnemen van gegevens. Vanwege deze laatste mogelijkheid moet er inderdaad rekening mee worden gehouden dat onderhavig wetsvoorstel sneller leidt tot de inzet van de bevoegdheid, maar de regering ziet dat niet bij voorbaat als een fundamenteel bezwaar en meent dat de ontwikkeling van de computercriminaliteit zodanig is dat deze de toepassing van de voorgestelde bevoegdheid kan rechtvaardigen, zeker in het licht van de strikte waarborgen die kunnen verzekeren dat de bevoegdheid uitsluitend wordt toegepast in ernstige gevallen, waarbij geen andere mogelijkheden beschikbaar zijn om de gegevens te verkrijgen of het strafbare feit te beëindigen, en adequate waarborgen gelden ter bescherming van de persoonlijke levenssfeer van de betrokkene.

De leden van de SP-fractie hebben gevraagd in hoeverre dit wetsvoorstel stand houdt voor de Nederlandse rechter en het Europese Hof voor de Rechten van de Mens. Tevens hebben zij gevraagd waarom niet is aangesloten bij het oordeel van het Duitse Bundesverfassungsgericht.
Het recht op eerbiediging van de persoonlijke levenssfeer wordt erkend in het EVRM (art. 8 EVRM). Individuen, groepen, organisaties en landen kunnen door een beroep te doen op het Europees Verdrag tot Bescherming van de Rechten van de Mens (EVRM) een klacht indienen tegen een lidstaat van de Raad van Europa. Hieronder wordt, naar aanleiding van een soortgelijke vraag van de leden van deze fractie, nader ingegaan op de vraag in hoeverre dit wetsvoorstel stand houdt voor het Europese Hof voor de Rechten van de Mens. Voor de vraag waarom niet is aangesloten

bij het oordeel van het Duitse Bundesverfassungsgericht wordt verwezen naar de beantwoording van de eerdere vraag van de leden van de SP-fractie.

De leden van de SP-fractie hebben gevraagd of de regering kan reageren op de uitspraak van de Autoriteit Persoonsgegevens tijdens het rondetafelgesprek over computercriminaliteit dat zij ernstig twijfelt of onderhavige wet stand zal houden.
De regering deelt het oordeel van de Autoriteit Persoonsgegevens niet. In het EVRM wordt het recht op eerbiediging van de persoonlijke levenssfeer beschermd (artikel 8 EVRM). Geen inmenging van enig openbaar gezag in de uitoefening van dit recht is toegestaan dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van, onder meer, de nationale veiligheid, de openbare veiligheid of het belang van het voorkomen van wanordelijkheden en strafbare feiten (artikel 8, tweede lid, EVRM). Onder het criterium «het voorkomen van strafbare feiten» is, zo blijkt uit de rechtspraak van het EHRM, de strafvorderlijke afwikkeling van strafbare feiten, waaronder de opsporing daarvan, begrepen. De eis van de inmenging «bij wet is voorzien» houdt in dat in het nationale recht is voorzien in een wettelijke regeling die voor de burger voldoende kenbaar en voorzienbaar is. Op basis van de jurisprudentie van het EHRM geldt daarbij dat de betreffende wettelijke regeling voldoende toegankelijk moet zijn en met voldoende precisie geformuleerd, zodanig dat deze een voldoende indicatie bevat van de omstandigheden waarin en de voorwaarden waaronder de overheid tot deze inmenging mag overgaan, en de rechtssubjecten een adequate bescherming tegen willekeurige inmenging biedt. Uit de jurisprudentie van het EHRM vloeit verder voort dat de inmenging door enig openbaar gezag in de privacyrechten moet voldoen aan vereisten inzake noodzakelijkheid en evenredigheid, en derhalve specifieke, expliciete en legitieme doeleinden moet dienen, en moet plaatsvinden op adequate en relevante wijze, en niet buitensporig mag zijn in verhouding van tot het doel van de inmenging. Het «noodzaakcriterium» wordt in de rechtspraak van het EHRM nader ingevuld aan de hand van de beginselen van proportionaliteit, subsidiariteit en van een «pressing social need» (er moet een dringende maatschappelijke behoefte bestaan om het legitieme doel te vervullen).
De voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen van een geautomatiseerd werk wordt bij wet vastgelegd. Daarbij worden de omstandigheden waarin, en de voorwaarden waaronder deze bevoegdheid kan worden toegepast, nauwkeurig vastgelegd. De opsporing van strafbare feiten is erkend als een belang dat inmenging van het openbaar gezag in het recht op bescherming van de persoonlijke levenssfeer kan rechtvaardigen. In dit geval gaat het om de opsporing van ernstige strafbare feiten, waarvoor voorlopige hechtenis mogelijk is. Met de opneming van de voorgestelde bevoegdheid in het Wetboek van Strafvordering wordt voorzien in een wettelijke regeling die voor de burger voldoende toegankelijk is. De voorgestelde regeling beschrijft nauwkeurig in welke omstandigheden, en onder welke voorwaarden de bevoegdheid kan worden toegepast. Vereist zijn een verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert, en een dringend onderzoeksbelang. De te verrichten onderzoekshandelingen zijn nauwkeurig omschreven, en sluiten merendeels aan bij bestaande bevoegdheden en maatregelen van het Wetboek van Strafvordering. De officier van justitie moet in het bevel de feiten en omstandigheden vastleggen waaruit blijkt dat de wettelijke voorwaarden voor de toepassing zijn vervuld. Met de wettelijke vereisten, in het bijzonder dat van een voorafgaande rechterlijke toetsing, wordt het risico van een willekeurige toepassing van de bevoegdheid door een overheidsorgaan uitgesloten. Aan het «noodzake-

lijkheidscriterium» wordt voldaan doordat de voorgestelde maatregel onvermijdelijk is om het hoofd te kunnen bieden aan de ontwikkeling van de cybercrime gedurende de afgelopen jaren. Dit heeft betrekking op de versleuteling van gegevens en de opslag van gegevens in de cloud, waardoor het in de praktijk vrijwel onmogelijk wordt een aanbieder te vinden bij wie de gegevens kunnen worden opgevraagd. De inzet van traditionele opsporingsbevoegdheden, als het aftappen van communicatie via de aanbieder en het vorderen van gegevens bij derden, is dan zinloos. De voorgestelde bevoegdheid van het op afstand heimelijk binnendringen van een geautomatiseerd werk voorziet in een dringende behoefte om ernstige vormen van criminaliteit te kunnen bestrijden. Aan het beginsel van evenredigheid is invulling gegeven doordat in het bevel moet worden aangegeven welke categorie van gegevens het betreft. Ook moeten gegevens over de onderzoekshandelingen worden vastgelegd (logging) zodat achteraf controle mogelijk is op de uitvoering van de bevoegdheid. Daarbij wordt, zoals hierboven naar aanleiding van een vraag van de PvdA-fractie aan de orde is gekomen, voorzien in systeemtoezicht op de rechtmatigheid van de uitoefening van de bevoegdheid. Verder is van belang dat de voorgestelde bevoegdheid een aanvulling vormt op de bestaande wettelijke bevoegdheden. De voorgestelde bevoegdheid mag alleen worden toegepast als blijkt dat met de bestaande wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt. Dit komt tevens tot uitdrukking in het vereiste van het dringende onderzoeksbelang. Verder is de bevoegdheid beperkt tot de in de wet vastgelegde onderzoekshandelingen, die merendeels aansluiten bij de bestaande bevoegdheden en maatregelen. Met de voorgestelde bevoegdheid wordt juist voorzien in een bevoegdheid om uitsluitend de gegevens, die nodig zijn voor de opsporing van het betreffende ernstige strafbare feit, vast te leggen ten behoeve van de opsporing. De regering ziet dan ook 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.

De leden van de CDA-fractie hebben gevraagd of de regering met politie en justitie de wenselijkheid voor de opsporingspraktijk heeft besproken een bevel als in Duitsland te kunnen opleggen voor maximaal drie maanden met verlengingsmogelijkheden van telkens drie maanden. Zij hebben tevens gevraagd of dit niet veel meer ruimte biedt voor de opsporing en gedurende een langere periode ongestoord onderzoek te kunnen doen dan de nu voorgestelde termijn van vier weken. Zij hebben gevraagd of de Duitse regering hiermee toch ook voldoet aan de gewenste Europese proportionaliteitseis. Deze leden zouden graag een aanpassing op dit punt zien in onderhavig wetsvoorstel.
De regering heeft voor de juridische voorwaarden voor de toepassing van de bevoegdheid aangesloten bij de systematiek rond de toepassing van bijzondere opsporingsbevoegdheden in het Wetboek van Strafvordering. Voor de toepassing van bevoegdheden die een vergelijkbaar ernstige inbreuk op de persoonlijke levenssfeer van de betrokkene vormen, zoals het aftappen van telecommunicatie of het direct afluisteren, geldt dat de duur van het bevel ten hoogste vier weken bedraagt, met de mogelijkheid van verlenging. De regering acht een termijn van vier weken aangewezen, omdat een dergelijke termijn een adequate periodieke toetsing van de rechtmatigheid van de toepassing door de rechter-commissaris verzekert. In hun adviezen hebben de politie en het openbaar ministerie hierover geen opmerkingen ingebracht.

De leden van de D66-fractie hebben gevraagd of het klopt dat Nederland met dit wetsvoorstel de meest vergaande hackwetgeving zou krijgen binnen de EU. Zij hebben de regering tevens gevraagd een overzicht in te sturen met bevoegdheden rondom het hacken van geautomatiseerde

werken in alle EU lidstaten. Zij hebben tevens gevraagd hoe het wetsvoorstel zich verhoudt tot de keuze van Frankrijk en Duitsland om juist af te zien van het gebruik van spyware omdat oneigenlijk gebruik door derden en de politie niet viel uit te sluiten.
De regering beschikt niet over inzicht in de bevoegdheden rondom het hacken van geautomatiseerde werken in alle EU-lidstaten. Op basis van de beschikbare kennis kan echter niet worden bevestigd dat Nederland met dit wetsvoorstel de meest vergaande hackwetgeving zou krijgen binnen de EU. Onder andere Frankrijk, Duitsland en Spanje hebben mogelijkheden in dezelfde richting. Daarnaast kan worden opgemerkt dat de huidige obstakels voor de Nederlandse opsporingsinstanties ook in andere EU-lidstaten worden ervaren. De oplossingsrichtingen in verschillende lidstaten lopen uitéén. De wettelijke regelingen van de lidstaten en, daarmee samenhangend, de verschillen in de wettelijke voorwaarden, laten zich dan ook lastig vergelijken.
Met de wet van 5 juni 2016 voorziet de Franse wetgeving in de bevoegdheid heimelijk een technisch hulpmiddel te installeren met het doel toegang te verkrijgen tot elektronische gegevens. Ingeval het opsporingsonderzoek met betrekking tot ernstige strafbare feiten als opgenomen in de artikelen 706–73 en 706-73-1 (zoals moord, drugshandel, mensenhandel, terroristische misdrijven, witwassen) van de Franse Code de procédure penale daartoe noodzaakt kan de «juge des libertés en de la détention» (rechter die over voorlopige hechtenis oordeelt), op verzoek van de procureur van de Republiek, de daartoe door de procureur aangewezen opsporingsambtenaren machtigen tot het plaatsen van een technisch hulpmiddel ten behoeve van het heimelijk binnendringen van een geautomatiseerd werk en het vastleggen en overnemen van de gegevens die in het geautomatiseerde werk zijn opgeslagen. De machtiging van de rechter bevat een omschrijving van het strafbare feit, de precieze locatie of de nauwkeurige beschrijving van het geautomatiseerde werk evenals de duur van de inzet. De maximale geldigheidsduur is een maand, met de mogelijkheid van verlenging met een maand.
Ook de Franse onderzoeksrechter («juge d'instruction») kan, ingeval van een opsporingsonderzoek in verband met de bovengenoemde strafbare feiten, tijdens een gerechtelijk vooronderzoek («sur commission rogatoire»), op advies van de procureur van de Republiek, de opsporingsambtenaren machtigen tot het plaatsen van een technisch hulpmiddel ten behoeve van het heimelijk binnendringen van een geautomatiseerd werk en het vastleggen en overnemen van de gegevens die in het geautomatiseerde werk zijn opgeslagen. De maximale geldigheidsduur van de machtiging is vier maanden, met de mogelijkheid van verlenging tot maximaal twee jaar.
In de memorie van toelichting is reeds ingegaan op de wetgeving in Duitsland, waarin een bevoegdheid is opgenomen die de Duitse Bondsrecherchedienst («Bundeskriminalamt») de mogelijkheid geeft om zich ter bestrijding van terrorisme onder bepaalde voorwaarden heimelijk met behulp van technische middelen toegang te verschaffen tot informatiseringsystemen en daaruit gegevens te verkrijgen. Daarvoor kan worden verwezen naar de beschrijving in paragraaf 2.7. van de memorie van toelichting (Kamerstukken II 2015/16, 34 372, nr. 3).
Het is de regering niet bekend dat Frankrijk en Duitsland hebben gekozen af te zien van het gebruik van spyware omdat oneigenlijk gebruik door derden niet viel uit te sluiten. Het feit dat in Frankrijk onlangs een bevoegdheid in de wetgeving is opgenomen tot het met een technisch hulpmiddel op afstand binnendringen in geautomatiseerd werken ten behoeve van het vastleggen en overnemen van de gegevens, wijst ook niet in die richting.

De leden van de D66-fractie hebben gevraagd of de keuze van Frankrijk en Duitsland niet zozeer principieel als wel door een gebrek van keuring was ingegeven.
Het is mij niet bekend door welke feiten de keuzes, die door de Franse en Duitse autoriteiten zijn gemaakt, destijds zijn ingegeven. Zoals hierboven aan de orde is gekomen, voorzien de Duitse en Franse wetgeving in de mogelijkheid van het op afstand binnendringen van een geautomatiseerd werk.

De leden van de D66-fractie hebben gevraagd hoe met keuring van het technische hulpmiddel misbruik precies wordt voorkomen.
De keuring van het technische hulpmiddel is gericht op de werking van het technische hulpmiddel. Een van de eisen waaraan een technisch hulpmiddel dient te voldoen en die neergelegd wordt in het besluit ter uitvoering van dit wetsvoorstel is dat een technisch hulpmiddel via versleuteling beveiligd wordt tegen misbruik.

De leden van de D66-fractie hebben de regering gevraagd nader in te gaan op de gevolgen voor het digitale vestigingsklimaat van Nederland als gevolg van deze situatie.
Het vestigingsklimaat van Nederland is gebaat bij een open, vrij en veilig internet. Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen, om zo een open, vrij en veilig internet te kunnen blijven garanderen. De bevoegdheid tot binnendringen in een geautomatiseerd werk is hiervoor van groot belang. Gezien de mogelijk grote inbreuk op de persoonlijke levenssfeer wordt de bevoegdheid alleen onder strenge voorwaarden ingezet en met passende waarborgen omkleed. Zoals hierboven, bij de beantwoording van eerdere vragen van de leden van deze fractie over cloudcomputingdiensten (paragraaf 2.1) aan de orde is gekomen, zijn er clouddienstverleners die niet erg constructief meewerken aan opsporingsonderzoeken en zelfs technische maatregelen nemen om de opsporing van strafbare feiten te verhinderen (zogenaamde bullet proof hosting providers). Het op afstand binnendringen bij dienstverleners kan om die reden niet bij voorbaat worden uitgesloten en zal zijn beperkt tot uitzonderlijke gevallen. Hier staat tegenover dat de voorgestelde bevoegdheid juist ook mogelijkheden biedt om de aanbieders te beschermen als jegens hen strafbare feiten zijn gepleegd met behulp van geautomatiseerde werken. Mede gelet op de wettelijke criteria voor de inzet van de voorgestelde bevoegdheid zal de mogelijkheid van de inzet daarvan naar verwachting geen grote gevolgen hebben voor de Nederlandse economie en het Nederlandse vestigingsklimaat.

Voorts hebben de leden van de D66-fractie een nadere toelichting gevraagd van de inschatting van de regering van het risico dat landen als China of Rusland dit wetsvoorstel zullen aangrijpen om hacken in het buitenland te rechtvaardigen.
Digitale aanvallen van statelijke actoren vormen op dit moment de grootste dreiging in het digitale domein voor de nationale veiligheid. Het gaat hierbij om grote belangen, waarbij niet alleen overwegingen rond de staatsveiligheid een rol spelen maar ook rond concurrentie. De modus operandi neemt in complexiteit toe, aanvallers worden vindingrijker en ontwikkelen steeds betere methodes om onderkenning en attributie te voorkomen. In de openbaarheid wordt iedere betrokkenheid ontkend. Het voorliggende wetsvoorstel zal naar verwachting dan ook geen verandering brengen in de overwegingen van andere landen om Nederlandse systemen wederrechtelijk binnen te dringen, noch om hun betrokkenheid hierbij te ontkennen.

De leden van de D66-fractie hebben gevraagd of de regering kennis heeft genomen van de stellingname van Apple, die juist vanwege de risico's van technische kwetsbaarheden voor alle andere gebruikers, weigert de beveiliging van de iPhone te kraken en een «gevaarlijke achterdeur» in te bouwen waardoor de FBI zich toegang kan verschaffen tot de iPhone van een vereende terrorist. De leden van deze fractie hebben tevens gevraagd hoe de regering de keuze van Apple beschouwt om niet ten behoeve van een persoon de beveiliging van alle iPhones wereldwijd op het spel te zetten door technische ontsleuteling te creëren van de beveiliging waar alle gebruikers van de iPhone wereldwijd op vertrouwen.
Met deze vraag verwijzen de leden van de D66-fractie naar de rechtszaak die inmiddels is gestopt waar de FBI wilde dat Apple zou helpen om de iPhone5 van een verdachte van een terroristisch misdrijf toegankelijk te maken voor onderzoek. Over deze zaak draagt de regering alleen kennis via de openbare publicaties. Bovendien is de zaak aanhangig gemaakt bij een Amerikaanse rechter, ter beoordeling naar Amerikaans recht. De Nederlandse regering is daarom terughoudend hierover een oordeel uit te spreken. De Nederlandse wetgeving voorziet reeds in de verplichting voor degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de wijze van beveiliging van een geautomatiseerd werk of de versleuteling van gegevens, tot het beschikbaar stellen van kennis omtrent de beveiliging of de versleuteling (art. 125k, 126m, zesde lid, en 126nh Sv). Deze verplichting strekt echter niet zover dat een aanbieder van een product of dienst gehouden zou zijn om kwetsbaarheden in te bouwen met het oog op mogelijk gebruik door politie en justitie behoeve van de opsporing en vervolging van strafbare feiten. Het bevel tot het verschaffen van toegang tot een geautomatiseerd werk kan niet aan de verdachte worden gegeven. Inmiddels heeft het kabinet, bij brief van 4 januari 2016, een standpunt over encryptie aan Uw Kamer doen toekomen (Kamerstukken II 2015/16, 26 643, nr. 383). In het kabinetsstandpunt wordt de noodzaak tot rechtmatige toegang tot gegevens en communicatie, in het licht van de taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen, onderstreept. Het kabinet onderschrijft tegelijkertijd het belang van sterke encryptie voor de veiligheid op internet ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven, en voor de Nederlandse economie. Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om, in aanvulling op de bestaande verplichtingen, beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland.

2.8 Onderzoek in een geautomatiseerd werk en rechtsmacht

2.8.1 Inleiding

De leden van de PvdA-fractie hebben gevraagd of zij het goed begrijpen als zij stellen dat indien bekend is dat een geautomatiseerd systeem in het buitenland staat dat dan voor de bevoegdheid tot het op afstand onderzoeken gebruik zal worden gemaakt van een rechtshulpverzoek. Zij hebben tevens gevraagd of dit standaard gebeurt of dat hierop uitzonderingen mogelijk zijn en wanneer de noodzaak om snel in te grijpen voor gaat op het achterhalen van de locatie van een server en het uitvaardigen van een rechtshulpverzoek.
De leden van de PvdA-fractie hebben het goed begrepen dat, indien bekend is dat het geautomatiseerde werk zich op het grondgebied van een andere staat bevindt, een verzoek tot rechtshulp aan de bevoegde autoriteiten van die staat zal worden gedaan. De regering hecht veel waarde aan internationale samenwerking bij de bestrijding van de criminaliteit en acht het van groot belang dat, zodra bekend is dat gegevens zich op het grondgebied van een andere staat bevinden, zo snel

mogelijk een verzoek tot rechtshulp wordt gedaan en verantwoording wordt afgelegd over de reeds verrichte handelingen en de daarbij gemaakte afwegingen. Dit is een standaard procedure en er is geen reden om, als bekend is dat een geautomatiseerd werk of de gegevens zich op het grondgebied van een andere staat bevinden, een rechtshulpverzoek uit te stellen. Daarbij is het echter niet uitgesloten dat, in afwachting van een reactie van de betreffende staat, bepaalde onderzoekshandelingen worden verricht. Dit is sterk afhankelijk van de aard en ernst van de strafbare feiten, de te verrichten onderzoekshandelingen en de aard van de rechtshulprelatie met het betreffende land. Het is bijvoorbeeld niet uitgesloten dat vanuit een andere staat een DDOS-aanval wordt gedaan op kritische Nederlandse infrastructuur, waardoor de online afhandeling van het betalingsverkeer door banken onmogelijk is of de werking van militaire installaties wordt belemmerd. In een dergelijk geval kan het dringend noodzakelijk zijn om op te treden en een server binnen te dringen en bepaalde gegevens ontoegankelijk te maken zodat de DDOS-aanval kan worden beëindigd. Ook kan worden gedacht aan een situatie waarin sprake is van een terroristische dreiging, waarbij in een geautomatiseerd werk wordt binnengedrongen om telecommunicatie af te tappen of gegevens over te nemen om de daders zo snel mogelijk te kunnen achterhalen en een aanslag te voorkomen. Dit optreden kan niet bij voorbaat worden uitgesloten wanneer de aangezochte staat niet of niet tijdig op het rechtshulpverzoek reageert. In een dergelijk geval gaat de noodzaak van onverwijld ingrijpen voor op het afwachten van de reactie van de aangezochte staat. Hierbij weegt de intensiteit van de rechtshulprelatie met die betreffende staat ook mee. Als het gaat om een staat waarmee Nederland een intensieve relatie onderhoudt dan is de afweging anders dan wanneer het een staat betreft die bekend staat als een notoire «safe haven» voor criminaliteit. Dit neemt uiteraard niet weg dat, als de betrokken staat daarom vraagt, altijd verantwoording zal worden afgelegd over het handelen de daarbij gemaakte afwegingen.

