34588 Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)

Nr. Nota naar aanleiding van het verslag

Inhoudsopgave

I. ALGEMEEN DEEL

Met belangstelling heb ik kennis genomen van de vragen en opmerkingen van de leden van de fracties van de VVD, PvdA, SP, CDA, D66, GroenLinks, ChristenUnie en SGP met betrekking tot het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Ik ben de leden van de vaste commissie voor Binnenlandse Zaken erkentelijk voor het feit dat zij, hoewel het hierbij gaat om een vrij omvangrijk en ingrijpend wetsvoorstel, op korte termijn na indiening van het wetsvoorstel een verslag hebben uitgebracht. Met de Tweede Kamer[1] ben ik van oordeel dat een voortvarende, maar tegelijkertijd ook zorgvuldige, totstandkoming van deze nieuwe wet van groot belang is om de Nederlandse inlichtingen- en veiligheidsdiensten van een bij de tijd gebracht instrumentarium te voorzien om het hoofd te bieden aan de vele dreigingen van onze nationale veiligheid, maar wel onder gelijktijdige versterking van de noodzakelijke waarborgen ter bescherming van de in het geding zijnde grond- en mensenrechten van de burgers. De voorziene versterking van het toezichts- en klachtstelsel verdient in dit kader speciale vermelding. Graag ga ik hieronder, mede namens de Minister-president, Minister van Algemene Zaken, de Minister van Defensie en de Minister van Veiligheid en Justitie op de gestelde vragen en gemaakte opmerkingen in. Bij de beantwoording is de volgorde van het verslag zoveel als mogelijk gevolgd. Waar dat dienstig werd geacht zijn vragen samengenomen en gebundeld beantwoord. Gelijktijdig met de nota naar aanleiding van het verslag wordt een nota van wijziging uitgebracht.

De leden van de GroenLinks-fractie hebben de regering gevraagd om per nieuw gecreëerde bevoegdheid aan te geven waarom deze bevoegdheid noodzakelijk en proportioneel is in het kader van de bescherming van de veiligheid. De enige nieuw gecreëerde bevoegdheid is die welke onderzoeksopdracht gerichte interceptie op de kabel mogelijk maakt. Bij de beantwoording van de vragen in paragraaf 3.3.3.3.5.1 van het verslag wordt nader ingegaan op de noodzakelijkheid en proportionaliteit van deze bevoegdheid.

De leden van de GroenLinks-fractie voorzien dat de voorgestelde wet veel consequenties zal hebben op het gebied van ICT en verzoeken de regering dan ook het onderhavige wetsvoorstel voor te leggen aan het Bureau ICT-toetsing (BIT). Ik zie daartoe geen reden. Het BIT is opgericht om te adviseren over ICT-projecten met een ICT-component van tenminste vijf miljoen euro. Nu het hier een wetsvoorstel betreft en geen ICT-project kan dit niet worden voorgelegd aan het BIT.

De leden van de SGP-fractie vragen zich – in navolging van de Afdeling advisering van de Raad van State – af of het bij deze grote omvang van de toelichting niet gewenst is te komen tot een duidelijker artikelsgewijze toelichting op het wetsvoorstel. In het nader rapport heb ik aangegeven waarom de keuze is gemaakt, zoals deze is gemaakt. Zoals daar is aangegeven gaat het bij onderhavig wetsvoorstel voor een aanzienlijk deel om complexe onderwerpen, waarbij een samenhangend betoog in al zijn aspecten aangewezen is geacht. Daardoor bleef relatief weinig over voor de artikelsgewijze toelichting. Niettemin is het een terecht aandachtspunt, waarmee rekening zal worden gehouden bij de voorbereiding van nieuwe wetsvoorstellen.

[1] Kamerstukken II 2016/17, 29 754, nr. 400.

1. Inleiding

De leden van de CDA-fractie vragen zich – mede in het licht van de conclusies en aanbevelingen van de Algemene Rekenkamer in het rapport Bezuinigingen en intensiveringen bij de AIVD (2015) – af welke consequenties de uitbreiding van bevoegdheden van de diensten zal hebben voor het benodigde budget, de formatie en de kennis en kunde van medewerkers van de diensten. Het budget bij de diensten wordt uitgebreid met 20 miljoen euro structureel ten einde mede te kunnen voorzien in de benodigde formatie, kennis en kunde bij de medewerkers van de diensten. Hiermee worden de diensten voorbereid op de inzet van de nieuwe bevoegdheden.

Deze leden vragen zich voorts af of de diensten zijn voorbereid op de inzet van nieuwe bevoegdheden en op welke wijze deze worden ingepast in het bestaande instrumentarium van de diensten. De bevoegdheden – die overigens al grotendeels tot het instrumentarium van de diensten behoren, maar ten aanzien van de inzet daarvan in onderhavig wetsvoorstel is voorzien in aanvullende waarborgen - zullen een onderdeel gaan vormen van het pakket aan mogelijkheden van de inlichtingen- en veiligheidsdiensten dat bij de taakuitvoering kan worden ingezet. Per specifieke inlichtingenbehoefte zal telkens afgewogen worden welk bevoegdheid het beste ingezet kan worden met inachtneming van de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.