De leden van de PvdA-fractie hebben gevraagd wat er gebeurt in het geval bekend is dat het geautomatiseerde werk in een land staat waar Nederland geen relatie mee heeft voor het uitwisselen van rechtshulpverzoeken of wanneer de aangezochte staat geen rechtshulp verleent. Zij hebben gevraagd of dan toch op afstand onderzoek kan worden gedaan. Zoals hierboven, naar aanleiding van een soortgelijke vraag van deze fractie, is opgemerkt wordt, zodra bekend is op het grondgebied van welke staat het geautomatiseerde werk zich bevindt, een rechtshulpverzoek aan die staat gericht. Dit geldt ook wanneer dit een staat betreft waarmee Nederland geen hechte rechtshulprelatie heeft. Echter, afhankelijk van de aard en ernst van het strafbare feit, de ingrijpendheid van de te verrichten onderzoekshandelingen en de intensiteit van de rechtshulprelatie, kan in uitzonderlijke gevallen worden besloten om op te treden, in afwachting van de reactie van de aangezochte staat. Dit is hierboven reeds aan de orde gekomen.

De leden van de ChristenUnie hebben gevraagd om een nadere toelichting op de vraag of het mogelijk is in computers of computergegevens die zich buitenslands bevinden binnen te dringen. En of de regering nader kan onderbouwen waarom dit niet op internationaalrechtelijke bewaren zal stuiten.
Het is inderdaad mogelijk om in computers binnen te dringen die zich in het buitenland bevinden en toegang te verkrijgen tot gegevens die op die computer zijn opgeslagen. In het rapport van de zogenaamde Transborder Group van de Raad van Europa wordt geconstateerd dat opsporingsdiensten van veel staten zich in de praktijk toegang verschaffen tot gegevens die zijn opgeslagen in geautomatiseerde werken die zich op het grondgebied van andere staten bevinden, ten behoeve van het veilig-

stellen van elektronisch bewijs. Hiermee kan echter inbreuk worden gemaakt op de soevereiniteit van die staten waar het geautomatiseerde werk zich bevindt. De Nederlandse regering acht het van groot belang dat de landen internationaal met elkaar samenwerken om te komen tot een gemeenschappelijk optreden bij de aanpak van grensoverschrijdende computercriminaliteit. Als Voorzitter van de Raad van de Europese Unie heeft Nederland dit onderwerp geagendeerd. Daarnaast neemt Nederland actief deel aan het overleg in het kader van de Cybercrime Conventie van de Raad van Europa. De ontwikkeling van een dergelijk gemeenschappelijk internationaal optreden is echter pas op langere termijn te realiseren. In afwachting daarvan zal, als een verzoek om rechtshulp geen uitkomst biedt, moeten worden gekozen tussen twee minder ideale situaties, namelijk het afzien van het verrichten van opsporingshandelingen wanneer niet bekend is waar deze gegevens zich bevinden of in uitzonderlijke gevallen het onder voorwaarden zelfstandig uitoefenen van uitvoerende rechtsmacht. Vanwege de dringende belangen die hierbij in het geding zijn kiest de regering voor de laatste optie, waarbij zo zorgvuldig mogelijk wordt gehandeld en, zodra bekend is dat een geautomatiseerd werk zich in een andere staat bevindt, zo snel mogelijk een verzoek tot rechtshulp wordt gedaan. In uitzonderlijke gevallen zal, in afwachting van een reactie op dit verzoek, opgetreden moeten kunnen worden. Dit is hierboven, in de beantwoording van de vragen van de leden van de PvdA-fractie, reeds aan de orde gekomen. De regering gaat ervan uit dat deze handelwijze niet op internationaalrechtelijke bezwaren stuit, juist omdat rechtshulp zal worden gevraagd zodra de locatie van het geautomatiseerde werk bekend is. Hiermee wordt tegemoet gekomen aan het soevereiniteitsbeginsel, dat met zich meebrengt dat een staat exclusief bevoegd is tot het handelen op het eigen grondgebied en jegens eigen onderdanen.

2.8.2 Uitvoerende rechtsmacht en de bestrijding van computercriminaliteit

De leden van de VVD-fractie zijn van mening dat zelfstandig optreden zorgvuldige inkadering behoeft op basis van een stapsgewijze aanpak. Deze leden hebben gevraagd welke stappen en criteria in een Aanwijzing door het OM worden uitgewerkt.
In gevallen waarin de feitelijke locatie van de gegevens redelijkerwijs niet te achterhalen is, bijvoorbeeld wanneer vrijwel alle gegevens in de cloud zijn opgeslagen, kan onder omstandigheden zelfstandig rechtsmacht worden uitgeoefend bij de bestrijding van computercriminaliteit. In dergelijke situaties dient de bevoegdheid tot het binnendringen en onderzoek doen in een geautomatiseerd werk op zorgvuldige wijze toegepast te worden. Het voorgestelde artikel 126nba, achtste lid, Sv biedt de mogelijkheid om bij algemene maatregel van bestuur regels te stellen over de bevoegdheid om onderzoekshandelingen te verrichten in een geautomatiseerd werk in de gevallen waarin niet bekend is waar de gegevens zijn opgeslagen. Het is goed denkbaar dat deze regels niet in een algemene maatregel van bestuur, maar in een OM-aanwijzing worden neergelegd. Het opsporingsonderzoek vindt plaats onder de verantwoordelijkheid van het openbaar ministerie. Via beleidsregels van het openbaar ministerie, in de vorm van een aanwijzing, kunnen de consistentie en de kwaliteit van de opsporing worden bevorderd en kunnen waarborgen worden geformuleerd voor een zorgvuldige toepassing van de bevoegdheid. De facultatieve formulering van de delegatiegrondslag in het eerdergenoemde achtste lid («kunnen regels worden gesteld») biedt ruimte voor regulering op het niveau van een OM-aanwijzing.
In een OM-aanwijzing kan worden uitgewerkt welke werkwijze wordt gehanteerd bij het zelfstandig optreden, hoe daarbij rekening gehouden wordt met veranderende omstandigheden gedurende het onderzoek, welke minimale inspanning vereist is bij het achterhalen van de identiteit

en locatie van een geautomatiseerd werk en welke criteria bij de afweging om over te gaan tot een vervolgstap in het onderzoek worden betrokken. Wanneer op basis van de beschikbare informatie de reikwijdte van het bevel onvoldoende kan worden ingeschat zal een stapsgewijze aanpak worden gevolgd waarbij de officier van justitie telkens een beperkt bevel afgeeft voor een bepaalde stap in het proces. Over het algemeen zal de officier van justitie starten met een beperkt eerste bevel op grond waarvan bepaalde kenmerken van het geautomatiseerde werk of de gebruiker in kaart kunnen worden gebracht. Eventuele vervolgstappen, zoals het overnemen van gegevens, kunnen dan pas plaatsvinden als de officier van justitie, na een zorgvuldige afweging van alle betrokken belangen, een aanvullend bevel heeft afgegeven. In een OM-aanwijzing kunnen de criteria die een rol spelen bij de belangenafweging nader worden uitgewerkt. Hierbij kan worden gedacht aan de ernst van het feit, de aanknopingspunten met de Nederlandse rechtsorde, de aard en ingrijpendheid van de opsporingshandelingen en de risico's voor het geautomatiseerde werk.

De leden van de PvdA-fractie hebben gelezen dat toch in een geautomatiseerd werk kan worden binnengedrongen als de locatie van gegevens niet te achterhalen is en hebben gevraagd of de regering de mening van het College van procureurs-generaal deelt dat Nederland op grond van de ubiquiteitsleer rechtsmacht heeft. Zij hebben tevens gevraagd of de regering kan uitleggen hoe deze leer in dat verband werkt en waar binnen het Nederlandse recht deze leer nog meer wordt gebruikt om rechtsmacht te vestigen. Ook hebben zij gevraagd of er relevante jurisprudentie bestaat en zo ja, wat deze inhoudt.
Volgens de ubiquiteitsleer wordt een misdrijf geacht te zijn gepleegd daar waar de dader gehandeld heeft of had moeten handelen of waar het constitutieve gevolg is ingetreden of naar de voorstelling van de dader had moeten intreden. De ubiquiteitsleer is vooral van belang voor het bepalen van de plaats waar een strafbaar feit (mede) is gepleegd, met het oog op het bepalen van de jurisdictie van een staat. Dit betreft de zogenaamde wetgevende rechtsmacht, die moet worden onderscheiden van de zogenaamde uitvoerende rechtsmacht. De uitvoerende rechtsmacht heeft betrekking op het uitvoeren van handelingen door de Nederlandse rechtshandhavingsautoriteiten met het oog op opsporing en vervolging in Nederland. In de gevallen waarin kan worden aangenomen dat Nederland over wetgevende rechtsmacht beschikt, voorziet artikel 539a Sv in een wettelijke basis om opsporingshandelingen te verrichten en dus uitvoerende rechtsmacht uit te oefenen buiten Nederland, voor zover het volkenrecht en interregionale recht dit toelaten. Op grond van het volkenrecht is het soevereiniteitsbeginsel relevant, dat als uitgangspunt hanteert dat een staat slechts uitvoerende rechtsmacht mag uitoefenen op het grondgebied van een andere staat met instemming van die staat. De regering is niet bekend met specifieke jurisprudentie over de uitoefening van uitvoerende rechtsmacht bij de opsporing van cybercrime. Wel is in andere strafzaken het verweer gevoerd dat het optreden van Nederlandse opsporingsambtenaren op het grondgebied van een andere staat, zonder voorafgaande instemming van die staat, als onbevoegd moet worden aangemerkt en de informatie onrechtmatig verkregen is. Dit betrof onder meer een geval waarin op Belgisch grondgebied door Nederlandse opsporingsambtenaren opsporingshandelingen waren verricht en een geval waarin een verdachte op Duits grondgebied door Nederlandse opsporingsambtenaren was aangehouden. De Hoge Raad oordeelde 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 BL5629 en HR 17 april 2012 BV9070). Dit laat echter onverlet dat de soevereiniteit van een andere staat kan worden aangetast. Zodra bekend is dat gegevens zich op het grondgebied van een andere staat bevinden zal dan ook zo snel mogelijk een verzoek tot rechtshulp wordt gedaan. De werkwijze in de gevallen waarin de feitelijke locatie van de gegevens redelijkerwijs niet te achterhalen is zal worden uitgewerkt in een OM-aanwijzing. Dit is hierboven reeds aan de orde gekomen, naar aanleiding van vragen van de leden van de fracties van de PvdA en de VVD.

De leden van de PvdA-fractie hebben gevraagd of de regering het mogelijk acht dat het binnendringen in een buitenlandse geautomatiseerd werk zonder de toestemming van de autoriteiten in dat buitenland weliswaar geen schending van de soevereiniteit van dat land betekent, maar dat dat land in kwestie daar weleens heel anders over zou kunnen denken. De leden van deze fractie hebben tevens gevraagd of de regering het mogelijk acht dat dat land dat dan als rechtvaardiging ziet om ook in Nederlandse systemen binnen te dringen. Zij hebben voorts gevraagd of dat al gebeurt door opsporingsdiensten van landen waar reeds de mogelijkheid bestaat om op afstand heimelijk in geautomatiseerde werken binnen te dringen.
Zoals hierboven reeds aan de orde is gekomen, is het uitgangspunt dat rechtshulp wordt gevraagd als de te verrichten opsporingshandelingen betrekking hebben op gegevens die zich op het territorium van een andere staat bevinden. Een staat dient zijn bevoegdheden met de grootste zorgvuldigheid uit te oefenen, gezien het belang van het respecteren van de soevereiniteit van andere staten. Er is een zekere inspanning vereist om de feitelijke locatie van gegevens te achterhalen. Als bekend is, of in de loop van het onderzoek bekend wordt, dat de gegevens zich in een andere rechtsmacht bevinden dan is een verzoek om rechtshulp aangewezen, waarbij aan de bevoegde buitenlandse autoriteiten verantwoording wordt afgelegd over de handelingen die zijn verricht en de afwegingen die daarbij zijn gemaakt. Bij de uitoefening van opsporingshandelingen met betrekking tot gegevens die zich op het territorium van een andere staat blijken te bevinden, is het van belang dat er zo snel mogelijk alsnog toestemming wordt gevraagd van het desbetreffende land.
In internationaal verband is vastgesteld dat het territorialiteitsbeginsel in cyberspace onder druk staat en dat het beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. Eind 2012 al constateerde het Cybercrime Convention Committee van de Raad van Europa dat opsporingsdiensten van diverse landen in de praktijk reeds elektronisch bewijs van internet vergaarden op een wijze die wellicht verder gaat dan voorzien in het Cybercrimeverdrag uit 2001.[4] In 2014 constateerde het comité dat een groeiend aantal landen, ook binnen de EU, unilateraal maatregelen neemt om digitaal bewijs uit het buitenland of van onbekende locaties te vergaren.[5]
De verdere ontwikkeling van een internationaalrechtelijk kader, dat is toegesneden op de toepassing van uitvoerende rechtsmacht bij de bestrijding van computercriminaliteit, verdient de voorkeur. De Nederlandse regering hecht veel waarde aan een gemeenschappelijk optreden van staten bij de bestrijding van de grensoverschrijdende criminaliteit. De ontwikkeling van een dergelijk internationaalrechtelijk kader betreft echter

[4] «Transborder Access and Jurisdiction; what are the options?», report of the Transborder Group, 6 december 2012, blz. 57 (adopted by the T-Cy)
[5] «Transborder access to data and jurisdiction: Options for further action by the T-CY», Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction, blz. 7.

een ideaal dat slechts op langere termijn kan worden gerealiseerd. Nederland zet zich in het kader van de Raad van Europa en binnen de EU actief in voor het ontwikkelen daarvan.

De leden van de D66-fractie hebben gevraagd of de regering het mogelijk acht dat op het moment dat Nederlandse opsporingsdiensten buitenlandse servers gaan binnendringen, daarmee het risico bestaat dat buitenlandse opsporingsdiensten dat andersom gaan doen en zo ja, wat dat betekent voor de veiligheid van onze systemen, en zo nee, waarom niet.
Zoals hiervoor is opgemerkt constateerde het Cybercrime Convention Committee van de Raad van Europa dat opsporingsdiensten van diverse landen in de praktijk reeds elektronisch bewijs van internet vergaarden op een wijze die wellicht verder gaat dan voorzien in het Cybercrimeverdrag uit 2001. In 2014 constateerde het comité dat een groeiend aantal landen, ook binnen de EU, unilateraal maatregelen neemt om digitaal bewijs uit het buitenland of van onbekende locaties te vergaren. Het risico waaraan de leden van de D66-fractie hebben gerefereerd, is dus reeds praktijk.

De leden van de PvdA-fractie hebben gevraagd of de bevoegdheid op afstand heimelijk onderzoek te doen in een geautomatiseerd werk of het ontoegankelijk maken van gegevens negatieve gevolgen voor het Nederlandse vestigingsklimaat kan hebben, niet zozeer omdat de Nederlandse overheid deze bevoegdheid heeft, maar veeleer omdat in het kader van de wederkerigheid buitenlandse entiteiten mogelijk makkelijker op een Nederlandse server binnendringen en daarmee Nederland niet veilig is voor hun gegevens. Deze leden hebben tevens gevraagd hoe deze bevoegdheid zich verhoudt tot het WRR-rapport waarin staat dat Nederland de integriteit van het world wide web zou moeten beschermen tegen statelijke actoren.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van twee soortgelijke vragen van de leden van de D66 fractie, over de gevolgen voor het vestigingsklimaat en over de invloed van dit wetsvoorstel op het handelen van andere staten (paragrafen 2.1 en 2.7).

De leden van de CDA-fractie hebben gevraagd of de regering voor zichzelf hier een rol weggelegd ziet in de eerste helft van dit jaar als EU-voorzitter om op dit terrein vooruitgang te boeken en zo ja, op welke wijze kan zij komen tot voorstellen om het zogeheten Cybercrime Verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290) te verruimen. Deze leden achten de aankondiging van de Minister van Buitenlandse Zaken op 12 februari 2016 dat Nederland komende maanden landen, bedrijven, denktanks en internetnetdeskundigen bij elkaar wil brengen om de cybersecurity te verbeteren niet alleen gewenst met betrekking tot de in het wetsvoorstel genoemde vormen van criminaliteit, maar ook ten aanzien van de huidige migratiecrisis en de daaraan verbonden samenwerking op terrein van mensensmokkel. Zij hebben gevraagd hoe de regering de waarde van onderhavig wetsvoorstel in dat perspectief beziet, welke bijdrage zij hiertoe levert en wat volgens de regering nog meer nodig is om op Europees en internationaal niveau stappen te zetten tot een betere aanpak van mensenhandel en digitale voorbereidingen hiertoe.
In antwoord op de vraag van de leden van de CDA-fractie over de inzet van Nederland als EU-voorzitter memoreer ik dat het onderwerp «jurisdictie in cyberspace» in verschillende Algemene overleggen (Kamerstukken II 2015/16, 32 317, nrs. 385 en 394) voorafgaand aan de JBZ raad van juni 2016 is besproken. De inspanningen van het Voorzitterschap richtten zich op het adequaat aanpakken van belemmeringen in de bestrijding van cybercriminaliteit en het vergaren van elektronisch bewijs

(e-evidence). Raadsconclusies over dit onderwerp zijn op 9 juni 2016 door de JBZ Raad aangenomen. De Raadsconclusies over criminal justice in cyberspace, hebben op hoofdlijnen betrekking op (1) 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 EU voor rechtshulp al eerder zijn ontwikkeld en gangbaar zijn, (2) het stroomlijnen en versnellen van de bestaande procedures voor wederzijdse rechtshulp en wederzijdse erkenning tussen EU-lidstaten onderling en tussen de lidstaten en derde landen, onder andere door digitalisering van verzoeken en automatische vertaling hiervan, als ook het vergroten van kennis en vaardigheden van hen die in de lidstaten deze verzoeken behandelen, en (3) het onderzoeken 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 is.
Daarnaast is Nederland is voorzitter van de Cybercrime Convention Committee van het Cybercrime Verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18 en Trb. 2004, 290). Nederland is actief voorstander van het uitwerken van mogelijkheden om het Cybercrime Verdrag te verruimen.

De leden van de CDA-fractie hebben gevraagd of de regering ook met welke derde landen zij een 24/7 contactpunt heeft om rechtshulp snel af te kunnen handelen en of gewerkt wordt aan uitbreiding van deze lijst teneinde met zoveel mogelijk landen een dergelijk contact op te bouwen. Er bestaan verschillende lijsten van deze contactpunten. Allereerst is er de lijst van verdragspartijen van het Cybercrime Verdrag (Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18 en Trb. 2004, 290). Deze landen zijn verplicht een contactpunt in te richten. Maar ook landen die waarnemer zijn bij dit verdrag, dan wel een verzoek om toetreding hebben gedaan, beschikken doorgaans over een dergelijk contactpunt. Het gaat dan om ruim 60 landen, waaronder de EU landen en de VS. Daarnaast heeft de G7 een lijst met contactpunten die gedeeltelijk overlapt met de lijst van de Raad van Europa. Deze lijsten breiden zich gaandeweg uit. Overigens kan rechtshulp ook ad hoc en rechtstreeks aan de centrale autoriteiten van een land worden gevraagd.

De leden van de D66-fractie hebben gelezen dat het bepaald niet is uitgesloten dat meerdere staten rechtsmacht hebben bij de opsporing en vervolging van vormen van computercriminaliteit, en hebben gevraagd welke medewerking en bereidheid tot onderling overleg Nederland in die gevallen kan verwachten zowel binnen als vooral buiten Europa. Deze leden hebben tevens gevraagd wat de ervaringen tot op heden zijn met overleg in geval van overlappende rechtsmacht.
Wanneer er sprake is van overlappende rechtsmacht leidt dit in de praktijk doorgaans tot constructief overleg en een gezamenlijke oplossing, zoals dat ook in de fysieke wereld het geval is wanneer er verschillende aanknopingspunten zijn om rechtsmacht aan te nemen om criminele feiten te onderzoeken. Voor internationaal contact in het kader van opsporingsonderzoeken op internet beschikken veel landen over een 24/7 contactpunt, zoals voorgeschreven door het Cybercrimeverdrag. Deze contactpunten bevorderen de snelheid van noodzakelijk internationaal overleg. Daarnaast kan voor contact tussen de EU-lidstaten gebruik worden gemaakt van «joint investigation teams» of overlegstructuren bij Europese instellingen zoals Europol en Eurojust.

De leden van de CDA-fractie hebben gevraagd hoeveel verzoeken er jaarlijks binnen komen en in hoeveel gevallen een rechtshulpverzoek van Nederland en aan Nederland is afgewezen.

In het tweede half jaar van 2014 zijn 48 rechtshulpverzoeken binnengekomen bij het 24/7 contactpunt van het team High Tech Crime van de nationale politie. In 2015 zijn hier 162 verzoeken binnengekomen. Dit jaar zijn er in de periode tot en met juni 87 verzoeken binnengekomen. Dit komt neer op een gemiddelde van 8 verzoeken per maand in 2014, 13,5 verzoeken in 2015 en 14,5 in 2016. Rechtshulpverzoeken aan Nederland worden in principe altijd in behandeling genomen. Het kan voorkomen dat na het in behandeling nemen van een verzoek door nader onderzoek blijkt dat de gevraagde informatie toch niet bij een Nederlandse server staat maar bij een buitenlandse «reseller» waar deze informatie vervolgens opgevraagd moet worden.

2.9 De bescherming van grondrechten

De leden van de SP-fractie hebben begrepen dat bij de afweging om een bevel tot heimelijk onderzoek in een geautomatiseerd werd sprake moet zijn van een dringend opsporingsbelang en hebben gevraagd wanneer een opsporingsbelang dringend is en wanneer niet.
In de tekst van het voorgestelde artikel 126nba/uba/zpa is vastgelegd dat de officier van justitie, indien «het onderzoek dit dringend vordert», kan bevelen dat door een opsporingsambtenaar wordt binnengedrongen in een geautomatiseerd werk. Het vereiste dat «het onderzoek dit dringend vordert» wordt eveneens als extra voorwaarde gebruikt bij enkele zeer ingrijpende opsporingsbevoegdheden als de infiltratie (art. 126h/p/ze Sv), het aftappen van communicatie (art. 126m/t/zg Sv), het direct afluisteren van vertrouwelijke communicatie (art. 126l/s/zf Sv) en het vorderen van gevoelige persoonsgegevens (art. 126nf/uf/zo Sv). Met deze voorwaarde wordt tot uitdrukking gebracht dat de inzet van de bevoegdheid voldoet aan de vereisten van proportionaliteit en subsidiariteit. De toetsing van de proportionaliteit hangt af van de concrete omstandigheden van het geval. Daarnaast moet worden vastgesteld dat de gegevens niet op een andere, minder ingrijpende wijze kunnen worden verkregen, waarbij rekening moet worden gehouden met de gevolgen van de toepassing van de bevoegdheid voor het betreffende geautomatiseerde werk en de betrokken personen. De officier van justitie en de rechter-commissaris dienen daarbij het onderzoeksbelang af te wegen tegen het belang van de bescherming van de persoonlijke levenssfeer, alsmede de risico's die aan de bevoegdheid zijn verbonden. Wanneer de rechter-commissaris wordt gevraagd een machtiging af te geven voor dergelijke, alleen bij dringende noodzakelijkheid in te zetten, bevoegdheden, dient hij niet alleen de rechtmatigheid van die inzet te beoordelen, maar daarbij tevens doelmatigheidsafwegingen in zijn oordeel te betrekken. In dat geval zal de rechter-commissaris ook de beleidsmatige keuze van de officier van justitie moeten toetsen, en kan hij niet volstaan met het oordeel dat de officier van justitie in redelijkheid heeft kunnen komen tot het standpunt dat de dringende noodzaak tot inzet van de bevoegdheid aanwezig is. Het belang van deze explicitering van het subsidiariteitsbeginsel schuilt vooral in het feit dat in het bevel tot infiltratie verantwoording zal moeten worden afgelegd van deze afweging.

De leden van de SP-fractie hebben gevraagd hoe men van tevoren weet waar men moet zijn. Deze leden hebben tevens gevraagd wat wordt gedaan met gegevens die niet relevant zijn voor de opsporing.
Er zijn verschillende soorten opsporingsonderzoeken, namelijk onderzoeken waarin van begin af aan duidelijk is naar welke informatie wordt gezochten opsporingsonderzoeken waarin er slechts aanwijzingen beschikbaar zijn die mogelijk kunnen leiden tot gegevens die voor de opsporing relevant zijn. Het inzetten van de bevoegdheid om heimelijk binnen te dringen in een geautomatiseerd werk wordt pas ingezet nadat er voldoende reden is en er ook aanwijzingen zijn naar welke gegevens

gezocht moet worden. Er zal dan gestart worden met zoeken in de geautomatiseerde systemen, waarvan verwacht mag worden dat daar de informatie gevonden kan worden, c.q. aanwijzingen te vinden zijn die kunnen leiden tot de te zoeken gegevens. De Wet politiegegevens is van toepassing op gegevens die worden verzameld met het oog op de uitvoering van de politietaak. De gegevens die niet relevant zijn voor de opsporing, zullen conform die wet worden verwijderd en vernietigd.

De leden van de PvdD-fractie wilden weten in hoeverre de regering recente jurisprudentie heeft meegenomen in dit wetsvoorstel en hoe de regering de bewering beoordeelt dat dit wetsvoorstel de privacy van Nederlanders aantast, zeker gezien de recente Europese ontwikkelingen om het recht op privacy juist te beschermen.
Het recht op privacy wordt zowel in het Nederlandse recht als het Europese recht beschermd. In de Grondwet is vastgelegd dat eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht heeft op eerbiediging van zijn persoonlijke levenssfeer (art. 10, eerste lid, GW). In het Europees Verdrag ter bescherming van de Rechten van de Mens en de fundamentele vrijheden (EVRM) is het recht van eenieder op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie (art. 8, eerste lid, EVRM) vastgelegd. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht dan voor zover bij de wet voorzien en in een democratische samenleving noodzakelijk is in het belang van bepaald aangewezen maatschappelijke belangen, waaronder het voorkomen van wanordelijkheden en strafbare feiten (art. 8, tweede lid, EVRM). Het Handvest van de grondrechten van de Europese Unie voorziet eveneens in het recht van eenieder op bescherming van zowel het privéleven en van het familie- en gezinsleven (art. 7 Handvest) als de bescherming van persoonsgegevens (art. 8 Handvest). Het recht op de bescherming van de persoonlijke levenssfeer is geen absoluut recht maar dient te worden afgewogen tegen andere maatschappelijk zwaarwegende belangen, zoals bijvoorbeeld het belang van de voorkoming en opsporing van strafbare feiten. In de rechtspraak van het Europese Hof ter bescherming van de rechten van de Mens en de Fundamentele vrijheden (EHRM), het Hof van Justitie van de Europese Unie en de Hoge Raad is nader invulling gegeven aan de regels ter bescherming van de persoonlijke levenssfeer, zoals neergelegd in respectievelijk het EVRM, het Handvest voor de grondrechten en de Grondwet. Het voorliggende wetsvoorstel is getoetst aan deze regels en de jurisprudentie die op basis daarvan tot stand is gekomen en hierover is verantwoording afgelegd in de memorie van toelichting (paragraaf 2.9).
De recente Europese jurisprudentie geeft geen aanleiding tot aanpassing van het wetsvoorstel, dit wordt hieronder nader toegelicht. Het Europese Hof van Justitie heeft onlangs enkele arresten gewezen over de bescherming van persoonsgegevens die aanleiding hebben gegeven tot publiciteit. In de zaken van Digital Rights Ireland en Seitlinger (zaken C-293/12 en C-294/12) heeft het Hof uitspraak gedaan over het bewaren van telecommunicatiegegevens van burgers ten behoeve van de opsporing en vervolging van ernstige misdrijven. Naar aanleiding van dit arrest en de Voorlichting daarover van de Afdeling advisering van de Raad van State heeft de regering een reactie aan Uw Kamer gezonden (Kamerstukken 2014/15, 33 542, nr. 16). Kernpunt van dit arrest betreft de vraag in hoeverre de overheid gegevens van burgers kan verzamelen en opslaan, zonder dat er op het moment van het verzamelen aanwijzingen bestaan dat er een verband bestaat tussen het gedrag van de personen van wie gegevens worden opgeslagen en hun betrokkenheid bij zware criminaliteit. In het onderhavige wetsvoorstel is echter geen sprake van het verzamelen en opslaan van gegevens van personen zonder dat er op het moment van het verzamelen sprake is van aanwijzingen van betrokkenheid van die personen bij strafbare feiten. De voorgestelde

bevoegdheid van het binnendringen in een geautomatiseerd werk kan uitsluitend worden toegepast in geval van verdenking van betrokkenheid van een persoon bij ernstig misdrijf. Het arrest Seitlinger heeft dus betrekking op een andere situatie.
Vermeldenswaard is voorts de zaak Maximilian Schrems/Data Protection Commissioner (C-362/15) over de verstrekking van persoonsgegevens aan derde landen. In deze zaak heeft het Europese Hof van Justitie de doorgifte van persoonsgegevens door een dochterbedrijf van Facebook in Ierland aan het moederbedrijf in de Verenigde Staten getoetst aan de eisen die op grond van de privacyrichtlijn (richtlijn 95/46/EU) aan een dergelijke doorgifte moeten worden gesteld. De privacyrichtlijn biedt de mogelijkheid van doorgifte van persoonsgegevens aan een derde land als in dat land een passend beschermingsniveau wordt gewaarborgd. De Europese Commissie had in de beschikking nr. 2000/520/EG van 26 juli 2000 (PbEG L 215), beter bekend als de zogenaamde Safe Harbour beschikking, vastgesteld dat dit voor de Verenigde Staten het geval is. Het Hof van Justitie oordeelde deze beschikking ongeldig. Dit oordeel hield nauw verband met de toegang tot de gegevens voor de Amerikaanse veiligheidsdiensten. Voor een nadere toelichting op deze zaak kan worden verwezen naar de brief van de regering aan Uw Kamer van 30 november 2015, met een appreciatie van het arrest van het Hof van Justitie van de Europese Unie (Kamerstukken II 2015/16, 32 317, nr. 363), en het fiche over de doorgifte van persoonsgegevens uit de EU naar de VS na uitspraak van het Hof van Justitie van de Europese Unie (Kamerstukken II 2015/16, 22 112, nr. 2040). Het onderhavige wetsvoorstel heeft echter geen betrekking op de verstrekking van persoonsgegevens van burgers door particuliere bedrijven aan de autoriteiten van derde landen, die zijn belast met de bescherming van de nationale veiligheid. Ook het arrest Schrems heeft dus betrekking op een andere situatie dat die waarvoor dit wetsvoorstel een regeling wil bieden.
Het EHRM heeft onlangs een arrest gewezen over het afluisteren van telefoonverkeer dat aanleiding heeft gegeven tot publiciteit. Dit betreft het arrest Zakharov tegen Rusland, van 4 december 2015 (Application no. 47143/06). In dit arrest heeft het EHRM de Russische wetgeving op het gebied van het afluisteren van telecommunicatie door de Russische veiligheidsdiensten getoetst aan het EVRM, in het bijzonder artikel 8 van het EVRM. De klager, Roman Zakharov, had aangevoerd dat aanbieders afluistervoorzieningen hadden geïnstalleerd die de Russische geheime dienst (FSB) in de gelegenheid stelde om zonder voorafgaande rechterlijke toetsing telecommunicatie af te tappen (punt 10). Het Hof stelt vast dat de wetgeving van de Russische Federatie voorziet in de mogelijkheid van het verrichten van heimelijke onderzoekshandelingen, waaronder de interceptie van communicatie, zowel in het kader van een strafzaak als daarbuiten. In beginsel is een voorafgaande rechterlijke instemming vereist, behoudens spoedeisende zaken. Alsdan dient de rechter binnen vierentwintig uur na aanvang van de onderzoekshandeling te worden geïnformeerd. Het Hof herhaalt dat inbreuk op de persoonlijke levenssfeer van personen in het licht van artikel 8 EVRM alleen kan worden gerechtvaardigd als deze inbreuk in overeenstemming is met de wet, gericht is op een of meer legitieme belangen die zijn genoemd in het tweede lid van dat artikel en noodzakelijk is in een democratische samenleving met het oog op het bereiken van dat belang. De woorden «in overeenstemming met de wet» hebben betrekking op zowel een grondslag in het nationale recht als de verenigbaarheid met de «rule of law». De wetgeving moet aan kwaliteitseisen voldoen, deze met toegankelijk zijn voor de betrokkene en voorzienbaar voor wat betreft de gevolgen. De voorzienbaarheid in de context van de heimelijke bevoegdheden voor het toezicht of het volgen van personen («surveillance»), zoals de interceptie van communicatie, betekent niet dat de betrokkene kan voorzien wanneer hij wordt afgeluisterd zodat hij zijn gedrag kan aanpassen. Niettemin is het van

essentieel belang dat er duidelijke, gedetailleerde regels zijn over de interceptie van communicatie, in het bijzonder nu de beschikbare technologie zich voortdurend ontwikkelt. De nationale wetgeving moet voldoende duidelijk zijn zodat de burgers een duidelijke indicatie heeft over de omstandigheden waarin en de voorwaarden waaronder de overheidsdiensten bevoegd zijn een dergelijke maatregelen toe te passen (punt 228). Het Hof licht toe dat de wetgeving op dit punt ten minste aan de volgende waarborgen dient te bevatten: de aard van de misdrijven die aanleiding kunnen geven tot een bevel tot aftappen, een omschrijving van de categorie van personen die kunnen worden afgetapt, een beperking van de tijdsduur van het aftappen, de procedure voor het onderzoek, gebruik en de opslag van de verkregen gegevens, de condities voor doorgifte van de gegevens aan andere partijen en de omstandigheden waarin de opnamen mogen of moeten worden vernietigd (punt 231). De misdrijven behoeven niet uitputtend te worden gespecificeerd maar voldoende detail is vereist inzake de aard van de betreffende misdrijven (punt 244). Voor wat betreft de vraag of een maatregel «noodzakelijk is in een democratische samenleving» erkent een Hof een zeker «margin of appreciation» bij de afweging van de belangen van de staatsveiligheid en de inbreuk van de maatregel op het recht op het privéleven (232). Toepassing van de voorwaarden «in overeenstemming met de wet» en «noodzakelijkheid» impliceren dat de nationale wetgeving niet alleen toegankelijk en voorzienbaar moet zijn in de toepassing maar tevens dient de verzekeren dat de heimelijke bevoegdheden voor het toezicht of het volgen van personen uitsluitend worden toegepast voor zover «noodzakelijk in een democratische samenleving», in het bijzonder door te voorzien in adequate en effectieve waarborgen tegen misbruik (punt 236). Vervolgens onderzoekt het Hof de wetgeving van de Russische Federatie op basis van de vereisten van «voorzienbaarheid;» en «noodzakelijkheid». Het Hof overweegt dat de wetgeving interceptie toelaat voor een zeer ruime kring van misdrijven, inclusief zakkenrollerij (punt 244). Verder geeft de wetgeving geen indicatie van de omstandigheden waaronder de communicatie van een persoon kan worden afgeluisterd in verband met gevaar voor de nationale veiligheid, dit wordt vrijwel geheel aan de bevoegde autoriteiten ter beoordeling over gelaten (punt 248). Het Hof stelt vast dat de Russische rechter in de praktijk niet nagaat in hoeverre er sprake is van een redelijke verdenking tegen de betrokken persoon en de noodzakelijkheids- en proportionaliteitstoets niet toepast (punt 265). De wetgeving bevat geen eisen voor de inhoud van een rechterlijke machtiging tot om interceptie, zodat de machtigingen soms geen naam van een specifieke persoon of telefoonnummer bevatten maar interceptie toestaan voor een gebied waar een strafbaar feit is gepleegd. Sommige machtigingen bevatten geen tijdsduur, zodat de wetgeving veel ruimte laat aan de rechtshandhavingsautoriteiten over welke communicatie af te tappen en voor hoe lang (punt 265). Verder overweegt het Hof dat in spoedeisende zaken geen voorafgaande rechterlijke machtiging is vereist, anders dan bij de opsporing van ernstige misdrijven bevat de procedure onvoldoende beperkingen in gevallen en waarin de staatsveiligheid in het geding is. Het is aan de bevoegde autoriteiten om te bepalen wanneer de niet-justitiële spoedprocedure wordt gebruikt (punt 266). Het Hof stelt vast dat de wettelijke regeling de inlichtingendiensten en de politie in staat stelt om iedere communicatie zonder voorafgaande rechterlijke machtiging af te luisteren en zonder dat de rechterlijke machtiging aan de aanbieder te tonen (punt 269). De wetgeving verbiedt de vastlegging van informatie over de interceptie (punt 272). Nu niet is voorzien in een verplichting tot notificatie van de betrokkene voorziet de Russische wetgeving niet in een effectieve rechtsmiddelen tegen heimelijke maatregelen op het gebied van het toezicht op en volgen van personen als er geen strafzaak volgt (punt 298). In het licht van deze tekortkomingen stelt het Hof vast dat de Russische wetgeving niet voldoet aan het vereiste

van de «kwaliteit van de wet» en de «inbreuk» niet beperkt tot hetgeen «in een democratische samenleving noodzakelijk is» en concludeert dat artikel 8 EVRM is geschonden (punten 304 en 305).
De zaak Szabó en Vissy tegen Hongarije, van 12 januari 2016, (Application no. 37138/14) betrof een klacht over schending van art. 8 EVRM (privéleven/correspondentie) vanwege de Hongaarse wetgeving en met name regeling 7/E (3) van de Politiewet in combinatie met de Wet Nationale Veiligheid, omdat deze volgens de klagers onvoldoende duidelijke bepalingen en geen waarborgen tegen misbruik en willekeur bevatte. Deze regeling voorzag in de bevoegdheid van een speciale antiterreureenheid van de politie om geheime onderzoeksmethoden toe te passen, in het kader van het onderzoek naar verdachten van bepaalde concrete misdaden, in welk geval een rechter hiervoor toestemming moet verlenen en er een aantal aanvullende waarborgen gelden (m.n. concrete verdenking, vernietiging van niet-relevant materiaal binnen acht dagen, gemotiveerde toestemming), en anderzijds in het kader van het onderzoek ter bescherming van de nationale veiligheid), in welk geval de Minister van justitie voor de inzet toestemming moet verlenen en minder waarborgen gelden. Het Hof herhaalde een aantal observaties van de zaak Zakharov, zoals over de reikwijdte van de woorden «in overeenstemming met de wet» en de invulling van de criteria van de »voorzienbaarheid» en de «noodzakelijkheid in een democratische samenleving». Het Hof herhaalt eveneens dat de technische ontwikkeling de mogelijkheid biedt van grootschalig aftappen van communicatie van burgers en het belang dat van een simultane ontwikkeling van juridische en procedurele waarborgen ter bescherming van de rechten van individuen. In het licht van de behoefte aan een meer dringende bescherming van het privéleven is het des te belangrijker dat de wet voorziet in goede waarborgen van voorzienbaarheid en procedure zodat de inbreuken alleen plaatsvinden wanneer dit noodzakelijk is in een democratische samenleving. Het Hof stelt echter vast dat op grond van de Hongaarse wetgeving vrijwel iedere persoon aan geheime onderzoeksmethoden kan worden onderworpen. De categorieën van personen van wie de communicatie kan worden afgetapt, zijn niet wettelijk ingekaderd (punt 66). De autoriteiten zijn niet gehouden enige relatie tussen de betrokken personen en de voorkoming van enige terroristische dreiging aan te tonen (punt 67). Voor wat betreft het vereiste van de «noodzakelijkheid in een democratische samenleving» wijst het Hof op het ontbreken van voorafgaande rechterlijke toestemming voor interceptie (punt 73). Het feit dat tot toepassing kan worden besloten door de Minister van Justitie als politieke autoriteit draagt bij aan het risico op misbruik (punt 75 en 76). Verder wordt gewezen op de duur van de maatregel, voor een periode van ten hoogste 90 dagen met de mogelijkheid van verlenging (punt 74). Anders dan bij Zakharov, benadrukt het Hof het belang van toezicht achteraf, zowel in individuele gevallen als in zijn algemeenheid. Het belang van een dergelijk toezicht kan niet worden overschat in het licht van de mogelijke grootschaligheid van de gegevensverzameling. Het Hof wijst op het gebrek aan dergelijk toezicht in Hongarije (punt 79). Verder voorziet de wet niet in een verplichting tot notificatie van de betrokken personen zodat onvoldoende controle kan worden uitgeoefend op de toepassing van de bevoegdheid in de praktijk (punten 86 en 87). Het EHRM stelt unaniem een schending van art. 8 EVRM vast (punt 89).
Met deze arresten geeft het Hof verder invulling aan de jurisprudentie over artikel 8 EVRM en de vereisten die daaruit voortvloeien voor de wetgeving van de aangesloten staten op het gebied van de heimelijke toepassing van bevoegdheden voor het toezicht op en het volgen van personen. Dit betreft specifiek de vereisten van noodzakelijkheid en voorzienbaarheid. Daarbij is voor het Hof in het bijzonder de mogelijkheid van misbruik van de mogelijkheid tot het gebruik van de technologie door overheidsdiensten om grootschalig gegevens te verzamelen over