1.1 Waarom de nieuwe wet?

De leden van de D66-fractie wijzen op de brief van de regering van 29 september 2015 (Kamerstuk 33 989, nr. 8), waarbij de Tweede Kamer is verzocht om de plenaire behandeling van het herzieningsvoorstel voor artikel 13 Grondwet aan te houden in afwachting van de afronding van de besluitvorming met betrekking tot de uitkomst van de consultatiefase van het voorstel van wet op de inlichtingen- en veiligheidsdiensten. Volgens deze leden wordt daarmee gesuggereerd dat de regering eerst de bevoegdheid voor de inlichtingen- en veiligheidsdiensten wil regelen, en daarna de grondwettelijke waarborgen ten aanzien van het brief- en communicatiegeheim daarop aanpast. Zou het juist niet andersom moeten zijn: de wet volgt de grondwet. De regering heeft inderdaad dat verzoek gedaan en ik constateer dat de Kamer daarin heeft bewilligd. In het grondwetsvoorstel wordt onder meer de beperkingsystematiek met betrekking tot het brief- en communicatiegeheim geregeld, waarbij een specifieke voorziening is getroffen voor zover de nationale veiligheid in het geding is. Daarmee bestaat er een inhoudelijke samenhang met het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten (Wiv) die in het oog gehouden moest worden. Voor zover met het verzoek de schijn is gewekt dat de regering voornemens zou zijn geweest de Grondwet aan te passen aan de regeling in de nieuwe Wiv, wil ik hier aangegeven dat dat geenszins de bedoeling is geweest. Overigens heeft de regering recent de Kamer laten weten dat nu het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten is ingediend, de behandeling van het hier bedoelde grondwetsvoorstel zou kunnen worden voortgezet.[2]

[2] Kamerstukken II 2016/17, 33 989, nr. 9.

Deze leden vragen voorts hoe de regering beziet dat de diensten – in de opgave om gegeven de geheime aard van hun werk toch vertrouwen te behouden – zo minimaal mogelijk, en alleen indien daar een goede rechtvaardiging voor bestaat, inbreuk maken op onze (grond)rechten? Het onderhavig wetsvoorstel biedt aan de diensten een adequaat en toekomstvast scala aan bevoegdheden om onderzoek te doen naar - gekende en ongekende - dreigingen voor onze nationale veiligheid en daaromtrent belangendragers te informeren. De uitoefening van deze bevoegdheden is onderworpen aan diverse wettelijk vastgelegde eisen waaraan moet worden voldaan en welke er juist mede toe strekken om de door de diensten te maken inbreuk op de aan de burgers toekomende grondrechten tot het strikt noodzakelijke te beperken. Daarbij zijn de grondwettelijke- en internationaalrechtelijke (EVRM) eisen die daaraan gesteld moeten worden uiteraard van essentieel belang geweest. In dit kader moet onder meer gedacht worden aan het toestemmingsregime (veel bevoegdheden zijn onderworpen aan ministeriële toestemming en in een aantal gevallen aan toestemming door de rechter), de verplichte toets aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, de rechtmatigheidstoets door de nieuwe Toetsingscommissie inzet bevoegdheden (TIB) voorafgaand aan de uitoefening van bevoegdheden, de plicht om zo snel mogelijk tot datareductie te komen enz. Voorts is voorzien in een – ten opzichte van de huidige situatie - versterkt toezicht- en klachtstelsel. Zo wordt de burger een laagdrempelige klachtvoorziening geboden, waarbij voorzien is in bindende klachtoordelen.

De leden van de D66-fractie constateren dat bij de lancering van het voorliggende wetsvoorstel een infographic over technische ontwikkelingen en de onrust in de wereld is gemaakt. Deze leden vragen zich af welke suggestie de regering met deze infographic heeft willen wekken en welk verband er is tussen de gepresenteerde technologische ontwikkelingen en de dreigingen. In aanvulling daarop stellen zij nog enkele vragen. Ik reageer daar als volgt op. De infographic met als titel ‘de nieuwe realiteit’ illustreert de noodzaak van modernisering van de Wiv 2002. Het is een hulpmiddel in de communicatie over het wetsvoorstel en maakt daar als zodanig geen onderdeel vanuit. De afbeelding benoemt een aantal ontwikkelingen in relatie tot het internet, zoals de komst van sociale netwerken, chat-apps en de exponentiele groei van data. Voorts illustreert het de onzekerheid en complexiteit op het gebied van veiligheid. Er is sprake van een toegenomen dreiging. Er is geen suggestie van een causaal verband tussen deze ontwikkelingen noch van volledigheid. De Wiv 2002 werd opgesteld lang voordat de wetgever de impact van bijvoorbeeld smartphones of de omvang van anonieme wifispots kon voorzien. Door de komst van toepassingen zoals bijvoorbeeld de smartphone, met de bijbehorende internetconnectiviteit, kan momenteel in steeds mindere mate de inlichtingenpositie worden bereikt die bijvoorbeeld voor een antipiraterijmissie nabij Somalië is benodigd. Feit is dat de som aan technische ontwikkelingen grote gevolgen heeft voor het inlichtingenwerk in binnen- en buitenland. Kwaadwillenden kunnen zich eenvoudig voordoen als iemand anders, schuil gaan in een anoniem netwerk, real-time strijders aansturen of een aanval plannen duizenden kilometers ver van Nederland. De technologische ontwikkelingen, voornamelijk in het kabelgebonden domein, in combinatie met het dreigingsbeeld stellen de diensten voor grote uitdagingen. Het feit dat de opstellers van de huidige wet nooit rekening hebben kunnen houden met deze nieuwe realiteit, is een belangrijke reden om de Wiv 2002 te herzien.

1.2 De balans modernisering bevoegdheden-grondrechtelijke waarborgen

1.2.1 Transparantie (§1.2.2 m.v.t.)

De leden van de D66-fractie lezen dat de regering maximale transparantie betracht over de inzet van de nieuwe bevoegdheid tot onderzoeksopdrachtgerichte interceptie (OOG-interceptie), maar constateren dat er niets wordt gezegd over het openbaar maken van geaggregeerde statistieken. Dat is nu niet het geval. Deze leden vragen zich af of ten aanzien van de OOG-interceptie wel samengevoegde data openbaar zal worden gemaakt en of vervolgens ook het beleid ten aanzien van de huidige tapstatistieken zal worden gewijzigd. Indien één van deze vragen met nee wordt beantwoord, dan vragen de leden zich af hoe zij er dan vertrouwen in kunnen hebben dat de beloofde transparantie daadwerkelijk betracht zal worden? Voor wat betreft de (on)wenselijkheid van het openbaar maken van kwantitatieve gegevens inzake de inzet van de bevoegdheid van gerichte interceptie en inzake de inzet van de bevoegdheid tot selectie van sigint, verwijs ik naar mijn brief van 7 oktober 2014 aan de voorzitter van de Tweede Kamer waarmee ik het toezichtsrapport van de CTIVD over de inzet van de afluisterbevoegdheid en de bevoegdheid tot selectie van sigint door de AIVD (CTIVD-rapport nr. 40) aan uw Kamer aanbood.[3] Hierin gaf ik aan dat het openbaar maken van dergelijke informatie inzicht in de modus operandi van de AIVD biedt en derhalve in strijd is met de geheimhoudingsplicht van artikel 15 van de Wiv 2002. Uw kamer heeft de motie van het lid Koser Kaya om deze informatie alsnog, respectievelijk voortaan, openbaar te laten maken door de AIVD en de CTIVD op 29 september 2016 verworpen. Vanzelfsprekend worden de aantallen volledig gedeeld met het parlement via het geëigende kanaal: de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD). Teneinde ook de transparantie over big data-verwerkingen te vergroten zet de regering in op het robuuster maken van twee instrumenten, te weten het Jaarplan van de AIVD en MIVD en capacitaire uitbreiding van het onafhankelijke toezicht door de CTIVD. Het Jaarplan van de AIVD en van de MIVD zijn vanwege hun inhoud staatsgeheim en worden integraal gedeeld met de Commissie voor de Inlichtingen- en Veiligheidsdiensten. Wel worden deze op hoofdlijnen openbaar gemaakt en aan het parlement aangeboden. De hoofdlijnen kunnen onder de aandacht van burgers worden gebracht op de website van de AIVD en de MIVD. De CTIVD kan op elk gewenst moment onderzoek doen naar de uitvoering van onderzoeksopdrachtgerichte interceptie en hierover in het openbaar rapporteren.

1.2.2 Niet-relevante data worden vernietigd(§1.2.4 m.v.t.)

De leden van de PvdA-fractie geven aan dat zij kennis hebben genomen van de zienswijze van de CTIVD met betrekking tot het voorliggende wetsvoorstel en van de conclusie van de CTIVD dat, waar het gaat om onder andere de verwerking en analyse van grote hoeveelheden data die er na de inwerkingtreding van deze wet beschikbaar komen, de in het voorliggende wetsvoorstel voorziene waarborgen onvoldoende zijn. In haar zienswijze heeft de CTIVD in het kader van "verantwoorde databeperking" aanbevolen een aantal nadere waarborgen op te nemen, waaronder het vereiste dat de inzet van bevoegdheden "zo gericht mogelijk"moet zijn. De PvdA-fractie geeft aan dergelijke waarborgen bijna vanzelfsprekend te vinden en vraagt of daar reeds op een andere wijze dan de CTIVD om vraagt al in is voorzien, en zo niet of daar alsnog in kan worden voorzien.
Ten aanzien van de door de CTIVD genoemde waarborg om in de wet op te nemen dat de inzet van bevoegdheden "zo gericht mogelijk" moet zijn, kan worden bevestigd dat