activiteiten van burgers een bron van zorg. De wettelijke regeling dient afdoende waarborgen te bevatten om dit risico te voorkomen. Te dien aanzien heeft het Hof in de zaken Zakharov en Szabo een aantal tekortkomingen benoemd in de wettelijke regelingen van respectievelijk de Russische Federatie en Hongarije. In de zaak Zakharov oordeelde het Hof dat het Russische wettelijke systeem geen adequate en effectieve garanties en waarborgen tegen misbruik bood, dit betrof in het bijzonder de omstandigheden waarin de autoriteiten bevoegd waren tot het heimelijk aftappen van telecommunicatie, de duur van het heimelijk aftappen, de procedures voor het vernietigen en opslaan van onderschepte data, de procedures voor het autoriseren van de autoriteiten om aftapmaatregelen te nemen, het toezicht op de interceptie en de notificatie van de interceptie en de effectiviteit van de beschikbare rechtsmiddelen. In de zaak Szabo ontbraken duidelijke criteria om te kunnen inschatten bij wie deze methoden wel of niet zullen worden toegepast (punt 67). Het Hof maakte zich er ernstig zorgen over dat in de Hongaarse regeling geen enkele verdenking nodig is en een volledige discretie voor de autoriteiten bestaat om te besluiten tot het toepassen van geheime onderzoeksmethoden, constateerde tevens tekortkomingen in de toestemmings- en toezichtprocedure. Het Hof achtte het buitengewoon problematisch dat er geen enkele onafhankelijke (rechterlijke) controle bestaat.
Het wetsvoorstel computercriminaliteit wijkt op vrijwel al deze punten af van de wettelijke regelingen van de Russische Federatie en Hongarije. Het wetsvoorstel is van toepassing op de opsporing en vervolging van strafbare feiten, en niet op de bescherming van de staatsveiligheid. De gevallen waarin de bevoegdheid kan worden toegepast worden duidelijk in de wet vastgelegd. Dit betreft ernstige misdrijven waarvoor voorlopige hechtenis mogelijk is en die een ernstige inbreuk op de rechtsorde opleveren, waarbij voor bepaalde onderzoekshandelingen de extra drempel geldt dat het een misdrijf betreft waarvoor een gevangenisstraf van acht jaar of meer kan worden opgelegd dan wel een ernstig misdrijf dat bij algemene maatregel van bestuur is aangewezen. De voorgestelde bevoegdheid kan uitsluitend worden ingezet bij een verdenking dat een persoon betrokken is bij het beramen of plegen van een dergelijk strafbaar feit, waarbij het bevel de nodige gegevens dient te bevatten ter identificatie van de betrokken persoon en het geautomatiseerde werk. Het is dus bepaald niet zo dat de bevoegde autoriteiten volledig naar eigen inzicht kunnen besluiten tot de toepassing van deze bevoegdheid. De duur van de inzet is beperkt tot vier weken, met de mogelijkheid van verlenging. Verder geldt dat altijd een voorafgaande rechterlijke machtiging is vereist, dat de betrokkene wordt geïnformeerd over de toepassing van de bevoegdheid, en dat systeemtoezicht wordt uitgeoefend op de uitvoering van de wettelijke regels in praktijk.
Op grond van het voorgaande moet dan ook geconcludeerd worden dat de wettelijke regelingen voor het aftappen ten behoeve van de staatsveiligheid en de opsporing en vervolging van strafbare feiten in de Russische Federatie en Hongarije, die onderwerp vormde van het arrest van het EHRM, op essentiële punten afwijken van die rond de toepassing van bijzondere opsporingsbevoegdheden in Nederland, zoals de bevoegdheid het op afstand heimelijk binnendringen in een geautomatiseerd werk met het oog op het verrichten van bepaalde onderzoekshandelingen, zodat de arresten in de zaken Zakharov en Szabo geen consequenties hebben voor het onderhavige wetsvoorstel. Er is daarnaast overigens geen reden te veronderstellen dat dit wetsvoorstel niet zou voldoen aan de eisen van die daaraan op grond van het EVRM, specifiek ten aanzien van de «noodzakelijkheid» en «voorzienbaarheid», moeten worden gesteld.

De leden van de SP-fractie hebben gevraagd of de regering bereid is het wetsvoorstel in te trekken en zo nee, waarom niet.

De regering ziet geen reden het wetsvoorstel in te trekken, de regering is daarentegen van oordeel dat het wetsvoorstel voorziet in een dringende behoefte van de opsporings- en vervolgingsinstanties om cybercrime beter te kunnen bestrijden en de burgers tegen te kunnen beschermen tegen vormen van criminaliteit die worden gepleegd met behulp van geautomatiseerd werken.

De leden van de PvdD-fractie merkten op dat privacy en de bescherming van de persoonlijke levenssfeer een groot goed is en te allen tijde gewaarborgd met worden en meenden dat veiligheid voorop moet staan en een wet die het mogelijk maakt een pacemaker te hacken elke vorm van proportionaliteit mist.
Met de leden van de PvdD-fractie acht de regering de privacy en de bescherming van de persoonlijke levenssfeer een groot goed. Het recht op privacy is echter geen absoluut recht maar moet worden afgewogen tegen andere belangen, zoals de beveiliging van burgers tegen de misdaad of de bescherming van slachtoffers van strafbare feiten. Het wetsvoorstel biedt de mogelijkheid om op afstand heimelijk een geautomatiseerd werk binnen te dringen. De omschrijving van het begrip geautomatiseerd werk is in internationale verdragen en in de EU-wetgeving vastgelegd, de kern van dit begrip is dat in het apparaat op basis van een programma geautomatiseerd gegevens worden verwerkt. Ook een apparaat als een pacemaker kan in theorie onder de definitie van geautomatiseerd werk vallen. Het is echter niet goed voor te stellen op welke wijze het op afstand binnendringen in een pacemaker kan bijdragen aan de opheldering van misdrijven. 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.

De leden van de SP-fractie constateerden dat er een aantal uitspraken is van Europese rechters waarbij ingegaan wordt op de proportionaliteit van het verzamelen van gegevens en hebben gevraagd in welke mate onderhavig wetsvoorstel voldoet aan de randvoorwaarden zoals die in deze rechtszaken door de verschillende rechters zijn gesteld aan de proportionaliteit van de verzameling van gegevens en inzet van opsporingsbevoegdheden.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de PvdD-fractie over de aantasting van de privacy van Nederlanders in het licht van de recente Europese ontwikkelingen om het recht op privacy juist te beschermen.

De leden van de D66-fractie hebben gevraagd hoe de regering meent dat de burger kan vertrouwen op de integriteit van een computersysteem indien zij niet kan uitsluiten dat door het gebruik van technische kwetsbaarheden de achterdeur ook open komt te staan voor kwaadwillende derden die dezelfde achterdeur willen gebruiken.
Voor het antwoord op deze vraag verwijs ik naar de eerdere beantwoording van een soortgelijke vraag van de leden van de D66 fractie over hoe de politie voorkomt dat derden gebruik maken van dezelfde kwetsbaarheid als waar de politie gebruik van maakt bij het doen van onderzoek in het geautomatiseerde werk dat in gebruik is bij de verdachte (paragraaf 2.5).

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

De leden van de VVD-fractie hebben gevraagd hoe de bevoegdheden ten aanzien van het aftappen of opnemen van (vertrouwelijke) communicatie zich verhouden tot de bevoegdheden op dit gebied zoals opgenomen in de Wet op de inlichtingen- en veiligheidsdiensten. Zij hebben tevens gevraagd of de bijbehorende gronden en waarborgen overeen komen.

In het Wetboek van Strafvordering zijn de bevoegdheden op het gebied van het aftappen of opnemen van (vertrouwelijke communicatie) in twee artikelen vorm gegeven, te weten de artikelen 126l en 126m Sv. Op grond van artikel 126l Sv kan vertrouwelijke communicatie worden opgenomen met een technisch hulpmiddel, dit kan een kleine microfoon zijn die aan het zicht van buitenstaanders is onttrokken (een «bug») of een microfoon die een zeer groot bereik heeft (richtmicrofoon). Op grond van artikel 126m Sv kan communicatie worden afgetapt en opgenomen die plaatsvindt via een openbaar telecommunicatienetwerk of met gebruikmaking van een openbare telecommunicatiedienst. De voorwaarden voor toepassing zijn vrijwel gelijkluidend, te weten een misdrijf waarvoor voorlopige hechtenis mogelijk is en dat een ernstige inbreuk op de rechtsorde oplevert, een dringend onderzoeksbelang en een voorafgaande machtiging van de rechter-commissaris.

Op grond van de Wet op de inlichtingen en veiligheidsdiensten 2002 (Wiv 2002) zijn de diensten bevoegd tot het met een technisch hulpmiddel gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk, ongeacht waar een en ander plaatsvindt (art. 25 Wiv 2002). Voor de uitoefening van deze bevoegdheid is de toestemming van de Minister vereist. Ook zijn de diensten bevoegd tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabel gebonden telecommunicatie voor een periode van drie maanden (art. 27 Wiv 2002). Voor de interceptie als zodanig is thans geen toestemming van de Minister vereist. Aan de hand van bepaalde criteria kan vervolgens nadere selectie van de verzamelde gegevens plaatsvinden, waarvoor wel ministeriële toestemming is vereist, omdat de selectie is gericht op het kennisnemen van de inhoud van de communicatie. De toestemming daarvoor wordt vereend door de door de dienst verantwoordelijke Minister en wel voor een periode van ten hoogste drie maanden ingeval het gaat om een selectie aan de hand van namen of nummers en een periode van ten hoogste jaar als het gaat om een selectie op trefwoorden.

In het conceptvoorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten wordt voorgesteld de bestaande bevoegdheid ex artikel 27 Wiv 2002 te vervangen door een nieuwe bevoegdheid, te weten het onderzoeksopdrachtgerichte onderzoek van communicatie. Deze bevoegdheid ziet zowel op de interceptie (in bulk) van niet-kabel gebonden als kabel gebonden telecommunicatie. Een vergelijkbare bevoegdheid ontbreekt in de sfeer van de strafvordering.

Op basis van de voorgaande beschrijving kan worden vastgesteld dat de bevoegdheden op het gebied van het aftappen of opnemen van communicatie van de opsporingsdiensten enerzijds en van de inlichtingen- en veiligheidsdiensten anderzijds inhoudelijk verschillend zijn. De opsporingsdiensten zijn bevoegd tot het aftappen van telecommunicatie en het direct afluisteren van vertrouwelijke communicatie. Deze bevoegdheden zijn beperkt tot de gerichte interceptie, dat wil zeggen dat de interceptie is beperkt tot de communicatie van een specifieke persoon of van een bepaald nummer. De opsporingsdiensten zijn thans niet bevoegd tot de ongerichte interceptie van communicatie, ongeacht of die communicatie

al dan niet via de kabel verloopt. De voorwaarden voor de toepassing van deze bevoegdheden zijn eveneens verschillend. In de regeling van het Wetboek van Strafvordering vormt het vereiste van een voorafgaande rechterlijke machtiging een belangrijke voorwaarde, in de regeling van de Wiv 2002 alsmede in het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten betreft dit de voorafgaande instemming van de verantwoordelijke Minister. Daarnaast is het onderscheid in het toezicht op de toepassing van de wettelijke bevoegdheden van belang. Het toezicht op de toepassing van de opsporingsbevoegdheden, zowel vooraf als achteraf, wordt uitgeoefend door de rechterlijke macht. Tevens is voorzien in systeemtoezicht door de Inspectie VenJ. Op de toepassing van de uitvoering van de bevoegdheden van de Wiv 2002 door de inlichtingen- en veiligheidsdiensten vindt het toezicht op de rechtmatigheid van de uitvoering van de bevoegdheden plaats door de Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD), die jaarlijks verslag uitbrengt van haar werkzaamheden.

3. De ontoegankelijkmaking van gegevens

3.1 De noodzaak tot aanpassing van de huidige wettelijke regeling

De leden van de CDA-fractie hebben (nogmaals) gevraagd of met het schrappen van de dwangsom uit het conceptwetsvoorstel ten aanzien van internetproviders nog wel afdoende maatregelen over blijven om handhavend effectief te kunnen optreden.
Deze vraag kan ik bevestigend beantwoorden. Daarbij speelt de Notice and Take Down gedragscode (verder NTD-gedragscode) een belangrijke rol. Deze gedragscode is in het verband van de Nationale Infrastructuur Cybercrime op basis van vrijwilligheid opgesteld en ondertekend door een groot aantal internetproviders. In deze gedragscode is een procedure opgenomen die antwoord geeft op de vraag hoe internetproviders moeten omgaan met meldingen van onrechtmatige en strafbare informatie op het internet. Het voldoen aan de NTD-gedragscode is vrijwillig en kan niet worden afgedwongen. Doordat de NTD-gedragscode door de marktpartijen zelf is opgesteld, is de acceptatie ervan zeer goed te noemen. In de dagelijkse praktijk functioneert de NTD-gedragscode zonder meer goed. Desgevraagd heeft de Landelijk officier van justitie voor Cybercrime & Interceptie gemeld dat een internetprovider vrijwel altijd meewerkt op het moment dat hij erop gewezen wordt dat strafbaar materiaal is geplaatst op de door hem aangeboden dienst. Af en toe vergt een attendering nadere toelichting over de aard van het strafbare materiaal. In een dergelijk geval overlegt het openbaar ministerie met de betreffende provider en het resultaat is tot nu toe steeds geweest dat na een dergelijk overleg het betreffende materiaal op de kortst mogelijke termijn is verwijderd. De Landelijk coördinerend officier van justitie kinderporno heeft gemeld dat de samenwerking met de internetproviders meer dan goed is. In het geval dat de internetprovider wordt gewaarschuwd dat er strafbaar materiaal via zijn dienst wordt gepubliceerd, wordt zonder uitzondering deze strafbare content binnen de kortst mogelijke tijd ontoegankelijk gemaakt.
In de gevallen waarin een aanbieder geen opvolging geeft aan de vrijwillige NTD-gedragscode of niet bij deze code is aangesloten kan de officier van justitie een bevel afgeven tot het ontoegankelijk maken van gegevens. Zoals hierboven in antwoord op een soortgelijke vraag van de leden van de CDA-fractie reeds aan de orde is gekomen, kan in een dergelijk geval strafvervolging worden ingesteld vanwege het niet opvolgen van een bevoegd gegeven ambtelijk bevel (art. 184 Sr.) dan wel het deelnemen aan of medeplegen van het gronddelict. Mede gelet op de ervaringen tot nu toe acht ik de beschikbare maatregelen voldoende om een effectieve handhaving te kunnen waarborgen.

De leden van de CDA-fractie hebben gevraagd of het thans in de praktijk voorkomt dat de aanbieder van een communicatiedienst niet bereid is op basis van de geldende NTD-gedragscode gegevens ontoegankelijk te maken. De leden van deze fractie hebben tevens gevraagd hoe daartegen kan worden opgetreden tot het moment dat onderhavig wetsvoorstel in werking treedt.
Voor het antwoord op de vraag over hoe de NTD-gedragscode in de praktijk functioneert verwijs ik naar de beantwoording van de bovenstaande vraag van de leden van deze fractie.
In het Algemeen Overleg van 13 april 2016 over de bestrijding van kinderpornografie is aan de orde geweest dat er problemen zijn met een provider die zich naar de mening van het Meldpunt Kinderpornografie op het Internet niet houdt aan de code (Kamerstukken II 2015/16, 31 015, nr. 126). Toegezegd is aan de Tweede Kamer om dit najaar het College van procureurs-generaal te vragen naar de werking van de «Notice and Take Downprocedure», waarbij veel providers sinds 2009 op basis van vrijwilligheid kinderporno-materiaal van hun server (laten) verwijderen, en het daarmee verband houdende project Nederland Schoon van politie en openbaar ministerie. Over de uitkomsten van dit gesprek en een eventueel vervolg zal ik berichten in de eerstvolgende voortgangsrapportage kinderporno die de Minister van Veiligheid en Justitie voor het kerstreces 2016 aan uw Kamer zal doen toekomen.

De leden van de CDA-fractie hebben gevraagd hoe onderhavig wetsvoorstel rekening houdt met strafbare uitingsdelicten als opruiing, het haat zaaien en belediging.
Naar aanleiding van het advies van het College van procureurs-generaal over het conceptwetsvoorstel is de bevoegdheid van de officier van justitie tot het geven van een bevel tot het ontoegankelijk maken van gegevens beperkt tot strafbare feiten waarvoor voorlopige hechtenis mogelijk is. Omdat deze bevoegdheid zal worden ingezet in gevallen waarin de vrijheid van meningsuiting vaak een rol speelt, dreigt het risico dat het openbaar ministerie in de rol van een censurerende internetpolitie wordt gedrongen. Het delict van opruiing is strafbaar gesteld met een gevangenisstraf van ten hoogste vijf jaar (art. 131, eerste lid, Sr) zodat voor dit delict een bevel tot ontoegankelijkmaking kan worden gegeven. Het aanzetten tot haat is strafbaar gesteld met een gevangenisstraf van ten hoogste een jaar (art. 137d, eerste lid, Sr). Voor dit delict kan geen bevel tot het ontoegankelijk maken van gegevens worden gegeven. Wanneer het feit wordt gepleegd door een persoon die daarvan een beroep of gewoonte maakt of door twee of meer verenigde personen (art. 137d, tweede lid, Sr) is voorlopige hechtenis toegelaten (art. 67, eerste lid, onder b, Sv). Ditzelfde geldt voor de belediging van een groep mensen (art. 137c, eerste lid, Sr). Als dit feit wordt gepleegd door een persoon die daarvan een beroep of gewoonte maakt of door twee of meer verenigde personen dan kan een bevel tot het ontoegankelijk maken van gegevens worden gegeven, omdat het misdrijf van artikel 137c, tweede lid, Sr een misdrijf is waarvoor voorlopige hechtenis is toegelaten (art. 67, eerste lid, onder b, Sv).

3.2 De uitvoering van een bevel tot ontoegankelijkmaking van gegevens

De leden van de SP-fractie hebben gevraagd of het correct is dat degene van wie de gegevens ontoegankelijk worden gemaakt kan klagen bij de rechtbank, en wat de situatie is als de eigenaar van de gegevens niet bekend is of onvindbaar.

Voorgesteld wordt dat de belanghebbenden zich bij de rechtbank kunnen beklagen over een bevel tot het ontoegankelijk maken van gegevens. Daartoe wordt voorgesteld artikel 552a Sv te wijzigen (Artikel II, onderdeel

X). Dit kan ook de persoon betreffen van wie de gegevens ontoegankelijk worden gemaakt. Tevens geldt een verplichting tot notificatie van de betrokkene, zodat deze op de hoogte kan komen van de ontoegankelijkmaking van de gegevens. Dit is geregeld in het bestaande artikel 125m Sv. Deze mededeling blijft echter achterwege indien uitreiking redelijkerwijs niet mogelijk is. Als de eigenaar van de gegevens niet bekend is of onvindbaar dan zal er geen notificatie kunnen plaatsvinden. Zodra de betrokkene langs andere weg op de hoogte is gekomen van de ontoegankelijkmaking van de gegevens kan hij zich op grond van het voorgestelde artikel 552a, eerste lid, Sv eveneens schriftelijk beklagen over de ontoegankelijkmaking.

4. Het wederrechtelijk overnemen en «helen» van gegevens

4.1 De voorgestelde strafbaarstellingen

De leden van de SP-fractie constateerden dat het strafbaar wordt om niet-openbare gegevens wederrechtelijk over te nemen en hebben gevraagd of dat wel proportioneel is. Ook hebben zij gevraagd wanneer sprake is van een algemeen belang, en of dat alleen is wanneer er ophef over ontstaat in de media. Voorts hebben zij gevraagd hoe wordt getoetst of iemand te goeder trouw handelde of niet.
Met het overnemen van niet-openbare gegevens kan ernstig inbreuk worden gemaakt op de belangen van de slachtoffers. Hiervoor kan worden gedacht aan misbruik van creditcards, waarvan de gegevens zijn verkregen door middel van «phishing». Hiermee wordt gedoeld op het opzetten van een valse website waardoor het slachtoffer wordt verleid tot afgifte van zijn creditcard gegevens. Ook kan worden gedacht aan vormen van «wraakporno», waarbij afbeeldingen van personen in een oneerbare pose worden ontvreemd en op internet gepubliceerd. De inbreuk op de belangen is tevens ingrijpend omdat het in de praktijk buitengewoon moeilijk kan zijn om gegevens, die eenmaal op het internet zijn geopenbaard, definitief en volledig te verwijderen. Gelet op de risico's voor de slachtoffers valt dan ook niet goed in te zien dat de voorgestelde strafbaarstelling niet proportioneel zou zijn. Met de term algemeen belang wordt volgens het spraakgebruik geduid op datgene dat voor de samenleving als geheel van betekenis is en het belang van een individu of van een groep van personen overstijgt. Het is aan de rechter om te beoordelen in een concreet geval sprake is van een algemeen belang, als bedoeld in de voorgestelde bepaling. Het rechterlijk oordeel komt in volledige onafhankelijkheid tot stand, en is niet afhankelijk van ophef in de media. Of iemand te goeder trouw handelde wordt eveneens getoetst wanneer de rechter in een concreet geval oordeelt over de strafbaarheid van de gedraging van de vervolgde persoon.

De leden van de SP-fractie hebben opgemerkt dat klokkenluiders en journalisten bepaalde informatie niet zullen durven delen omdat het nog maar de vraag is of zij voldoen aan de eis dat sprake moet zijn van een algemeen belang en bovendien te goeder trouw zijn en ontvingen graag een reactie op deze zorgen.
In de memorie van toelichting is aangegeven dat het wetsvoorstel niet beoogt te voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders, of van degenen die hen daarbij faciliteren (blz. 66). Het recht op een vrije nieuwsgaring kan worden aangemerkt al een algemeen belang. Ditzelfde geldt voor het recht op de vrijheid van meningsuiting, dat ook grondwettelijk verankerd is (art. 7 GW). Of journalisten en klokkenluiders in een concreet geval een beroep kunnen doen op omstandigheden als het algemeen belang of de goede trouw is aan de rechter om te beoordelen. Met de voorgestelde strafuitsluitingsgrond wordt beoogd expliciet in de wet een uitzondering op te

nemen voor de door artikel 10 van het EVRM beschermde vrijheid van meningsuiting. De Hoge Raad heeft geoordeeld dat uit de rechtspraak van her EHRM volgt dat journalisten in beginsel niet op basis van hun door artikel 10 EVRM gegeven bescherming kunnen worden ontslagen van hun verplichting de door de strafwet getrokken grenzen in acht te nemen. Het door artikel 10 EVRM gewaarborgde recht op vrijheid van meningsuiting kan echter dwingen tot het maken van een uitzondering op dit uitgangspunt. Bij de beantwoording van de vraag of de strafvervolging en veroordeling wegens een in het kader van een journalistiek onderzoek gepleegd strafbaar feit een noodzakelijke inbreuk op de journalistieke vrijheid van meningsuiting wordt gemaakt, moeten de plichten en verantwoordelijkheden van degene die met een beroep op zijn vrijheid van meningsuiting dat feit pleegde worden meegenomen. Hierbij is een afweging van belangen aan de orde, dit betreft de afweging van in het bijzonder de ernst van de inbreuk op de rechtsorde door de normschending, gelet op het belang van het geschonden voorschrift, tegen het maatschappelijk belang van de door de fraude voorbereide openbaarmaking, het daadwerkelijke nadeel dat door het bewezenverklaarde feit is ontstaan en de mate waarin de openbaarmaking daadwerkelijk op andere wijze had kunnen worden voorbereid (HR 26 maart 2013, LJN BY3752). Ook kan worden gewezen op een uitspraak van de rechtbank Oost-Brabant, waarin de verdachte door middel van computervredebreuk was binnengedrongen in een server van een website en vervolgens de medische dossiers had bekeken, ook in aanwezigheid van journalisten. De verdachte vond dat de beveiliging van deze gegevens tekort schoot en beriep zich op de absolute maatschappelijke noodzaak om deze misstand zeer snel aan de kaak te stellen. De rechtbank overwoog dat computervredebreuk strafbaar is tenzij er onder zeer bijzondere omstandigheden hogere belangen zijn die een dergelijke inbreuk in volle omvang kunnen rechtvaardigen. Bij de beoordeling of sprake is van dergelijke omstandigheden waren naar het oordeel van de rechtbank mede gelet op het bepaalde in artikel 10 EVRM drie factoren van belang, namelijk (1) of de verdachte heeft gehandeld in het kader van een wezenlijk maatschappelijk belang, (2) of het handelen proportioneel was en (3) of er geen andere, minder vergaande, manier is om het beoogde doel te kunnen bereiken. De rechtbank was van oordeel dat het aantonen van gebreken bij de bescherming van vertrouwelijke medische gegevens een wezenlijk maatschappelijk belang kan dienen (ECLI:NL:RBOBR:2013:BZ1157).

De leden van de D66-fractie hebben instemmend kennis genomen van het uitgangspunt dat dit wetsvoorstel niet mag voorzien in de strafbaarstelling van gerechtvaardigde activiteiten van journalisten en klokkenluiders of van degenen die hen daarbij faciliteren en hebben gevraagd of de regering een nadere toelichting kan geven op hetgeen op grond van jurisprudentie en naar haar opvatting als medewetgever wordt verstaan onder algemeen belang.
Bij de voorgestelde strafbaarstelling van de heling van gegevens zijn conflicterende belangen aan de orde. Enerzijds het belang van de rechthebbende op strafrechtelijke bescherming tegen het onbevoegde gebruik van gegevens door derden, welke gegevens door misdrijf zijn verkregen. Anderzijds het maatschappelijke belang dat misstanden vrijelijk kunnen worden geopenbaard door journalisten of klokkenluiders zonder dat het risico bestaat op strafvervolging vanwege de voorgestelde strafbaarstelling van de heling van gegevens. Bescherming van de vrijheid van meningsuiting zoals vastgelegd in artikel 10 EVRM is hierbij van belang, evenals het belang dat een democratische samenleving heeft bij de wetenschap van de openbaar gemaakte gegevens. Met de term «algemeen belang» wordt gedoeld op een maatschappelijk belang, dat het belang van een individu overstijgt. Hiervoor valt bijvoorbeeld te

denken aan de bekendmaking van gegevens ter voorkoming of beëindiging van een ernstige calamiteit, zoals een ramp, of een misstand. Als hoofdregel geldt hierbij dat sprake moet zijn van een «serieuze» misstand, terwijl de wijze van melden in verhouding behoort te staan tot de ernst van de misstand. Het is aan de rechter om in een concrete strafzaak, op basis van een afweging van belangen, te beoordelen in hoeverre het algemeen belang de strafbaar te stellen handelingen rond gegevens vereiste. Illustratief hiervoor is de jurisprudentie die eerder, naar aanleiding van vragen van de leden van de SP-fractie, aan de orde is geweest. Op grond van die jurisprudentie is een afweging van belangen aan de orde, namelijk de afweging van de ernst van de inbreuk op de rechtsorde door het handelen van de verdachte en het nadeel dat hierdoor is ontstaan tegen het maatschappelijk belang dat wordt gediend met openbaarmaking van de gegevens. Bij het handelen moeten de grenzen van de proportionaliteit en subsidiariteit in acht worden genomen, dat wil zeggen dat niet verder is gegaan dan noodzakelijk om het doel (verbetering van de beveiliging van medische gegevens) te bereiken en dat er geen andere, minder vergaande, manieren waren om dit doel te bereiken. Het binnendringen in een geautomatiseerd werk, het raadplegen van medische dossiers, en het uitprinten van gegevens zijn door de rechter niet wederrechtelijk geoordeeld in het licht van het hogere belang dat daarmee gediend was, namelijk het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens. De rechter oordeelde dat deze handelwijze een wezenlijk maatschappelijk belang kon dienen.

De leden van de D66-fractie hebben de regering gevraagd nader toe te lichten wat er gebeurt als gegevens van het internet worden gebruikt die niet alleen niet openbaar zijn maar ook onvoldoende beveiligd, waardoor als niet-openbaar betitelde informatie feitelijk wel toegankelijk is en door derden wordt gebruikt.
Voor het antwoord op de vraag of informatie openbaar is dient gewicht te worden toegekend aan de wil van degene die de beschikkingsmacht heeft over die informatie. Als deze de gegevens op zodanige wijze heeft opgeslagen dat daaruit kan blijken dat de rechthebbende niet de intentie had de gegevens voor het publiek beschikbaar te stellen, dan is deze informatie niet openbaar. Dat de informatie niet of niet voldoende is beveiligd tegen de intenties van kwaadwillenden doet daaraan niet af. Een voorbeeld betreft een afbeelding die is opgeslagen op een mailserver in de cloud. Als een derde beschikking krijgt over die gegevens door zich toegang te verschaffen tot de mailbox, dan verandert daardoor niet het karakter van de betreffende afbeelding. Uit het feit dat die afbeelding is opgeslagen in een mailbox die niet voor anderen dan de rechthebbende(n) op de betreffende mailbox toegankelijk is, volgt dat het hier gaat om gegevens die niet voor het publiek beschikbaar en daarmee niet openbaar zijn.

De leden van de D66-fractie hebben gevraagd of de regering een onderscheid maakt in het soort gegevens dat uit een geautomatiseerd werk van een ander zijn ontvreemd, bekend gemaakt aan een ander, verkocht of op internet geplaatst. Zij hebben tevens gevraagd of de niet-openbaarheid als uitsluitend criterium geldt.
De regering maakt geen onderscheid in het soort gegevens dat uit een geautomatiseerd werk wordt ontvreemd. De strafbaarstelling is evenmin beperkt tot elektronische gegevens, deze is van toepassing op alle gegevens, inclusief niet-elektronische gegevens. In dit laatste geval zal er doorgaans sprake zijn van het verlies van de beschikkingsmacht van de rechthebbende, zodat dan diefstal of verduistering aan de orde is. De regering is geen voorstander van nadere beperking. In de eerste plaats acht de regering het onwenselijk om bij voorbaat de reikwijdte van de

voorgestelde strafbepaling te beperken tot bepaalde gegevens, terwijl aan het wederrechtelijk verkrijgen en via het internet breed verspreiden van gegevens van anderen in zijn algemeenheid grote risico's kunnen zijn verbonden voor de slachtoffers. Daarnaast is het gecompliceerd om een criterium vast te stellen dat enerzijds voldoende onderscheidend vermogen heeft en anderzijds niet leidt tot ongewenste gevolgen voor de strafbaar stelling. Dit alles overziend geeft de regering er de voorkeur aan geen onderscheid te maken in de aard van de gegevens. In het (hypothetisch) geval waarin dit onderscheid redengevend zou kunnen zijn voor de strafbaarheid van de gedraging, kan de rechter in een concrete strafzaak daarmee rekening houden bij het oordeel over de strafbaarheid van de gedraging en de hoogte van de op te leggen straf. Tenslotte geldt de niet-openbaarheid inderdaad als uitsluitend criterium, dat wil zeggen dat als de gegevens voor het publiek beschikbaar zijn er geen sprake kan zijn van een strafbare gedraging wanneer iemand die gegevens voorhanden heeft of aan anderen bekend maakt. Hierbij moet wel worden opgemerkt dat, zoals in eerdere vragen van deze fractie aan de orde is gekomen, de intentie of de wil van de rechthebbende van belang is bij de beoordeling van de vraag of gegevens voor het publiek beschikbaar zijn.

De leden van de ChristenUnie-fractie hebben geconstateerd dat het wetsvoorstel heling van computergegevens strafbaar maakt en hebben gevraagd waarom de regering niet heeft gekozen voor een nadere differentiatie op grond van de aard van de betreffende gegevens.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van de bovenstaande, soortgelijke vraag van de leden van de D66-fractie.

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

De leden van de VVD-fractie hebben opgemerkt dat bij inzet van lokpubers gebruik gemaakt kan worden van profielfoto's en vragen nader toe lichten aan welke voorwaarden het gebruik van zo'n foto dient te voldoen, bijvoorbeeld ten aanzien van de herkomst van de foto.
De opsporingsambtenaar die fungeert als lokpuber zal zich, om het verwijt van uitlokking te voorkomen, passief opstellen en afwachten totdat iemand contact met hem legt via internet. Het profiel dat door de opsporingsambtenaar die als lokpuber fungeert aangemaakt wordt, zal een profiel zijn dat niet opvalt tussen andere profielen van deelnemers aan het sociale medium waarop de opsporingsambtenaar zich begeeft. Gelet op het feit dat de deelnemers vaak jonge kinderen zijn, kan bijvoorbeeld gedacht worden aan een foto van een dier of een plaatje van een stripfiguur.

De leden van de VVD-fractie hebben gevraagd wat er tegenover burgerinitiatieven om pedofielen op te sporen staat.
Tegenover burgerinitiatieven om pedofielen op te sporen staan opsporing en vervolging door de daartoe bevoegde instanties, de politie en het openbaar ministerie. Het terugdringen van kinderpornografie en kindersekstoerisme maakt deel uit van de Veiligheidsagenda 2015–2018 en heeft hoge prioriteit. De prestaties van politie en openbaar ministerie in de aanpak van kinderporno en kindersekstoerisme op dit gebied zijn de afgelopen jaren substantieel verbeterd en waren in 2015 zelfs boven verwachting (Kamerstukken II 2015/16, 31 015, nr.121).

De leden van de PvdA-fractie of er omstandigheden zijn waarin de opsporingsambtenaar wel zelf contact legt en hoe dit zich verhoudt tot het Tallon-criterium.

Opsporingsambtenaren dienen zich met inachtneming van het Tallon-criterium zodanig op te stellen dat de verdachte niet wordt gebracht tot andere handelingen dan waarop zijn opzet van tevoren was gericht. Om te voorkomen dat sprake is van uitlokking zal de opsporingsambtenaar die als lokpuber fungeert zich daarom passief opstellen en wachten tot iemand contact legt.

De leden van de PvdA-fractie hebben gevraagd naar de uitkomsten van het WODC-onderzoek naar de normstelling en samenhang van de zedentitel in het Wetboek van Strafrecht en wanneer de Kamer dit onderzoek voorzien van een beleidsreactie tegemoet kan worden gezien. Bij brief van 29 februari 2016 (Kamerstukken II 2015/16, 29 279, nr. 300) is het onderzoek «Herziening van de zedendelicten?» dat is uitgevoerd door de Rijksuniversiteit Groningen in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), voorzien van een beleidsreactie naar Uw Kamer gestuurd. Het WODC-onderzoek bevestigt dat de strafrechtelijke bescherming die de zedenwetgeving biedt tegen seksueel onwenselijk gedrag uit juridisch oogpunt in beginsel toereikend en in overeenstemming met de internationale wet- en regelgeving is. Tegelijkertijd toont het onderzoek aan dat de zedenwetgeving op onderdelen kan worden verduidelijkt en vereenvoudigd. Daarom wordt een wetgevingstraject gestart met als doel modernisering van de zedentitel. Om aan de in de WODC-onderzoek geconstateerde bezwaren tegemoet te komen wordt de huidige zedentitel geherstructureerd en vereenvoudigd. Het onderzoek bevat hiertoe waardevolle suggesties. Daarnaast wordt de zedenwetgeving inhoudelijk gemoderniseerd. De strafrechtelijke bescherming tegen digitale ontucht wordt verruimd. Bezien wordt in hoeverre de bescherming tegen lichamelijke ontucht verruiming behoeft. Naar verwachting wordt in het najaar van 2016 een wetsvoorstel tot modernisering van de zedenwetgeving in consultatie gebracht.

De leden van de SP-fractie hebben gevraagd of zij het goed begrijpen als zij stellen dat grooming straks ook strafbaar is als sprake is van uitlokking door een opsporingsambtenaar die geen minderjarige is. Tevens hebben deze leden erop gewezen dat volgens de regering er in de praktijk geen sprake zal zijn van uitlokking, omdat de opsporingsambtenaar in beginsel niet zelf de communicatie zal starten. Zij hebben gevraagd wat «in beginsel» in deze contact betekent, en hoe wordt voorkomen dat grooming niet bewezen kan worden omdat sprake is van uitlokking.
De leden van de SP-fractie hebben goed begrepen dat grooming straks ook strafbaar is als sprake is van uitlokking door een opsporings-ambtenaar die geen minderjarige is en die zich voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt. Met de woorden «in beginsel» wordt bedoeld dat het niet bij voorbaat is uitgesloten dat het de opsporingsambtenaar is die de communicatie start; de opsporings-ambtenaar zal een profiel moeten aanmaken zodat de groomer in staat is contact te leggen. In het licht van het eerdergenoemde Tallon-criterium zal de opsporingsambtenaar zich zodanig opstellen dat de verdachte niet wordt gebracht tot andere handelingen dan waarop zijn opzet van tevoren was gericht.

De leden van de SP-fractie hebben gevraagd of het niet verstandig is om alsnog in de wet vast te leggen wanneer een lokpuber mag worden ingezet.
Bij de huidige stand van de jurisprudentie wordt geen aanleiding gezien voor een nadere regeling over de inzet van de lokpuber. Die inzet vindt een toereikende grondslag in de algemene taakstellende bepalingen van opsporingsambtenaren, zoals die in de rechtspraak is genormeerd. Wel zal, zoals ook in de contourennota modernisering Wetboek van Strafvor-

dering tot uitdrukking is gebracht (Kamerstukken II 2015/16, 29 279, nr. 278, blz. 54) in het kader van de voorgenomen modernisering van het Wetboek van Strafvordering worden bezien of het Tallon-criterium als algemene bepaling voor het voorbereidend onderzoek in het wetboek kan worden gecodificeerd.

De leden van de SP-fractie hebben gevraagd in hoeverre sprake kan zijn van een strafbaar feit als de verdachte zelf minderjarig is en het slachtoffer bijvoorbeeld tien jaar oud is.
De strafbepaling stelt geen eisen aan de leeftijd van de dader. Ook minderjarige daders kunnen zich schuldig maken aan grooming. Voor een veroordeling voor grooming is nodig dat alle delictsbestanddelen bewezen kunnen worden. In de strafbepaling (art. 248e Sr) is een ontuchtbestanddeel opgenomen. Er moet sprake zijn van een oogmerk om ontuchtige handelingen te plegen. Dat betekent dat er sprake moet zijn van het oogmerk om gedragingen te plegen die in strijd zijn met de sociaal-ethische norm. In het gegeven voorbeeld, een kind van zestien benadert een kind van tien, zal dit aan de orde kunnen zijn. Als het gaat om vrijwillige contacten tussen leeftijdsgenoten, bijvoorbeeld twee vijftienjarigen, dan kan dit van invloed zijn op het ontuchtkarakter van de handeling. Indien er geen sprake is van handelingen met een strafbaar karakter blijft vervolging achterwege.

De leden van de CDA-fractie hebben gevraagd of met dit wetsvoorstel de toezegging gestand wordt gedaan om sexting wettelijk te bestrijden (Kamerstukken II 2014/15, 28 684, nr. 443).
In de brief van 12 juni 2015 aan Uw Kamer, waarnaar de leden van de CDA-fractie in hun vraagstelling verwijzen, is toegezegd dat in het wetsvoorstel Computercriminaliteit III nieuwe strafbaarstellingen geïntroduceerd zouden worden op grond waarvan het strafbaar wordt om vertrouwelijke gegevens van personen, zoals seksueel getint beeldmateriaal, te kopiëren of gegevens die door misdrijf zijn verkregen voorhanden te hebben of bekend te maken. Deze strafbaarstellingen zijn in het wetsvoorstel opgenomen, dit betreft de voorgestelde de artikelen 138c en 139g Sr (Artikel I, onderdelen C en E). Hiermee wordt een lacune in de huidige strafrechtelijke wetgeving gedicht.

Ten aanzien van het Verdrag van Lanzarote inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik hebben de leden van de CDA-fractie gevraagd of Nederland als EU-voorzitter voor zichzelf geen rol ziet weggelegd om juist nu andere lidstaten te bewegen om grooming ook op nationaal niveau strafbaar te stellen.
Het comité van verdragsluitende partijen bij het Verdrag van Lanzarote inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik heeft dit onderwerp besproken. De Nederlandse vertegenwoordiger heeft daarbij de Nederlandse rechterlijke uitspraken over grooming uitgebreid toegelicht. Verschillende andere landen bleken de in Nederland ervaren problemen met de objectieve leeftijd in het groomingsartikel niet te herkennen. Het comité heeft niet geconcludeerd dat er een probleem is met de implementatie van het artikel 23 van het verdrag.

De leden van de ChristenUnie-fractie hebben gevraagd of de regering nader kan onderbouwen waarom zij de inzet van een «lokpuber» bij grooming een gerechtvaardigd middel acht. De leden van deze fractie hebben tevens gevraagd of de regering kan aangeven op welke plekken in het Wetboek van Strafrecht een dergelijke uitlokking reeds mogelijk is.
De regering acht de inzet van de lokpuber, een vorm van preventieve opsporing, gerechtvaardigd ter voorkoming van schadelijke contacten van volwassenen met kinderen. De inzet vindt een toereikende grondslag in de

algemene taakstellende bepalingen van opsporingsambtenaren, zoals die in de rechtspraak is genormeerd.

De leden van de GroenLinks-fractie hebben gevraagd of de regering kan uiteenzetten hoe uitlokking in de praktijk voorkomen wordt.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van soortgelijke vragen van de leden van de fracties van de PvdA en de SP.

De leden van de GroenLinks-fractie hebben opgemerkt dat voor een begin van uitvoering voldoende wordt geacht dat de verdachte een voorstel voor een ontmoeting doet. Tussen het moment van het voorstellen voor een ontmoeting en de ontmoeting zélf zou verdachte op eigen initiatief kunnen afzien van die geplande ontmoeting. Deze leden hebben gevraagd of voor de strafbaarheid van grooming niet moet worden vereist dat de verdachte daadwerkelijk daad bij woord voegt.
Onder invloed van internationale regelgeving is de strafrechtelijke bescherming van kinderen uitgebreid tot de voorfase van fysiek misbruik. De strafbaarstelling van grooming, het benaderen van kinderen voor seksuele doeleinden, is een gevolg van het Verdrag van Lanzarote. Nederland is partij bij dit Verdrag en is dus verplicht om grooming strafbaar te stellen. Op grond van het Verdrag dient de dader enige handeling te verrichten gericht op het verwezenlijken van een ontmoeting met een minderjarige. Het Verdrag vereist niet dat daadwerkelijk een ontmoeting heeft plaatsgevonden. Het stellen van een dergelijke eis zou strijdig zijn met het doel van dit verdrag, namelijk het beschermen van kinderen tegen seksuele exploitatie.