[3] Kamerstukken II 2014/15, 29 924, nr. 116.

dit een waarborg is welke reeds voortvloeit uit de wettelijke vereisten. Voor de inzet van elke bijzondere bevoegdheid zullen de diensten moeten afwegen of hetzelfde doel kan worden bereikt met de inzet van een minder inbreuk makende bevoegdheid. Deze afweging zal ook in de motivering van het verzoek om instemming voor inzet van de bijzondere bevoegdheid tot uitdrukking moeten komen. De CTIVD merkt daarbij overigens terecht op dat genoemde eis niet noodzakelijkerwijs hoeft te leiden tot een keuze voor de meest gerichte bevoegdheid. Zo kan bijvoorbeeld, omdat de inzet van de meest gerichte bevoegdheid tot een grotere inbreuk op de privacy leidt, toch worden gekozen voor de inzet van een andere bijzondere bevoegdheid.
Voor het overige kan worden opgemerkt dat het wetsvoorstel een groot aantal waarborgen bevat met betrekking tot de verwerking van gegevens, waaronder begrepen verworven gegevens. De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en voor zover dat noodzakelijk is voor een goede uitvoering van de wet. De verwerking dient te geschieden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze. Gegevens die worden verwerkt, moeten zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing te bevatten naar het document of de bron waaraan de gegevens zijn ontleend. Daarnaast is limitatief vastgelegd op welke categorieën personen de verwerking van persoonsgegevens betrekking mag hebben. De AIVD en de MIVD moeten door middel van inzet bijzondere bevoegdheden verkregen gegevens zo spoedig mogelijk op relevantie onderzoeken. Gegevens die niet relevant zijn, moeten worden vernietigd. Gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren, worden verwijderd en vernietigd. Op de hoofden van de diensten rust de plicht te zorgen dat de personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens de wet is bepaald. Het gebruik van data is dan ook met het onderhavige wetsvoorstel aan strikte wettelijke regels gebonden.

Verder, zo merken de leden van de PvdA-fractie op, is de CTIVD van mening "dat het beperkte betekenis [heeft] een motivering gekoppeld aan toestemming en onafhankelijke toetsing aan de voorkant van het proces te eisen. Men weet immers vaak op voorhand nog niet naar wie en wat men precies zoekt. Een dergelijk systeem van waarborgen vooraf krijgt vooral inhoud bij de gerichte inzet van bevoegdheden bij een gekende dreiging, waarbij een persoon of organisatie al in beeld is". De leden van de PvdA-fractie delen de mening dat ook tijdens de fase van verwerking en analyse van deze grote hoeveelheden data er waarborgen moeten zijn in die "fase van het gegevensverwerkingsproceswaar de (privacy)inbreuk daadwerkelijk plaatsvindt, te weten tijdens de geautomatiseerde bewerkings-, analyse- en gebruiksfase". De leden van de PvdA-fractie zouden de regering dan ook willen vragen te reageren op de stelling van de CTIVD dat er een wettelijke zorgplicht voor geautomatiseerde gegevensverwerking moet komen. Die moet inhouden dat de diensten door middel van een bij wet vastgelegd instrumentarium verantwoording afleggen over de kwaliteit van de geautomatiseerde gegevensverwerkingsprocessen en dat hierop effectief toezicht kan worden gehouden. De CTIVD is van mening dat een dergelijke zorgplicht zich zou moeten uitstrekken "tot de kwaliteit van de gegevensvergaring, van de gebruikte gegevens(bestanden), van de toe te passen algoritmes en modellen en tot de kwaliteit van de resultaten van deze processen". Hierover moeten de diensten verantwoording afleggen (compliance). De toezichthouder is daarmee in staat effectief te toetsen of geautomatiseerde gegevensverwerking rechtmatig plaatsvindt en hierover te rapporteren aan de Kamer.

De leden van de PvdA-fractie geven aan dat zij de mening van de CTIVD delen dat ook tijdens de fase van verwerking en analyse van grote hoeveelheden data er waarborgen moeten zijn. De leden van de PvdA-fractie vragen of de regering wil reageren op de stelling van de CTIVD dat er een wettelijke zorgplicht voor geautomatiseerde gegevensverwerking moet komen.

Naar aanleiding van hetgeen door de leden van de PvdA-fractie is gesteld en mede gelet op hetgeen onder meer door de CTIVD in haar zienswijze er zake is gesteld, ben ik tot de conclusie gekomen dat er in een vorm van een zorgplicht dient te worden voorzien. In de nota van wijziging heb ik daartoe ook een voorstel opgenomen, waarbij artikel 24, tweede lid, onderdeel a, van het wetsvoorstel wordt aangepast. Deze zorgplicht houdt in dat de hoofden van diensten dienen zorg te dragen voor de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt alsmede ter bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen. Nu het begrip gegevensverwerking diverse handelingen en processen omvat, is het naar mijn mening niet noodzakelijk om daarvan enkele specifiek te benoemen. Er is afgezien van een aparte zorgplicht voor de bevordering van de kwaliteit van de gegevens. Er bestaat immers reeds een zorgplicht om de juistheid en de volledigheid van de gegevens te bevorderen; daarnaast bestaat de plicht de gegevens die door de diensten worden verwerkt te voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend (zie artikel 18, derde lid, van het wetsvoorstel). Naar mijn oordeel dient hiermee te worden volstaan. De wettelijke verankering van de voorgestelde (uitbreiding van de) zorgplicht biedt naar mijn oordeel de CTIVD voldoende handvatten om op de uitwerking daarvan binnen het kader van de aan haar opgedragen taak daarop toe te zien.

De leden van de PvdA vragen tot slot of het noodzakelijk is dat meer vormen van geautomatiseerde data-analyse als bijzondere bevoegdheid worden aangemerkt met de daarbij passende waarborgen.
Ik zie geen aanleiding om andere gevallen van geautomatiseerde data-analyse dan die welke het wetsvoorstel als bijzondere bevoegdheid aanmerkt, ook als bijzondere bevoegdheden aan te merken. In artikel 50, eerste lid, onder b, jo. vierde lid van het wetsvoorstel is opgenomen dat in het geval van metadata-analyse, gericht op het identificeren van personen of organisaties, ten aanzien van de in het kader van onderzoeksopdrachtgerichte interceptie verzamelde gegevens, ministeriële toestemming met bindend oordeel van de toetsingscommissie inzet bevoegdheden vereist is. Hiermee dient naar mijn mening te worden volstaan. Om daarnaast overige activiteiten in de fase tussen verwerving en verstrekking te kwalificeren als bijzondere bevoegdheid, acht ik niet noodzakelijk. Deze activiteiten zijn gericht op het helder krijgen van correlaties tussen data. Als voor al deze verwerkingsprocessen toestemming aan de minister en aan de toetsingscommissie inzet bevoegdheden moet worden gevraagd, wordt de slagkracht van de diensten aangetast en kan onvoldoende worden geborgd dat dreigingen tijdig worden onderkend. De toezichthouder CTIVD kan gedurende het hele proces de rechtmatigheid van de verwerving, verwerking en verstrekking beoordelen.

1.2.3 Taakgebondenheid en proportionaliteit (§1.2.6 m.v.t.)

De leden van de D66-fractie lezen dat inzet van bevoegdheden door de AIVD en MIVD moet voldoen aan de vereisten van proportionaliteit, subsidiariteit en doelgerichtheid. Deze leden vragen zich af of de regering kan uitsluiten dat alle communicatie in een bepaalde Nederlandse wijk of buurt voor een bepaalde periode wordt geïntercepteerd om zo te bezien of voor de diensten relevante gegevens zijn binnengehaald. Het intercepteren van alle communicatie in een bepaalde Nederlandse wijk of buurt voor een bepaalde periode om zo te bezien of voor de diensten relevante gegevens zijn binnengehaald zal in geen geval de toetsing aan de wettelijke vereisten als proportionaliteit en subsidiariteit kunnen doorstaan. Een inzet om dergelijke redenen sluit ik uit. Een nadere verduidelijking van hetgeen in dit kader onder ' relevante' gegevens wordt verstaan, waarnaar deze leden vragen, kan naar mijn mening dan ook verder achterwege blijven.