De leden van de GroenLinks-fractie hebben gevraagd wat in de brief van het wetenschappelijk bureau van het Openbaar Ministerie van 13 april 2015 wordt bedoeld met de opmerking dat opsporing en grooming door het niet inzetten van lokpubers vrijwel onmogelijk is geworden. Deze leden hebben tevens gevraagd of er mogelijkheden bestaan tot opsporing van grooming en in hoeverre deze opsporingsmogelijkheden alternatieven bieden voor de lokpuber.
Door het stopzetten van de inzet van de lokpuber is de preventieve opsporing van grooming feitelijk onmogelijk geworden. Opsporing achteraf kan nog steeds plaatsvinden, op basis van meldingen of aangifte. Dit is echter geen aanvaardbaar alternatief voor de preventieve inzet van de lokpuber omdat het schadelijke contact met een minderjarige dan vaak al heeft plaatsgevonden, met alle gevolgen van dien.

6. De online handelsfraude

De leden van de SP-fractie zijn verheugd te lezen dat online handelsfraude specifiek strafbaar wordt gesteld. De leden van deze fractie hebben opgemerkt dat men zich bij herhaling schuldig moet maken aan het verkopen of aanbieden zonder te leveren en hebben gevraagd wat bij herhaling is. De leden van deze fractie hebben voorts weinig gelezen over de rol van online advertentiesites, zoals Marktplaats en eBay, en hebben gevraagd wat hun rol is bij de aanpak van online handelsfraude. Tenslotte hebben zij gevraagd hoe samenwerking tussen overheid, opsporingsinstanties en deze private partijen plaatsvindt.
Zowel bij de politie als bij de online handelsplaatsen leeft de wens om online handels fraude centraal aan te pakken. Aanleiding is de toenemende (private) handel via de online handelsplaatsen en bijkomende vormen van fraude; meer in het bijzonder het strafbaar niet-nakomen van leverings- of betalingsverplichtingen (oplichting in de zin van artikel 326 Sr.). Sinds 2005 heeft een aantal online handelsplaatsen actief samenwerking gezocht met de politie en het openbaar ministerie om samen te

werken bij de aanpak van fraude. Met name Marktplaats heeft sindsdien uitgebreid geïnvesteerd om een gezamenlijke aanpak mogelijk te maken. Voor een effectieve aanpak van deze vorm van criminaliteit werd samenwerking tussen opsporingsinstanties, de private online handelsplaatsen en een landelijke coördinatie op aangiftes en meldingen noodzakelijk geacht. Dat heeft ertoe geleid dat politie en openbaar ministerie in nauwe samenwerking met Marktplaats in 2010 het Landelijk Meldpunt Internet Oplichting (LMIO) hebben opgericht met als doel het verbeteren van de aanpak van internet gerelateerde fraude op online handelsplaatsen, sociale media en via valse websites. Het LMIO is thans ondergebracht in het Landelijk Service Centrum e-Crime.
De samenwerkingsafspraken tussen Marktplaats, politie en openbaar ministerie zijn neergelegd in een convenant. Deze afspraken hebben niet alleen betrekking op snelle gegevensuitwisseling in gevallen van online handelsfraude, maar ook op het treffen van preventieve maatregelen en het geven van adequate voorlichting. Mede ter uitvoering van het convenant doet Marktplaats het nodige om te voorkomen dat bezoekers van de site slachtoffer worden van online handelsfraude. Marktplaats geeft voorlichting en adviezen over de wijze waarop de gebruikers zelf veilig kunnen handelen. Zo heeft Marktplaats een uitgebreide checklist online staan die men kan doorlopen alvorens een transactie aan te gaan. Daarnaast neemt Marktplaats maatregelen zoals het verwijderen van advertenties, het blokkeren van accounts, het versturen van waarschuwingsmails en het proactief melden bij politie of andere opsporingsinstanties. Marktplaats ontvangt ook informatie over alle aangiften die bij het LMIO worden gedaan over fraude via hun site om zo gerichte maatregelen te kunnen nemen.
In 2014 is een convenant gesloten tussen Marktplaats, LMIO, de Nederlandse Vereniging van Banken, de vier grootbanken en het openbaar ministerie. In dit convenant zijn eveneens afspraken neergelegd over preventieve maatregelen, adequate voorlichting en snelle gegevensuitwisseling in gevallen van fraude. Indien hetzelfde bankrekeningnummer in meerdere aangiftes wordt genoemd, stuurt het LMIO geautomatiseerd een bericht aan de betreffende bank. Deze melding is voor de bank aanleiding om maatregelen te nemen. Deze kunnen bestaan uit het aanspreken van de cliënt, het blokkeren van diens rekening en het beëindigen van de bankrelatie.

De leden van de CDA-fractie hebben gevraagd of de voorgestelde regeling alle grenzen in de huidige rechtspraktijk wegneemt om online handelsfraude te bestrijden.
Op dit moment zijn de strafrechtelijke mogelijkheden om op te treden tegen verkopers die zich schuldig maken aan het aanbieden of leveren van goederen of diensten beperkt. Vervolging wegens oplichting (art. 326 Sr) is mogelijk als sprake is van het aannemen van een valse naam of hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels. De enkele omstandigheid dat een verdachte goederen aanbiedt via een website en deze goederen vervolgens niet levert is onvoldoende voor het aannemen van een valse hoedanigheid. Hiervoor zijn bijkomende omstandigheden, zoals het opzettelijk hanteren van foute contactgegevens vereist.
Het wetsvoorstel breidt de strafrechtelijke mogelijkheden om op te treden tegen malafide verkopers uit. Het bij herhaling aanbieden van goederen of diensten zonder de intentie om deze daadwerkelijk te leveren wordt strafbaar. Hierdoor wordt het voor politie en openbaar ministerie mogelijk om strafvorderlijke bevoegdheden in te zetten bij verdenking van grootschalige handelsfraude.

De leden van de D66-fractie hebben gelezen dat vanwege de schaarse capaciteit prioriteiten gesteld moeten worden en dat niet bij ieder geval

van internetfraude over kan worden gegaan tot opsporing en vervolging, en hebben gevraagd hoe die keuze wordt gemaakt. Tegen de achtergrond van het zeer ingrijpende voorliggende wetsvoorstel hebben de leden van deze fractie tevens gevraagd hoe deze voetnoot bij opsporing en vervolging van internetfraude zich verhoudt tot de verwachtingen die de Wet computercriminaliteit III, en vooral de ronkende persberichten van de regering hierover, bij mensen zijn gewekt. Zij hebben tenslotte gevraagd wat wel mag en kan worden verwacht bij de aanpak van internetfraude.
De bestrijding van fraude waarvan burgers en bedrijven het slachtoffer worden, de zogenaamde horizontale fraude, is een prioriteit van dit kabinet. Internet gerelateerde fraude, waaronder onlinehandelsfraude, is één van de verschijningsvormen van horizontale fraude. De bestrijding van onlinehandelsfraude is een gedeelde verantwoordelijkheid van zowel private als publieke partijen. Belangrijke onderdelen van deze integrale aanpak zijn: het vergroten van de weerbaarheid en bewustwording van burgers en bedrijven en het opwerpen van barrières die potentiële fraudeurs de mogelijkheid tot frauderen ontnemen. Als zich desondanks fraude heeft voorgedaan, dient deze door een gerichte inzet van het strafrecht te worden bestreden.
Voor de aanpak van horizontale fraude zijn tussen openbaar ministerie en de politie in het kader van de Veiligheidsagenda kwantitatieve afspraken gemaakt. Landelijk worden er in 2016 tenminste 1600 fraudezaken aangepakt. Binnen die kwantitatieve afspraken, heeft internetgerelateerde fraude nadrukkelijk de aandacht.
De strafrechtelijke handhaving van fraude vindt altijd plaats binnen de actuele financiële, capacitaire- en wegingskaders. De online door het eerdergenoemde LMIO ontvangen aangiftes worden door het LMIO geanalyseerd. Aan de hand van een aantal verwante aangiftes, het schadebedrag en/of de (eventuele) minderjarigheid van een verdachte, worden zaken geselecteerd. Daarbij worden ook de omstandigheden rond de persoon van de verdachte betrokken (recidive, ISD-kandidaat, begeleiding in kader voorwaardelijke veroordeling). Een andere reden om een LMIO-zaak niet op te pakken kan zijn dat in bepaalde zaken een niet-strafrechtelijke interventie effectiever kan zijn.

7. Financiële paragraaf

De leden van de SP-fractie hebben gevraagd in hoeverre in de gaten zal worden gehouden of uitvoerende organisaties, vooral politie en rechtspraak, genoeg middelen hebben om deze taken uit te voeren, en hoe rekening is gehouden met de bezuinigingen op ICT bij de politie.
De uitvoering van de bevoegdheid vergt onder meer inzet van gespecialiseerde ICT-middelen. De voorbereiding wordt projectmatig vorm gegeven. Bij de prioritering voor ICT-ontwikkeling wordt rekening gehouden met aanpassingen van wetgeving en nieuwe bevoegdheden.

De leden van de SP-fractie hebben gevraagd of er voldoende expertise bij de politie is om deze extra bevoegdheden op te vangen, en of er bovendien genoeg middelen zijn om alle experts op te leiden om niet alleen om te gaan met de bevoegdheid maar ook met de techniek die erbij komt kijken.
De consequenties betreffen vooral de inrichting van een nieuw werkproces, de aanpassing van bestaande processen en een andere manier van werven van nieuwe medewerkers. Het betreft bijvoorbeeld het verkrijgen van de benodigde kennis, een verhoging van de expertise en het kennisniveau binnen bestaande afdelingen, en de aanleg, inrichting en het beheer van nieuwe ICT-infrastructuren en -middelen. De vraag en noodzaak van de digitaal experts wordt onderkend. De aankomende jaren zal middels door- en zijinstroom van medewerkers in deze vraag worden voorzien.

De leden van de SP-fractie hebben gevraagd of de regering een overzicht kan geven van de extra bevoegdheden die de rechter-commissarissen de afgelopen jaren erbij hebben gekregen en welk (extra) budget daartegenover heeft gestaan.
Hiervan is geen overzicht beschikbaar.

De leden van de SP-fractie hebben nogmaals aandacht gevraagd voor de capaciteit bij de politie. De leden van deze fractie hebben opgemerkt dat er 2.000 fte wordt weggehaald bij de politie, en hebben gevraagd hoeveel extra capaciteit dan kan worden ingezet bij uitvoering van bevoegdheden op grond van dit wetsvoorstel. De leden van deze fractie hebben tevens gevraagd of deze capaciteit van binnen de nationale politie en zo ja, waar vandaan, en of de regering haar antwoord kan toelichten.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de SP-fractie.

De leden van de CDA-fractie hebben gevraagd in hoeverre het in het kader van de werklaststijging voor met name de rechter-commissaris verstandig is geweest om de zelfstandige bevelsbevoegdheid van de officier van justitie uit het conceptwetsvoorstel te schrappen.
Zoals eerder, naar aanleiding van vragen van de leden van de CDA-fractie aan de orde is gekomen, is de regeling van de bevoegdheid van de officier van justitie tot het vorderen van het ontoegankelijk maken van gegevens bedoeld als aanvulling op de bestaande vrijwillige NTD-gedragscode. De NTD-gedragscode functioneert in de praktijk goed zodat de bevoegdheid van de officier van justitie is bedoeld als stok achter de deur, voor uitzonderlijke gevallen waarin de tussenpersoon weigert te handelen in overeenstemming met de gedragscode. De bevelsbevoegdheid van de officier van justitie zal naar verwachting dan ook niet veelvuldig aan de orde zijn, waardoor dat de werklaststijging voor de rechter-commissaris gering zal zijn. Overigens kan hierbij nog worden opgemerkt dat ook de huidige regeling van artikel 54a Sr uitgaat van een voorafgaande schriftelijke machtiging van de rechter-commissaris, zodat ten opzichte van de bestaande situatie bezwaarlijk kan worden gesproken van een werklaststijging.

De leden van de CDA-fractie hebben aangegeven met verwondering te hebben kennisgenomen van het standpunt dat de uitvoerende organisaties de kosten voor de inzet van het onderzoek in een geautomatiseerd werk moeten dekken binnen het reguliere budget zonder dat de regering daarbij aangeeft wat die precieze kosten zijn. Alleen voor de Raad voor de rechtspraak (Rvdr) is een verwachte inschatting gegeven (€ 500.000) en alleen al daarvan kunnen deze leden zich voorstellen dat het geen eenvoudige klus zal zijn voor de Rvdr om dit binnen de huidige financiële (beperkte) begroting in te passen. De leden van deze fractie hebben gevraagd hoe de regering dit aspect ziet.
De rechtspraak wordt gefinancierd middels outputfinanciering. In het kader van zijn wettelijke adviestaak heeft de Raad 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 de Raad voor de rechtspraak en het Ministerie van Veiligheid en Justitie.

De leden van de CDA-fractie hebben gevraagd waarom de regering de impact-analyse niet aan de Kamer heeft gezonden, dan wel de resultaten hiervan verwerkt in onderhavig wetsvoorstel. Deze leden hebben gevraagd of de regering alsnog bereid is zo spoedig mogelijk na ontvangt van dit verslag deze impactanalyse aan de Kamer te zenden.

De impactanalyse die de politie heeft uitgevoerd is voor zover relevant meegenomen en verwerkt in het wetsvoorstel. Het doel van de impactanalyse is de politie voor te bereiden op de implementatie van het wetsvoorstel. De impactanalyse is gezien de inhoud ervan gerubriceerd als zeer vertrouwelijk en kan daarom niet worden gedeeld.

De leden van de CDA-fractie hebben gevraagd wat precies de aanzienlijke consequenties zijn waarover de nationale politie het heeft in haar advies van 12 december 2014. De leden van deze fractie hebben verder gevraagd wat onderhavig wetsvoorstel niet alleen budgettair betekent, maar ook qua aantal benodigde extra fte voor de uitvoering hiervan. Deze leden hebben in het bijzonder gevraagd of er voldoende capaciteit in de technische teams is aanwezig is.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de SP-fractie.

De leden van de CDA-fractie hebben gevraagd of te verwachten valt dat er veel meer gebruik zal worden gemaakt van de voorgestelde bevoegdheden en zo ja, of zij hierop de personele bezetting van technische en tactische teams dan ook aanpast. De leden van deze fractie hebben tevens gevraagd wat de stand van zaken is van het implementatieplan van de nationale politie, waarnaar in het hierboven genoemde advies wordt verwezen.
De politie is sinds 2015 bezig met zich voor te bereiden op de implementatie van dit wetsvoorstel. De politie zal in het begin de bevoegdheid zeer beperkt inzetten. Aan de hand van de eerste ervaringen kan worden bezien of de bezetting van teams en de verwachtingen over het gebruik van de bevoegdheid moeten worden aangepast.

De leden van de CDA-fractie hebben gevraagd of er nog meer impactanalyses zijn opgesteld, bijvoorbeeld ten aanzien van het OM. Indien dat het geval is, vragen de leden van deze fractie de regering deze aan de Kamer te doen toekomen. De leden van deze fractie hebben ook gelezen dat er een «quick-scan online handelsfraude» is uitgevoerd, zij zouden deze ook graag ontvangen in het kader van de behandeling van dit wetsvoorstel.
Op deze vraag moet ontkennend worden geantwoord. Er zijn geen andere impactanalyses opgesteld.

De leden van de D66-fractie hebben aangegeven aan dat voor de politie en het OM de bedragen ontbreken. Deze leden missen de financiële gevolgen die uit het wetsvoorstel zullen voortvloeien voor de politie en hebben gevraagd aan welke bedragen dan moet worden gedacht en wat de financiële gevolgen van het voorstel betekenen voor andere activiteiten van de politie die uit hetzelfde bestaande budget gefinancierd worden.
De nationale politie financiert de voorbereidingen uit de middelen die beschikbaar zijn voor digitalisering en de bestrijding van cybercrime. De structurele inzet van de bevoegdheid wordt uit het reguliere budget van de politie gefinancierd. Het gaat daarbij vooral om de inzet van capaciteit ter ondersteuning van operationele onderzoeken. Deze capaciteit maakt deel uit van de landelijke eenheid van het landelijk politiekorps.

De leden van de D66-fractie hebben de regering gevraagd de Kamer een impactanalyse met kostenplaatje te doen toekomen gelijktijdig met nota naar aanleiding van het verslag zodat de Kamer ook daar kennis van kan nemen.
Voor het antwoord op deze vraag wordt verwezen naar de eerdere beantwoording van een soortgelijke vraag van de leden van de CDA-fractie.

De leden van de D66-fractie hebben gevraagd om een reactie op het bericht van de politie dat zij de nieuwe online opsporingstaken niet kan gaan uitvoeren als er voor 40 miljoen euro moet worden bezuinigd op de ICT, zoals de regering wil. Het plaatsvervangend hoofd van de Landelijke Recherche noemt de twee ambities van de regering «volstrekt onverenigbaar» en zegt dat «de politiek heel veel vraagt van de politie en zich goed moet afvragen waar de prioriteit ligt.» De leden van deze fractie hebben gevraagd wat mijn reactie is op deze noodklok van de recherche en hoe ik denk er in te voorzien dat de ICT-faciliteiten van de politie geschikt zijn om de nieuwe hackbevoegdheden te kunnen uitvoeren.
De politie ontvangt een bijzondere bijdrage van 13,8 miljoen euro per jaar voor de verdere professionalisering in een gedigitaliseerde wereld en de bestrijding van cybercrime. Onder meer de aanschaf en implementatie van ICT-hulpmiddelen wordt hieruit gefinancierd. Ook de voorbereiding van de implementatie van dit wetsvoorstel wordt hier grotendeels uit bekostigd. De personeels- en IV-capaciteit en de structurele kosten voor beheer en onderhoud komen ten laste van de algemene begroting van de politie. Overigens is aan de begroting een extra bedrag toegevoegd voor het aanpakken van cybercrime. Voor 2017 is dit een bedrag van 1,4 miljoen euro, voor 2018 wordt dit bedrag verhoogd tot 1,5 miljoen euro, ten behoeve van de versterking van de personele en materiële capaciteit.

8. De adviezen over het wetsvoorstel

8.1 Het onderzoek in een geautomatiseerd werk

De leden van de SP-fractie hebben gevraagd hoe groot de kans is dat opsporingsdiensten stuiten op gegevens van niet-verdachten en tevens hoe hiermee wordt omgegaan.
Zoals eerder, in de beantwoording van vragen van de leden van de SP-fractie, is aangegeven zal het vrijwel altijd zo zijn dat de opsporingsdiensten bij het verzamelen van informatie over verdachten op gegevens van niet-verdachten stuiten. Dit is bij de uitoefening van alle opsporingsbevoegdheden aan de orde. Doordat verdachten onder meer de geautomatiseerde werken gebruiken voor communicatie is er altijd ook sprake van andere participanten aan deze communicatie. Daarbij zal er ook sprake zijn van communicatie die niet of minder relevant is voor de opsporing. Zoals hierboven naar aanleiding van vragen van de leden van de fractie van D66, in paragraaf 2.3.1, aan de orde is gekomen, gelden specifieke verplichtingen rond het verdere gebruik en de vernietiging van de verzamelde gegevens bij de inzet van bepaalde opsporingsbevoegdheden waarbij gegevens van derden ter kennis kunnen komen van de opsporing. Deze verplichtingen zijn onverkort van toepassing voor de toepassing van het aftappen van telecommunicatie en het opnemen van vertrouwelijke communicatie, nadat op afstand een geautomatiseerd werk is binnengedrongen.

De leden van de SP-fractie hebben erop gewezen dat volgens de regering uit een masterscriptie blijkt dat het voorgestelde artikel 126nba Sv in beginsel de noodzakelijkheidstoets van artikel 8, tweede lid, EVRM kan doorstaan en hebben gevraagd wat wordt bedoeld met «in beginsel» en wanneer dit niet het geval is.
In de masterscriptie getiteld «Hacken als opsporingsbevoegdheid in het licht van artikel 8 lid 2 EVRM: de zoektocht naar een *«fair balance»* tussen opsporing en privacy (Y.J.G.H.L. Straus, Masterscriptie Straf(proces)recht Faculteit der Rechtsgeleerdheid, Radboud Universiteit Nijmegen), wordt de noodzakelijkheid van de voorgestelde bevoegdheid tot het binnendringen in een geautomatiseerd werk (aangeduid als: hackbevoegdheid)

in het licht van artikel 8, tweede lid, EVRM onderzocht[6]. Vastgesteld wordt dat de inbreuk op het privéleven, vanwege de voorgestelde bevoegdheid, moet aansluiten op een *pressing social need* en in een redelijke verhouding moet staan tot het belang van de opsporing van strafbare feiten. Er moet derhalve een *fair balance* worden gecreëerd tussen het dringende belang van de opsporing bij invoering (en uiteindelijk toepassing) van een bevoegdheid tot het binnendringen in een geautomatiseerd werk enerzijds en het belang van burgers bij de waarborging van hun recht op privéleven anderzijds (blz. 59). De eerste eis voor een *fair balance* is dat er, mede in het licht van het vereiste van de *pressing social need*, voldoende grond is voor de bevoegdheid. Op basis van een analyse van het onderzoeksbelang wordt geconcludeerd dat een hackbevoegdheid in redelijke verhouding staat tot het belang van de opsporing van strafbare feiten wanneer de toepasbaarheid wordt beperkt tot de categorie «zeer zware delicten». Aan het eerste vereiste voor een *fair balance* is dan voldaan(blz. 60). De tweede eis voor een *fair balance* is dat de bevoegdheid tot het binnendringen in een geautomatiseerd werk wordt omkleed met voldoende waarborgen om te garanderen dat de beginselen van proportionaliteit en subsidiariteit ook bij concrete toepassingen van de bevoegdheid voldoende in acht genomen worden. Toetsing van deze vereisten aan het conceptwetsvoorstel computercriminaliteit III voert de auteur tot de slotsom dat de voorgestelde bevoegdheid voldoet aan het eerste vereiste van de *fair balance* (blz. 61). Voor wat betreft het tweede vereiste is de auteur van mening dat de voorgestelde bevoegdheid met voldoende waarborgen wordt omkleed om aan dit vereiste te voldoen. Uitzondering hierop vormt vooralsnog het gebrek aan een duidelijk mechanisme voor de *logging* van de handelingen die de opsporingsambtenaren op een binnengedrongen geautomatiseerd werk verrichten (blz. 62). Voor zover het gaat om de bescherming van het privéleven zijn er naar het inzicht van de auteur geen juridische bezwaren verbonden aan het destijds voorgestelde artikel 125ja Sv, inmiddels gewijzigd in artikel 126nba/uba/zpa Sv, en worden de praktische problemen voor een groot deel reeds zoveel mogelijk beperkt door de gestelde waarborgen (blz. 62). De overige problemen zullen in de praktijk moeten worden opgelost. Geconcludeerd wordt dat het destijds voorgestelde artikel 125ja Sv in beginsel de noodzakelijkheidstoets van artikel 8, tweede lid, EVRM kan doorstaan. Met de woorden «in beginsel» wordt kennelijk gedoeld op bepaalde handelingen rond niet-versleutelde gegevens, die de zogenaamde relevantietoets niet kunnen doorstaan. Dit betreft volgens de auteur het direct afluisteren van gesprekken en de stelselmatige observatie van personen, waarbij geen sprake is van de versleuteling van gegevens (blz. 34 en 36).

Naar aanleiding van deze bevindingen kan worden opgemerkt dat de onderzoekshandelingen als het direct afluisteren en de stelselmatige observatie tevens kunnen zijn gericht op niet-versleutelde gegevens. De versleuteling van gegevens is weliswaar een belangrijke oorzaak voor het tekort schieten van de bestaande opsporingsbevoegdheden maar de afhandeling van communicatie via het internet stelt de opsporing voor andere problemen, zoals dat het gebruik van internet kan belemmeren dat een aanbieder kan worden gevonden die kan worden aangesproken op de wettelijke verplichting aftapbaar te zijn. In dit geval kan het direct afluisteren van een geautomatiseerd werk, bijvoorbeeld door het gebruik van een microfoon of luidspreker van een computer of smartphone, dringend noodzakelijk voor de opsporing van ernstige strafbare feiten.

In zijn advies heeft Afdeling advisering van de Raad van State opgemerkt dat deze bevoegdheden minder ingrijpend zijn en dat daarbij met de thans op grond van het Wetboek van Strafvordering geldende voorwaarden kan

[6] http://njb.nl/Uploads/2014/2/Scriptie-Straf-proces-recht-Yannick-Straus-Radboud-Universiteit-Nijmegen---inzending-NJB.pdf

worden volstaan. Verder kan nog worden opgemerkt dat de functionaliteit voor de logging zal worden uitgewerkt in een algemene maatregel van bestuur ter uitvoering van het wetsvoorstel.

De leden van de SP-fractie wilden weten hoe wordt gecontroleerd of de software buiten de grenzen van de bevoegdheid kan worden ingezet, zoals Bits of Freedom opmerkt. De leden van deze fractie hebben tevens gevraagd wat de ervaringen van de Duitse autoriteiten hiermee zijn, maar ook waar het gaat om aanvallen van derden.
Onder verwijzing naar de eerdere beantwoording van vragen over de keuring van de software en de scheiding tussen de technische en de tactische politiefunctionarissen kan aanvullend worden opgemerkt dat het gebruik van technische hulpmiddelen bijna altijd met zich meebrengt dat niet alle mogelijkheden die de techniek heeft ook benut zullen worden. De inzet van de technische middelen is gebonden aan de wettelijke grenzen en in dit geval aan de toestemming die is verkregen van de rechter commissaris. In het bevel staat omschreven voor welke handeling toestemming gegeven wordt. Naar aanleiding hiervan richten de technische functionarissen de software zodanig in dat tijdens de inzet daarvan wordt voldaan aan de in het bevel aangegeven kaders. De tactische medewerkers kunnen daar geen invloed op uitoefenen. Zoals eerder, in paragraaf 2.6, naar aanleiding van vragen van onder meer de leden van de PvdA-fractie aan de orde is gekomen, zal aanvullend worden voorzien in systeemtoezicht op de uitvoering van het bevel tot het op afstand binnendringen van een geautomatiseerd werk.

De leden van de SP-fractie hebben gevraagd in hoeverre IT-bedrijven en instanties betrokken zijn bij de totstandkoming van onderhavig wetsvoorstel en zo nee, waarom zij niet betrokken zijn.
De discussie over het wetsvoorstel loopt reeds gedurende enkele jaren. In veel van de gremia waar de overheid overlegt met bedrijven en instanties is gesproken over de voornemens om de bevoegdheden van de opsporingsdiensten op het internet uit te breiden. Soms ging dit in de vorm van een presentatie, soms stond het onderwerp op de agenda en werd mondeling toegelicht vanuit overheidswege. Met name de bijeenkomsten van het Platvorm Internetveiligheid en de bijeenkomsten die georganiseerd zijn door de NCTV waar de overheid overlegt met de private partijen, zijn hiervoor benut. Ook heeft mijn ambtsvoorganger gesprekken gevoerd met medewerkers van de universiteiten over de nieuwe bevoegdheid. Politie en openbaar ministerie kennen ook hun contacten met het bedrijfsleven en hebben in het verleden ook samen met gespecialiseerde IT-bedrijven in onderzoeken samengewerkt. De internet consultatie bood de mogelijkheid voor eenieder, waaronder IT-bedrijven en andere organisaties, om een bijdrage te leveren aan de meningsvorming. Deze mogelijkheid is door diverse organisaties benut.

De leden van de SP-fractie hebben gevraagd om een reactie op de zorgen van de Raad voor de rechtspraak over de binnendringingsbevoegdheid op buitenlands geautomatiseerde werken, omdat het betrokken justitieel personeel zich dan naar het recht van veel landen schuldig zal maken aan het misdrijf van computervredebreuk, met alle gevolgen van dien.
De regering is niet bekend met de door de leden van de SP-fractie aangehaalde zorgen van de Raad voor de rechtspraak op dit punt. Overigens kan worden opgemerkt dat het vraagstuk van strafbaarheid van politie- en justitiefunctionarissen zich ook kan voordoen bij de uitoefening van andere opsporingsbevoegdheden waarbij wordt geraakt aan de rechtsmacht van andere landen zonder dat dit op dat moment bekend is, zoals bij het aftappen van communicatie. Tot nu toe levert dit in de praktijk geen problemen op. En zoals eerder in paragraaf 2.8, naar aanleiding van vragen van de leden van de fractie van de PvdA is opgemerkt zal, zodra

bekend is dat gegevens zich op het grondgebied van een ander land bevinden, zo snel mogelijk een verzoek tot rechtshulp wordt gedaan.

De leden van de CDA-fractie hebben gevraagd of de regering kan aangeven hoe het OM de betreffende vertegenwoordiger heeft voorbereid op deze hoorzitting. De leden van deze fractie hebben tevens gevraagd wat nu precies het standpunt van het OM is ten aanzien van het terugkomen in het wetsvoorstel van het encryptiebevel. Ook hebben deze leden de regering gevraagd dit nogmaals te inventariseren bij de nationale politie en bij andere betrokken veiligheidsdiensten in de keten.
De vertegenwoordiger van het openbaar ministerie heeft aangegeven dat hij geen kennis had van een ander standpunt ten aanzien van het decryptiebevel dan het standpunt van het openbaar ministerie, dat is vastgesteld tijdens de consultatieronde in juli 2013. In het schriftelijk advies van 8 juli 2013 is opgenomen dat het voorgestelde decryptiebevel praktische en juridische bezwaren oproept. Het College vroeg zich af of het voorgestelde bevel en de daaraan gekoppelde strafbaarstelling verenigbaar is met het nemo-teneturbeginsel. Voorts is het openbaar Ministerie van mening dat de wetgever terughoudend zou moeten zijn met een instrumentele inzet van het strafrecht. De bedoeling is om misdadigers te straffen voor feiten die zij hebben begaan, niet om verdachten te straffen voor het niet meewerken aan bewijsgaring. Als het decryptiebevel toch zou worden ingevoerd dan was het volgens het College noodzakelijk om daar zwaarwegende omstandigheden aan te verbinden.

De leden van de CDA-fractie menen dat het volledig schrappen van het decryptiebevel aan de verdachte een gemiste kans is en hebben gevraagd hoe het schrappen van het decryptiebevel aan de verdachte valt te plaatsen in het licht van eerdere uitlatingen van de voormalig Minister van Veiligheid en Justitie.
In de brief aan uw Kamer van 10 juni 2011 is de voormalig Minister van Veiligheid en Justitie ingegaan op de door het lid Van Toorenburg van de fractie van het CDA opgeworpen vraag of er wetgeving zou moeten komen om verdachten in kinderpornozaken te kunnen verplichten medewerking te verlenen aan het toegankelijk maken van gegevens op een computer die met gebruik van encryptie zijn versleuteld (hierna: decryptiebevel). Hij heeft daarbij aangegeven het van essentieel belang te achten dat de te treffen maatregelen daadwerkelijk effectief zijn en over een aantal aspecten rond het decryptiebevel overleg te voeren met het openbaar ministerie (Kamerstukken II 2010/11, 32 500 VI, nr. 106).
In zijn brief van 27 januari 2012 heeft de voormalig Minister van Veiligheid en Justitie te kennen gegeven op grond van de ervaringen in het Verenigd Koninkrijk de mogelijkheden van een vergelijkbare regeling in de Nederlandse strafwetgeving met een positieve grondhouding te willen benaderen. Binnen het Nederlandse stelsel van strafvordering kan een verdachte echter niet worden verplicht mee te werken aan zijn eigen veroordeling. Vanwege de onduidelijkheid omtrent de juridische haalbaarheid van een decryptiebevel, in het licht van het in artikel 6 EVRM vervatte nemo tenetur-beginsel, achtte hij een nader onderzoek naar de verenigbaarheid van een decryptiebevel met dit beginsel wenselijk alvorens tot het in voorbereiding nemen van wetgeving te besluiten (Kamerstukken II 2011/12, 31 015, nr. 77).
Bij brief van 27 november 2012 heeft de voormalig Minister van Veiligheid en Justitie het rapport van het Tilburg Institute for Law Technology and Society (TILT) van de Universiteit van Tilburg (TILT), getiteld «Decryptiebevel en artikel 6 EVRM» aan Uw Kamer aangeboden[7]. Op basis van de

[7] Het decryptiebevel en het nemo-teneturbeginsel, nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voorverdachten?, B.J. Koops, WODC, 305.

afweging van de verschillende opties ging zijn voorkeur uit naar opneming in het Wetboek van Strafvordering van een bevoegdheid tot het geven van een bevel aan een verdachte tot het verschaffen van toegang tot versleutelde elektronische gegevens en het toegankelijk maken van die gegevens. In de brief zijn de kaders weergegeven, op basis waarvan een wetsvoorstel zou worden voorbereid (Kamerstukken II 2012/13, 33 400 VI, nr. 68).
Tijdens het Algemeen Overleg over een aantal onderwerpen met betrekking tot informatie- en communicatie technologie (ICT), gehouden op 15 januari 2013, heeft de voormalig Minister van Veiligheid en Justitie aangegeven na grote aarzeling te hebben gezegd naar het decryptiebevel aan de verdachte te zullen kijken en tot de conclusie te zijn gekomen dat men dat zou moeten doen (Kamerstukken II 2012/13, 26 643, nr. 265).
Uit deze stukken blijkt dat de voormalig Minister van Veiligheid en Justitie heeft aangegeven het voor de bestrijding van kinderpornografie van groot belang te vinden dat politie en justitie toegang krijgen tot versleutelde gegevens, ook om de slachtoffers van kinderpornografie beter te kunnen beschermen en een decryptiebevel aan de verdachte vanuit een positieve grondhouding te benaderen. Daarbij heeft hij ook gewezen op de juridische complicaties, in het bijzonder het beginsel dat een verdachte niet kan worden verplicht aan zijn eigen veroordeling mee te werken. Op basis van de uitkomsten van het onderzoek van TILT is wetgeving in voorbereiding genomen. Met de voormalig Minister van Veiligheid en Justitie ben ik van oordeel dat al het mogelijke dat effectief is dient te worden gedaan om kinderpornografie te bestrijden en de slachtoffers te beschermen. Naar aanleiding van het advies van de Afdeling advisering van de Raad van State ben ik echter tot de conclusie gekomen dat een decryptiebevel aan de verdachte zowel juridisch als praktisch nauwelijks haalbaar is en overigens niet voldoende tegemoet komt aan de behoefte van de opsporingspraktijk. Hieronder zal ik, naar aanleiding van de andere vragen van de leden van de CDA-fractie, nader ingaan op de overwegingen die aan deze beslissing ten grondslag liggen.

De leden van de CDA-fractie hebben erop gewezen dat de Minister van Veiligheid en Justitie heeft aangegeven dat een ontsleutelplicht verenigbaar is met het nemo teneturbeginsel mits de regeling met goede waarborgen is omkleed en hebben gevraagd wat er sedertdien is veranderd dat de regering gevolg heeft gegeven aan de argumentatie van de Afdeling advisering van de Raad van State dat de ontsleutelplicht zich niet goed verhoudt tot het nemo teneturbeginsel als onderdeel van artikel 8 EVRM, immers pas na dit advies heeft de regering haar standpunt gewijzigd.
Vanwege verschillende overwegingen is de regering tot het inzicht gekomen dat een decryptiebevel aan de verdachte nauwelijks haalbaar is. Deze overwegingen zijn zowel van meer praktische aard, verband houdend met de effectiviteit van een dergelijk bevel, als van meer juridische aard, verband houdend met het recht op een eerlijk proces zoals dat wordt beschermd door het EVRM.
In de eerste plaats hebben zowel het College van Procureurs-Generaal, de Nederlandse Vereniging voor Rechtspraak en de Afdeling advisering gewezen op de complicaties rond de bewijslevering. Nu het gaat om een misdrijf is opzet vereist, dat wil zeggen dat wordt bewezen dat de verdachte opzettelijk niet heeft voldaan aan een bevel tot ontsleuteling van versleutelde gegevens. Dit bewijs zal in de praktijk bijzonder lastig zijn te leveren, als de verdachte een beroep doet op geheugenverlies of onjuiste gegevens verstrekt. Het College heeft er zelfs voor gewaarschuwd dat in «verreweg de meeste gevallen het bewijs van het opzet niet zal zijn te leveren». Een ander probleem betreft de technische ontwikkeling, die het mogelijk maakt geheime bestanden aan het oog van de buitenwereld te onttrekken. Ook in het rapport van TILT was hierop reeds gewezen (blz.

42). De incriminerende bestanden kunnen worden opgeslagen in het «hidden volume» van het geautomatiseerde werk, waarvan de autoriteiten het bestaan niet kunnen bewijzen. De verdachte kan dan de gegevens beschikbaar stellen tot bestanden waarin onschuldige gegevens zijn opgeslagen, zodat hij heeft voldaan aan het decryptiebevel. Verder is in dit verband van belang dat de verdachte in de praktijk de voorkeur zal geven aan het niet voldoen aan een decryptiebevel, als de strafbedreiging lager is dan voor het gronddelict, om een veroordeling voor het gronddelict te ontlopen. Dit risico houdt nauw verband met de hoogte van de strafbedreiging voor het niet voldoen aan een decryptiebevel, en daarmee met de aanvaardbaarheid van een decryptiebevel in het licht van artikel 8 van het EVRM. Hierop wordt hieronder nader ingegaan.
Verder is de verhouding tussen het decryptiebevel en het beginsel van nemo tenetur van belang. De Afdeling advisering heeft in dit verband gewezen op de jurisprudentie van het EHRM over de druk op terrorismeverdachten om informatie te verstrekken. Dit betreft de zaak O'Heaney en Mc Guiness tegen Ierland van 21 december 2000. Deze zaak had betrekking op een bomaanslag op een controlepost in Noord-Ierland waarbij een persoon om het leven kwam en enkele Britse militairen zwaargewond raakten (Application no. 34720/97). De Ierse politie arresteerde kort na de aanslag drie verdachten in een woning in de omgeving van de controlepost, en verzocht hen te verklaren over de bomaanslag, hun aanwezigheid in de woning en hun bewegingen gedurende de nacht. Zij weigerden te antwoorden en werden vervolgd. Zij werden vrijgesproken van het lidmaatschap van een criminele organisatie maar veroordeeld vanwege het niet voldoen aan de verplichting, vastgelegd in sectie 52 van de State Act 1939, tot een gevangenisstraf van zes maanden. Het EHRM stelde vast dat het in deze zaak geen materiaal betrof dat bestond onafhankelijk van de wil van de klagers en dat er sprake was van een «charge» in de zin van artikel 6 EVRM. Het Hof oordeelde dat de mate van dwang die met de toepassing van sectie 52 op de klagers werd uitgeoefend om hen te brengen tot het verstrekken van informatie de essentie van hun zwijgrecht aantastte en concludeerde dat artikel 6 EVRM was geschonden. Het verweer van de Ierse regering dat sectie 52 van de State Act 1939 de nodige waarborgen bevatte werd door het Hof verworpen omdat deze regeling de betrokkene de keuze liet tussen het leveren van de gevraagde informatie of een veroordeling tot ten hoogste zes maande gevangenisstraf (punt 51). Het verweer van de regering gericht op de proportionaliteit van de regeling in het licht van de dreiging van terrorisme werd door het Hof eveneens verworpen, onder verwijzing naar de zaken Saunders (17-12-1996, NJ 1997/699) en Brogan (29-11-1988, Series A no. 145-B), omdat deze belangen niet een bepaling kunnen rechtvaardigen die de essentie van het recht om te zwijgen en zichzelf niet te belasten uitwissen (punt 58). Volgens het EHRM was de dreiging bij terrorismeverdachten met een gevangenisstraf van zes maanden om informatie te verstrekken zodanig, dat het recht om zichzelf niet te belasten in de kern was aangetast en oordeelde unaniem tot een schending van artikel 8 EVRM (punten 55 en 59). Uit deze uitspraak kan worden afgeleid dat het EHRM ook in gevallen van zeer ernstige misdrijven, zoals terroristisme, van oordeel is dat een strafbedreiging van zes maanden reeds een zodanig mate van dwang oplevert dat het recht om zichzelf niet te belasten in de kern is aangetast. De strafbedreiging voor het niet voldoen aan het decryptiebevel is met drie jaar echter aanzienlijk hoger. Op dit punt dient zich de afweging aan tussen drie variabelen, te weten de hoogte van de strafbedreiging, de verenigbaarheid met artikel 6 EVRM en het risico van calculerend gedrag door de verdachte. De voorgestelde strafbedreiging van drie jaar gevangenisstraf is aanzienlijk hoger dan de zes maanden gevangenisstraf waarover het EHRM zich in de zaak O'Heaney en Mc Guiness tegen Ierland heeft uitgesproken. Verlaging van die strafbedreiging kan bijdragen aan de kans

dat het decryptiebevel door het EHRM verenigbaar wordt geacht met artikel 6 EVRM. Een dergelijke verlaging zal het risico op calculerend gedrag door de verdachte echter navenant doen toenemen. Verhoging van de strafbedreiging heeft een omgekeerd effect.
Dit alles klemt temeer daar het decryptiebevel aan de verdachte niet leidt tot het daadwerkelijk beschikbaar komen van de versleutelde gegevens voor de opsporing. De verdachte kan ervoor kiezen niet te voldoen aan het decryptiebevel en vervolging op grond van het voorgesteld artikel 184b Sv te riskeren, waarbij de gevangenisstraf niet hoger dan drie jaar kan zijn. Ook het College van procureurs-generaal en de Nederlandse Vereniging voor Rechtspraak hebben hierop gewezen. Als het decryptiebevel al verenigbaar zou zijn met artikel 6 EVRM, dan is het weinig bevredigend als een verdachte ervoor kiest niet te voldoen aan een decryptiebevel. De gegevens blijven dan versleuteld en daarmee blijven de slachtoffers onttrokken aan het zicht van de hulpverlening. De regering geeft daarom de voorkeur aan de bevoegdheid van het op afstand binnendringen van een geautomatiseerd werk. Met behulp van deze bevoegdheid kunnen wachtwoorden en inlogcodes worden achterhaald en vastgelegd, zodat de versleutelde bestanden eenvoudig kunnen worden ontsleuteld en de versleutelde gegevens daadwerkelijk beschikbaar komen voor de opsporing. Bijkomend voordeel is dat deze bevoegdheid heimelijk wordt toegepast, zodat gedurende het opsporingsonderzoek gegevens kunnen worden verzameld met het oog op het bewijs van ernstige vormen van kinderpornografie en de betrokkenheid van de verdachte daarbij.

De leden van de CDA-fractie konden in het advies van de Afdeling advisering geen verwijzingen naar Europese jurisprudentie terugvinden waaruit zou blijken dat het encryptiebevel niet kan worden gegeven in het licht van artikel 6 EVRM en hebben gevraagd of de regering deze mening deelt en zo ja, of de regering kan toelichten waarom zij desalniettemin deze keuze heeft gemaakt.
Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van de vorige vraag van de leden van de CDA-fractie. Op basis van de uitspraak van het EHRM in de zaak O'Heaney en Mc Guiness tegen lerland, is het niet waarschijnlijk dat een decyptiebevel aan de verdachte, waarbij een strafbedreiging van meer dan zes maanden geldt, door het EHRM verenigbaar wordt geacht met artikel 6 van het EVRM.