1.3 Waarom modernisering van bevoegdheden?

De leden van de VVD-fractie vragen zich af hoe onderzoeksopdrachtgerichte interceptie gaat bijdragen aan de veiligheid van onze uitgezonden militairen en aan de snelheid waarmee een beeld kan worden opgebouwd van de veiligheidssituatie in een gebied waar onze militairen naar toe uitgezonden worden? Ik beantwoord deze vragen graag als volgt. De directe omgeving van het NAVO-verdragsgebied en de EU kenmerkt zich door een toenemende dreiging, onzekerheid en complexiteit, waardoor het belang om nieuwe (hybride) dreigingen vroegtijdig te onderkennen toeneemt. De komende jaren zal naar verwachting een groter beroep worden gedaan op de Nederlandse krijgsmacht om het hoofd te bieden aan crises aan de randen van het eigen (verdrags)grondgebied. Toekomstige defensie-operaties zullen plaatsvinden in een hoog risico-omgeving met een onvoorspelbaar geweldsspectrum. Het tijdig opbouwen van een adequate inlichtingenpositie over deze gebieden is cruciaal voor de veiligheid van uitgezonden eenheden. Onderzoeksopdrachtgerichte interceptie biedt een cruciale aanvulling op reeds bestaande inlichtingenmiddelen voor de opbouw van een inlichtingenpositie over (mogelijke) inzet- of operatiegebieden waar weinig informatie over beschikbaar is en waar de meer traditionele inlichtingenmiddelen een langere opbouwfase kennen alvorens opbrengst te genereren.
Door toegang tot de kabel kunnen de diensten ongekende dreigingen beter achterhalen en targets volgen die nu welbewust onder de radar blijven. Het is ten opzichte van enige jaren geleden zonder deze toegang niet mogelijk een kwalitatief gelijkwaardige informatiepositie te bereiken. Relevante datastromen zijn naar de kabel verplaatst of hebben zich daar ontwikkeld. Zelfs in crisisgebieden vormen allerhande internettoepassingen de command and control infrastructuur van tegenstanders. Het per definitie uitsluiten van zicht op deze communicatie is een risico voor de effectiviteit van de operatie en de veiligheid van onze militairen.
Toegang tot de kabel is ook noodzakelijk voor een goede eigenstandige informatiepositie van Nederland. Internationale samenwerking is en blijft belangrijk, maar eigenstandig gegevens verwerven, verwerken en analyseren is een must voor onafhankelijke oordeelsvorming, onder meer in relatie tot besluitvorming rondom militaire missies en de veiligheidssituatie aan de grenzen van Europa.
Militaire operaties kenmerken zich door een grote dynamiek in de veiligheidssituatie en inzet met een lange adem. De snelheid waarmee de diensten moeten kunnen optreden is hoger dan ooit. Snel informatie correleren, valideren of een informatiepositie opbouwen is van levensbelang. Wanneer het kabelgebonden domein uit het zicht blijft van de

diensten, is het tijdig en structureel realiseren van een hoogwaardige inlichtingenpositie in afnemende mate mogelijk.
De krijgsmacht werkt in internationale coalities en voert gezamenlijke militaire operaties uit. Ook op inlichtingengebied is sprake van een gemeenschappelijke inspanning en de uitwisseling van gegevens. Omdat artikel 27 van de Wiv 2002 kabelinterceptie niet toestaat, kunnen de diensten op dat terrein thans niet internationaal samenwerken; een U-bocht constructie is immers uiteraard – nu en in de toekomst - niet toegestaan. Voor een geslaagde missie en een zo veilig mogelijke inzet van militairen is het van belang dat de MIVD ook met betrekking tot het kabelgebonden domein kan samenwerken.

De leden van de VVD-fractie lezen het volgende in de Defensie Cyber strategie: "Om voldoende armslag in het digitale domein te krijgen is modernisering van de Wiv noodzakelijk. Toegang tot kabelgebonden telecommunicatie is een voorwaarde om cyberdreiging vroegtijdig te kunnen onderkennen en inlichtingen te kunnen verzamelen over de aard van de dreiging." Deze aan het woord zijnde leden zouden hier graag een toelichting op hebben. Door verregaande digitalisering en beschikbaarheid van sensoren neemt de beschikbaarheid van informatie die verwerkt of beschermd moet worden toe. Dit levert nieuwe kansen en bedreigingen op voor de Nederlandse krijgsmacht. Het biedt kansen, zowel ter versterking van het strategisch anticiperend vermogen als voor de vergroting van de operationele effectiviteit. Tegelijk ontstaan in het digitale domein ook dreigingen. De MIVD onderkent op wekelijkse basis pogingen tot digitale inbreuken bij Defensie, toeleveranciers van Defensie en bondgenoten. Deze (pogingen tot) spionage en/of manipulatie verlopen veelal via kabelgebonden netwerken. Ook de zogenoemde exfiltratie van verkeer, dus de data die aanvallers na succesvolle aanvallen ontvreemden, vindt plaats via kabelgebonden netwerken. Zonder gemoderniseerde capaciteiten zal de MIVD steeds minder effectief (digitale) inlichtingen kunnen verzamelen, verwerken en verspreiden ten behoeve van de krijgsmacht en de internationale rechtsorde. Sinds het verschijnen van de Defensie Cyber Strategie in 2012 is de veiligheidscontext ingrijpend veranderd en zijn ook cyberdreigingen fors toegenomen (zie het Cyber Security Beeld Nederland 2016). De beleidsbrief Internationale Veiligheid van het kabinet (Kamerstuk 33 694 nr.6) onderstreepte dat cyberdreigingen – die zich veelal via kabelgebonden infrastructuren manifesteren – juist ook in deze nieuwe veiligheidscontext als één van de belangrijkste aandachtsgebieden voor de toekomst moeten worden beschouwd. Krijgsmachten en inlichtingendiensten van bijvoorbeeld Rusland en China ontwikkelen in hoog tempo capaciteiten voor digitale spionage, manipulatie van datastromen, information warfare en digitale middelen om zich heimelijk te nestelen in (industriële) controlesystemen voor sabotagedoeleinden. Staten maken in toenemende mate gebruik van het digitale domein om hun (geopolitieke) doelstellingen te verwezenlijken. Bovendien is ook de Nederlandse samenleving in het cyberdomein een mogelijk doelwit van terroristische activiteiten. Voor Defensie is cyberspace het vijfde domein voor militair optreden geworden (naast land, zee, lucht en de ruimte). In hedendaagse statelijke en niet-statelijke conflicten zijn aanvallen op de digitale infrastructuur een gegeven. Ook Defensie is in hoge mate afhankelijk van de goede werking van digitale systemen. Voorts gebruiken strijdende partijen, zoals nu ISIS het internet als command and control systeem, als rekruteringsmiddel en voor propaganda. Defensie, als zwaardmacht, ook in het digitale domein, kan dit niet negeren. De MIVD moet inzicht en handelingsperspectief bieden ten aanzien van (potentiële) conflicten en relevante ontwikkelingen. Aangezien cyberspace voor het overgrote deel bestaat uit een kabelgebonden infrastructuur, moet de dienst over voldoende armslag beschikken in dit domein. Zoals ook door de Commissie Dessens