De leden van de CDA-fractie hebben de regering gevraagd in te gaan op de gevolgen die deze keuze heeft voor de bestrijding op nationaal- en internationaal niveau van onder meer kinderpornonetwerken en hebben gevraagd of de regering nog steeds het nut in ziet van haar oorspronkelijke voorstel dan wel in de voorgestelde wijziging door het College van procureurs-generaal, zodat in de meest gruwelijke en ernstige omstandigheden het bevel voor een doorbraak in het opsporingsonderzoek kan zorgen en zo ja, of de regering bereid is dit onderdeel alsnog in het wetsvoorstel op te nemen.
Zoals in de eerdere beantwoording van de vragen van de leden van de CDA-fractie hierboven reeds aan de orde is gekomen, ziet de regering in de praktijk weinig ruimte voor een effectief decryptiebevel aan de verdachte. In plaats daarvan hecht de regering aan de bevoegdheid van het op afstand binnendringen in een geautomatiseerd werk zodat de gegevens daadwerkelijk beschikbaar kunnen komen voor de opsporing, ook als deze zijn versleuteld, en de slachtoffers kunnen worden beschermd.

8.2 Het wederrechtelijk overnemen en helen van gegevens

De leden van de CDA-fractie vinden het een gemiste kans dat in het wetsvoorstel geen regeling is opgenomen om een domeinnaam van een website te verwijderen en hebben gevraagd of dit toch niet een mogelijkheid geeft om tegen misleidende websites op te treden. Ook hebben zij gevraagd of van deze verwijdering niet een belangrijke signaalwerking uitgaat en wat de regering in plaats daarvan voorstelt te doen. Deze leden hebben verder gevraagd of de regering bereid is deze keuze te heroverwegen, nu ook het College van procureurs-generaal heeft voorgesteld een wettelijke bevoegdheid te creëren waardoor het mogelijk wordt te bevelen dat een domeinnaam wordt doorgehaald of wordt overgeschreven naar de overheid.

Zoals in de memorie van toelichting is toegelicht, is tijdens de consultatie door het College van procureurs-generaal en SIDN (Stichting Internet Domeinregistratie Nederland) gewezen op de mogelijkheid van misbruik van een domeinnaam. Met de keuze voor een domeinnaam die lijkt op die van een bekende instelling kan een bezoeker van een website in de waan worden gebracht zich op de website van die instelling te bevinden. Daardoor kunnen onbevoegden de inloggegevens van de klanten of relaties van die instellingen bemachtigen. Deze partijen hebben geadviseerd in het wetsvoorstel een regeling op te nemen voor het bevel tot het doorhalen van een domeinnaam. Aan dit advies is geen gevolg gegeven omdat, zoals SIDN zelf ook opmerkt, de verwijdering van de domeinnaam er niet toe zal leiden dat de website niet meer bereikbaar is. Door een ISP een domeinnaam te laten blokkeren, worden alleen de aangesloten klanten van die ISP beperkt in hun mogelijkheden om de website via die domeinnaam te bezoeken. De domeinnaam blijft voor de rest van de wereld actief, net als de website die daarmee kan worden bereikt. En verder kan door aan de website een andere domeinnaam te koppelen deze weer snel vindbaar worden gemaakt. Het effect van het blokkeren van domeinnamen is zeer beperkt. Het Domeinnaamsysteem ofwel DNS is één van de kernprotocollen van het internet. De regering is van mening dat, in het licht van het maatschappelijk belang van het vertrouwen in het neutraal en betrouwbaar functioneren van het internet als technisch systeem, voorzichtigheid op zijn plaats is bij het ingrijpen op de kernprotocollen van het internet door de overheid.

II ARTIKELSGEWIJZE TOELICHTING

Artikel I, onderdeel C

Artikel 138c

De leden van de CDA-fractiedelen delen de mening van de Nederlandse vereniging voor Rechtspraak dat de voorgestelde strafbedreiging van een jaar voor het voorgestelde artikel 138c te laag is en hebben gevraagd hoe de regering er over denkt om een hogere strafmaat op te nemen voor niet alleen het voorgestelde artikel maar ook ten aanzien van het al bestaande artikel 273 Sr.
Met de voorgestelde strafbedreiging van een jaar wordt aangesloten bij de strafbedreiging voor het opzettelijk en wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk (art. 139c Sr). Het bezitten en verspreiden van afgeluisterde gegevens is strafbaar gesteld met gevangenisstraf van ten hoogste zes maanden (art. 139e Sr). De NVvR heeft zich afgevraagd waarom ter zake van deze strafbepaling geen aansluiting is gezocht bij de strafbepaling van diefstal. Daarnaast kan de handeling die

onder het voorgestelde artikel 138c Sr valt, ingrijpende zaken met een grote maatschappelijke impact betreffen, zoals bedrijfsspionage. In reactie hierop wordt opgemerkt dat met de voorgestelde strafbedreiging juist rekening is gehouden met het feit dat de rechthebbende de beschikkingsmacht over de gegevens behoudt, indien de rechthebbende de beschikkingsmacht over de gegevens verliest dan kan op grond van de jurisprudentie worden aangenomen dat sprake is van diefstal. De bedrijfsspionage waar door de NVvR naar wordt verwezen, valt onder de reikwijdte van artikel 273 Sr, waarvoor thans een strafbedreiging geldt van een gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie. De regering is dan ook van mening dat de voorgestelde strafbedreiging voor schending van artikel 138c Sr goed past in de systematiek van de wet.

Artikel I, onderdelen F en G

Artikelen 248a en 248e

De leden van de SP-fractie hebben gevraagd hoe bij grooming bewezen kan worden dat een verdachte het oogmerk had van misbruik van seksueel misbruik van een kind beneden de leeftijd van zestien jaren en wijzen erop dat in de memorie van toelichting wordt gesteld dat veroordeling kan plaatsvinden als meerdere keren is aangedrongen op een ontmoeting. Deze leden merken op dat daarmee echter nog niet automatisch is vastgesteld dat sprake is van het oogmerk van misbruik.
Het oogmerk om ontuchtige handelingen te plegen maakt nu ook al onderdeel uit van de delictsomschrijving van grooming. De dader moet blijk geven van de wil het digitale contact te willen omzetten in fysiek misbruik. Al dan niet voorwaardelijk opzet kan afgeleid worden uit gevoerde chatgesprekken ter voorbereiding van een beoogde ontmoeting.

Artikel I, onderdeel I

Artikel 326d

De leden van de CDA-fractie hebben gevraagd waarom de regering aan het opleggen van voorlopige hechtenis bij verdenking van grootschalige handelsfraude de eis heeft gekoppeld dat eerst vijf jaar moet zijn verstreken sinds een eerdere onherroepelijke veroordeling.
Aangesloten is bij de regeling zoals die geldt voor verwante delicten als oplichting en flessentrekkerij (artikelen 326 en 326a Sr). Het voordeel van toevoeging van het misdrijf van artikel 326d Sr aan artikel 67a, tweede lid, onder 3, Sv is dat een recidiverende internetoplichter eenvoudiger in voorlopige hechtenis kan worden genomen. Recidivegevaar kan op grond van artikel 67a, tweede lid, onder 3, Sv als grond voor voorlopige hechtenis aangenomen worden bij verdenking van diverse vermogensdelicten als de verdachte in de vijf jaren voor het plegen van het feit wegens een dergelijk delict veroordeeld is en er ernstige vrees bestaat dat de verdachte een dergelijk misdrijf opnieuw zal begaan.

Artikel II, onderdeel A

Artikel 67

De leden van de CDA-fractie hebben gevraagd waarom de regering niet bij meer van de voorgestelde strafbaarstellingen de toepassing van voorlopige hechtenis mogelijk maakt. Zij geven te kennen een aanscherping niet meer dan logisch te achten, in elk geval met betrekking tot grooming (artikel 248e Sr).

In artikel 67 van het Wetboek van Strafvordering is geregeld in welke gevallen voorlopige hechtenis mogelijk is. 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. Artikel 67, eerste lid, onder b, Sv bepaalt daarnaast dat bij verdenking van enkele specifieke misdrijven waarin sprake is van een lagere strafbedreiging voorlopige hechtenis kan worden toegepast. Artikel 248e Sr wordt ook genoemd in het eerste lid, onder b. Er is derhalve reeds voorzien in de door de leden van de CDA-fractie gesuggereerde mogelijkheid. Aanscherping van de regeling van de voorlopige hechtenis met betrekking tot grooming is gelet hierop niet nodig.

Artikel II, onderdeel C

Artikel 125m

De leden van de CDA-fractie hebben gevraagd wat de sanctionering is wanneer de geheimhoudingsverplichting worden geschonden door bijvoorbeeld webhostingbedrijven.
De niet-naleving van de geheimhoudingsverlichting uit hoofde van ambt, beroep of wettelijk voorschrift levert het strafbare feit op van artikel 272 Sr. Degene die opzettelijke een dergelijke geheimhoudingsverplichting schendt kan worden gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.

Artikel II, onderdeel D

Artikel 125p

De leden van de CDA-fractie hebben nogmaals gevraagd of het wel verstandig is ook een rechterlijke machtiging te vereisen bij het bevel tot ontoegankelijkmaking van gegevens, juist gezien de spoedeisendheid waar de regering naar verwijst.
Zoals eerder, naar aanleiding van soortgelijke vragen van de leden van de CDA-factie, aan de orde is gekomen, raakt het bevel van de officier van justitie tot de ontoegankelijkmaking van gegevens aan de vrijheid van meningsuiting. De vrijheid van meningsuiting wordt beschermd door artikel 7 van de Grondwet en artikel 10 van het EVRM. Op grond van de jurisprudentie over het EVRM blijkt dat de regeling voldoende precies dient te zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden bevoegdheden mogen worden toegepast, en voldoende waarborgen te bieden tegen willekeurige inmenging van de overheid in het persoonlijk leven van de burger. Door het vereiste van een voorafgaande rechterlijke machtiging wordt deze waarborg geboden. De rechter-commissaris stelt degene tot wie het bevel is gericht in de gelegenheid te worden gehoord. De aanbieder tot wie het bevel is gericht is bevoegd zich bij het horen door een raadsman te doen bijstaan. De mogelijkheid van een mondeling bevel lijkt niet goed te verenigen met deze procedurele eisen. Met het oog op een afgewogen oordeelsvorming door de rechter-commissaris, en daarmee een zorgvuldige toepassing, acht de regering een schriftelijke machtiging gewenst.

Artikel II, onderdeel G

Artikel 126nba

De leden van de SP-fractie hebben gelezen dat voor de bevoegdheid om te kunnen hacken vereist is dat het geautomatiseerde werk bij de verdachte in gebruik is en hebben gevraagd of het ook kan gaan om

werken waar door de verdachte gebruik van is gemaakt of dat vereist is dat de verdachte er nog steeds gebruik van maakt.
Met het vereiste dat het geautomatiseerde werk in gebruik is bij de verdachte wordt bedoeld dat de verdachte gebruik maakt van het geautomatiseerde werk. Hiermee is beoogd de reikwijdte van de bevoegdheid te beperken, doordat deze niet kan worden ingezet in een geautomatiseerd werk dat niet bij de verdachte in gebruik is, teneinde gegevens te verzamelen over de betrokkenheid van de verdachte bij het beramen of plegen van ernstige strafbare feiten. Niet is vereist dat de verdachte ten tijde van de toepassing van de bevoegdheid van het binnendringen feitelijk van het geautomatiseerde werk gebruik maakt. Met de aanduiding «een geautomatiseerd werk dat bij de verdachte in gebruik is» is dus tevens bedoeld het geautomatiseerde werk waarvan de verdachte gebruik heeft gemaakt.

De leden van de SP-fractie hebben geconstateerd dat de officier van justitie moet onderbouwen waarom het nodig is dat onderzoek in een geautomatiseerd werk plaatsvindeten hebben gevraagd of ook wordt onderbouwd waarom een alternatief niet ingezet kan worden. Ook hebben zij gevraagd of bovendien wordt aangegeven hoe groot de kans is dat de privacy van niet-verdachten wordt geschonden en dus inzage kan worden verkregen in meer gegevens dan nodig voor het opsporingsonderzoek en zo nee, waarom niet.
Zoals eerder, naar aanleiding van vragen van de leden van de SP-fractie aan de orde is gekomen, worden met de voorwaarde dat het onderzoek dit dringend vordert, de vereisten van (proportionaliteit en) subsidiariteit expliciet in de wet vastgelegd. Het subsidiariteitsvereiste strekt ertoe dat de officier van justitie kan onderbouwen waarom een alternatief niet kan worden ingezet. Ook mag, in die gevallen waarin dit aan de orde is, van de officier van justitie worden verwacht dat deze aan kan geven in hoeverre gegevens van derden zijn betrokken en op welke wijze de software wordt ingezet zodat wordt voorkomen dat kennis wordt genomen van andere gegevens dan welke van belang zijn voor het inzicht in de betrokkenheid van de verdachte bij het beramen of plegen van ernstige strafbare feiten.

De leden van de SP-fractie hebben gevraagd of er strengere eisen worden gesteld aan stelselmatige observatie dan aan eenmalig onderzoek doen in een geautomatiseerd werk.
Het binnendringen van een geautomatiseerd werk is uitsluitend mogelijk met het oog op het verrichten van bepaalde onderzoekshandelingen. Dit kan de stelselmatige observatie betreffen, waarbij het geautomatiseerde werk wordt gebruikt als peilbaken om de locatie van het werk, en daarmee van de gebruiker, te bepalen. Dit is in het bijzonder aan de orde bij het gebruik van mobiele apparaten als laptops of smartphones. De wettelijke voorwaarden voor de inzet van de onderzoekshandelingen zijn echter gedifferentieerd. Voor de stelselmatige observatie, het aftappen van communicatie en het direct afluisteren van communicatie is een strafbaar feit vereist waarvoor voorlopige hechtenis mogelijk is. Voor het overnemen van gegevens en het ontoegankelijk maken van gegevens is een misdrijf vereist waarvoor een gevangenisstraf van ten minste acht jaar kan worden opgelegd of dat bij algemene maatregel van bestuur is aangewezen.

De leden van de CDA-fractie delen volledig de zorgen van de nationale politie ten aanzien van de keuze om enkel in te grijpen bij systemen die bij de verdachte in gebruik zijn en hebben gevraagd of het in het kader van een effectieve opsporing en dus in de geest van onderhavig wetsvoorstel niet van belang is een stap voor te kunnen zijn op de digitale crimineel dan wel maximaal een stap achter te lopen. Ook hebben zij gevraagd of

het wetsvoorstel wel voldoende rekening houdt met criminelen die bewust verschillende apparaten gebruiken als dekmantel voor politie en justitie.
Zoals eerder aan de orde is gekomen, is de voorgestelde bevoegdheid tot het op afstand heimelijk binnendringen in een geautomatiseerd werk noodzakelijk om de ontwikkeling van de cybercrime het hoofd te kunnen bieden. De bevoegdheden van politie en justitie hebben geen gelijke tred gehouden met deze ontwikkeling, daarom dienen deze bevoegdheden te worden aangepast. De regering heeft ernaar gestreefd te komen met een afgewogen voorstel waarin rekening wordt gehouden met alle belangen, ook die van de burgers die wel gebruik maken van internet maar die niet betrokken zijn bij strafbare feiten. Het bewust gebruiken van verschillende geautomatiseerde werken door criminelen op zich heeft geen invloed op de mogelijkheid van het onderzoek in een geautomatiseerd werk van de betreffende personen, omdat die verschillende apparaten bij de verdachte in gebruik zijn. Wel zal dit gebruik de toepassing van de bevoegdheid in de praktijk kunnen bemoeilijken vanwege de noodzaak van een zorgvuldige voorbereiding voor ieder geautomatiseerd werk, waarbij rekening wordt gehouden met de specifieke situatie rond het geautomatiseerde werk met het oog op het op afstand binnendringen.

De leden van de CDA-fractie hebben opgemerkt dat het gebruik van een apparaat van een partner of huisgenoot voor de politie nog wel te voorzien zal zijn maar hebben gevraagd hoe het zit met een verdachte die afwisselend gebruik maakt van verschillende computers in bijvoorbeeld internetcafés en bibliotheken. Deze leden hebben tevens gevraagd of het wetsvoorstel hiermee wel voldoende inspeelt op de het uitlenen en uitwisselen van telefoons in vriendengroepen en familiekringen en zouden hierop graag een reactie vernemen en desgewenst aanpassing van het wetsvoorstel.
De voorwaarde dat het geautomatiseerde werk in gebruik is bij de verdachte betekent dat het op grond van feiten of omstandigheden aannemelijk moet zijn dat de verdachte gebruik maakt van het geautomatiseerde werk. Niet is vereist dat de verdachte de enige gebruiker is, voldoende is dat het geautomatiseerde werk ook door de verdachte wordt gebruikt. Zoals hierboven, naar aanleiding van vragen van de leden van de SP-fractie aan de orde is gekomen zal de officier van justitie in voorkomende gevallen moeten kunnen aangeven op welke wijze de onderzoekshandelingen worden verricht zodat zoveel mogelijk wordt voorkomen dat kennis wordt genomen van de gegevens van derden. Voor wat betreft het afwisselend gebruik van verschillende geautomatiseerde werken, zoals bijvoorbeeld computers van een internetcafé of van familieleden vormen niet zozeer de wettelijke criteria een belemmering als wel het feitelijk binnendringen in het geautomatiseerde werk, dat een zorgvuldige voorbereiding en uitvoering vergt. Het behoeft nauwelijks betoog dat dit wordt bemoeilijkt als afwisselend gebruik wordt gemaakt van verschillende geautomatiseerde werken.

Artikel II, onderdeel U

Artikel 126ee

De leden van de SP-fractie vinden het belangrijk dat eisen worden gesteld aan de software maar maken zich zorgen over de controle voorafgaand aan en tijdens de inzet en hebben gevraagd hoe dit wordt gewaarborgd en wie deze controle op zich zal nemen. Ook hebben zij gevraagd of dat wordt gedaan door de Autoriteit Persoonsgegevens en zo nee, waarom niet.
De controle op de werking van de software vindt plaats door middel van een technische keuring, voorafgaand aan de inzet. Alleen wanneer de

software is gecontroleerd en gecertificeerd mag het worden ingezet. Tevens worden alle handelingen die verricht worden ter uitvoering van het bevel van de officier van justitie automatisch vastgelegd op de politieserver, dit wordt ook wel logging genoemd. Het voorgestelde artikel 126nba, zevende lid, Sv, geeft een grondslag voor regeling bij algemene maatregel van bestuur. Het besluit dat ter uitvoering van het wetsvoorstel wordt opgesteld zal regels bevatten over de logging. De logging dient het mogelijk te maken om zowel tijdens het onderzoek als achteraf te controleren of het tijdens het onderzoek vergaarde bewijs betrouwbaar en integer is. Zoals eerder, in paragraaf 2.6, naar aanleiding van vragen van onder meer de leden van de PvdA-fractie aan de orde is gekomen, zal toezicht op de uitvoering van de voorgestelde bevoegdheid van het onderzoek in een geautomatiseerd werk worden uitgeoefend door de Inspectie VenJ. De Inspectie VenJ is een rijksinspectie en is op grond van de wet reeds belast met het toezicht op de kwaliteit van de taakuitvoering door de politie. Dit geldt niet voor de Autoriteit Persoonsgegevens, die is belast met het toezicht op de naleving van de privacywetgeving.

Artikel II, onderdeel X

Artikel 552a

De leden van de SP-fractie hebben gelezen dat de regering het minder wenselijk vindt om te voorzien in een schadevergoedingsprocedure indien na beklag is gebleken dat ontoegankelijkmaking niet rechtmatig was en hebben gevraagd waarom dit minder wenselijk is. Nu de betrokkene wordt gedwongen tot een langdurige en dure civiele procedure terwijl reeds is komen vast te staan dat er in strijd met de wet is gehandeld pleiten deze leden net als de Rvdr dus voor een afzonderlijke schadevergoedingsprocedure.
Het Wetboek van Strafvordering kent thans regelingen voor de vergoeding van specifieke vormen van schade. Dit betreft bijvoorbeeld de mogelijkheid van schadevergoeding na een onterecht voorarrest (art. 89 Sv). Het wetboek kent geen regeling voor andere vormen van strafvorderlijke schade, zoals schade die is ontstaan door de inbeslagneming van voorwerpen, een huiszoeking of de toepassing van een bijzondere opsporingsbevoegdheid. Ditzelfde geldt voor een maatregel als de ontoegankelijkmaking van gegevens. Indien het beklag van de belanghebbende tegen de ontoegankelijkmaking wordt toegewezen, worden de gegevens weer ter beschikking van de belanghebbende gesteld. Het lijkt weinig aannemelijk dat het ontoegankelijk maken van de gegevens zal leiden tot op geld waardeerbare schade bij de betrokkene, zodat een schadevergoedingsprocedure in veel gevallen niet aan de orde is. Voor die bijzondere gevallen waarin een betrokkene wel schade leidt, kan op grond van het burgerlijk recht een procedure worden gestart. In het kader van het onderzoek naar een algemene schadevergoedingsregeling zal nog wel worden bezien of en in hoeverre het passend is om ook deze bevoegdheid onder die algemene regeling te laten vallen.

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