geconcludeerd, betekent dit dat de MIVD verkenningen met het oog op mogelijke militaire operaties moet kunnen uitvoeren en in het kader van vooraf geautoriseerde onderzoeksopdrachten toegang moet hebben tot kabelgebonden telecommunicatie. Attributie-onderzoek, dus wie er precies achter een aanval zit, hoe de uitvoering plaatsvindt, met welke intentie, kan alleen wanneer de diensten ook de data kunnen vergaren die daarvoor nodig is. Als niet kan worden vastgesteld waar vandaan een dreiging of aanval komt, zijn de mogelijkheden tot een effectieve respons beperkt. Attributie is benodigd voor het kunnen nemen van passende maatregelen (diplomatiek, militair, economisch etc.). Een wezenskenmerk van Defensie is het bieden van afschrikking tegen externe dreigingen. Het doeltreffend kunnen uitvoeren van attributie-onderzoek, waar kabeltoegang een belangrijke schakel in vormt, is een belangrijke voorwaarde om de afschrikkende rol ook in het digitale domein waar te maken.

De leden van de D66-fractie vragen de regering of zij het eens is met hun analyse dat er een verschil in inbreuk op de persoonlijke levenssfeer van mensen blijft bestaan tussen interceptie van communicatie die via de ether dan wel via de kabel verloopt. Doordat de huidige wet niet techniekonafhankelijk is terwijl de technologie zich onmiskenbaar heeft ontwikkeld, wordt de taakuitvoering van de diensten op dit ogenblik belemmerd zonder dat dit destijds de bedoeling van de wetgever was. De Commissie Dessens heeft daarom aanbevolen de Wiv 2002 techniekonafhankelijk te maken en de beperking in de wet tot «ongericht ontvangen en opnemen van «niet-kabelgebonden» telecommunicatie» op te heffen. Het kabinet heeft deze aanbeveling overgenomen (Kamerstukken II 2014/15, 33 820, nr. 4). De CTIVD heeft voorts in haar reactie op het rapport van de Commissie Dessens (brief van 11 maart 2014) onderstreept dat bij het vaststellen van de Wiv 2002 geen grondrechtelijke reden bestond waarom een bericht dat door de kabel gaat niet mag worden onderschept terwijl datzelfde bericht wel mag worden onderschept als het door de lucht gaat. Ik deel de opmerkingen en aanbevelingen van bovenstaande commissies en kom dus tot de conclusie dat er geen principieel verschil bestaat tussen interceptie van communicatie die via de ether dan wel via de kabel loopt.

1.3.1 Technologische ontwikkelingen (§1.3.2 m.v.t.)

De leden van de VVD-fractie vragen of een overzicht kan worden gegeven van (voorbeelden van) technologische ontwikkelingen die zich hebben voorgedaan sinds de Wiv 2002 en toe te lichten waarom de Wiv 2002 hier niet op toegerust is? Deze leden zouden graag willen weten wat de voordelen zijn van kabelgebonden interceptie. Het voorstel van de huidige wet is in 1998 aan de Tweede Kamer aangeboden en kreeg kracht van wet in 2002; op 29 mei 2002 trad de Wiv 2002 in werking. Sindsdien is onze manier van communiceren ingrijpend veranderd. Er heeft zich een ontwikkeling voorgedaan van klassieke telefonie naar digitale communicatie. Het internet is in deze tijd exponentieel gegroeid en biedt inmiddels een waaier aan communicatiediensten. In dit kader is in het bijzonder het op de markt verschijnen van de smartphone in 2007 van belang.
Net als ieder ander maken de targets van de diensten gebruik van een verscheidenheid aan communicatiemiddelen, zoals whats-app, telegram, snapchat, chatapplicaties in games en Skype-communicatie. De targets van de diensten wisselen daarbij doelbewust zoveel mogelijk van communicatiewijze om onder de radar te blijven.
Voor zogenaamde gerichte interceptie oftewel de inzet van de afluisterbevoegdheid is een tot de persoon herleidbaar kenmerk nodig waarmee de diensten zich kunnen wenden tot een aanbieder van een communicatiedienst. Dat is in de praktijk in

toenemende mate tijdrovend of onmogelijk gebleken, met steeds minder opbrengst. De inzet van gerichte interceptie is tijdrovend en gecompliceerd, omdat de diensten iedere keer dat een target wisselt van communicatiewijze zich moeten wenden tot een andere aanbieder van een communicatiedienst. De diensten kunnen zich in veel gevallen niet tot een aanbieder van een communicatiedienst wenden omdat targets bijvoorbeeld gebruik maken van aanbieders van communicatiediensten die zich in het buitenland bevinden of omdat de betreffende aanbieder van een communicatiedienst zelf niet bij de noodzakelijke gegevens kan. Zo lopen de diensten in toenemende mate achter de feiten aan en missen zij steeds meer de noodzakelijke snelheid en slagkracht.
Het wetsvoorstel maakt het mogelijk datastromen op de kabel te onderscheppen. Deze interceptie van de datastroom is noodzakelijk omdat een merendeel van de telecommunicatie zich sinds de invoering van de Wiv 2002 heeft verplaatst van de lucht naar kabelnetwerken, die de ruggengraat zijn gaan vormen van het digitale domein. Zoals aangegeven, heeft de snelle opkomst en mondiale verspreiding van digitale technologie en het internet vergaande gevolgen gehad voor de mogelijkheden van de diensten de noodzakelijke communicatie te onderscheppen. De diensten moeten in toenemende mate dreigingen inschatten op basis van een gefragmenteerd beeld van de communicatie van targets. Met kabelgebonden interceptie beogen de diensten het dreigend gevaar van afnemend zicht op de targets af te wenden.

Voor het cyberdomein is onderzoeksopdracht gerichte interceptie op de kabel voorts van bijzonder belang. Ten eerste kunnen signalen van digitale aanvallen met een potentiële impact op de nationale veiligheid vroegtijdig worden onderkend. Wanneer bijvoorbeeld uit inlichtingen de handelswijze van een bepaalde aanvaller kan worden bepaald, dan kan met behulp van kabelinterceptie gericht worden gezocht op kenmerken van deze aanvalsmethode waardoor toekomstige aanvallen snel kunnen worden gedetecteerd en erop vroegtijdig op kan worden gereageerd. Ten tweede kan wanneer een aanval onderkend en geanalyseerd is, onderzoek worden verricht naar andere slachtoffers (in Nederland). De specifieke kenmerken die zijn verkregen kunnen worden onderzocht met kabelinterceptie. Hieruit kan worden gedestilleerd welke bedrijven en instellingen nog meer zijn getroffen door deze aanvaller.

De leden van de D66-fractie vragen om meer onderbouwing bij de stelling dat de taakuitvoering van de diensten op dit moment ernstig belemmerd wordt zonder dat dit destijds de bedoeling van de wetgever was. Tevens vragen deze leden zich af waarom er zo lang gewacht is met het aanpassen van de Wiv en waarom de aanpassing zelf zo lang heeft geduurd. Daarbij vragen de aan het woord zijnde leden zich af hoe de verantwoordelijke regering heeft gereageerd op de zorgen van de diensten dat de taakuitvoering belemmerd wordt. Allereerst verwijs ik naar de reactie die ik hiervoor in antwoord op leden van de VVD-fractie heb gegeven, waarbij ik heb geschetst welke technologische ontwikkelingen zich hebben voorgedaan sinds de inwerkingtreding van de huidige wet. De diensten hebben hun zorgen over die ontwikkeling en de gevolgen die dat heeft voor hun onderzoeksmogelijkheden onder de aandacht van verantwoordelijke ministers gebracht. Die zorgen zijn uiterst serieus genomen. Een herziening van het wettelijke kader voor de activiteiten van de inlichtingen- en veiligheidsdiensten is echter geen eenvoudige opgave en kost – mede vanwege alle in het geding zijnde belangen – gewoonweg tijd. Er is immers een inherente spanning tussen enerzijds de democratische rechtsstaat en de daaraan ten grondslag liggende waarden en anderzijds het bestaan en functioneren van inlichtingen- en veiligheidsdiensten. Daar moet een juiste balans in gevonden worden. Daarbij komt dat, zoals bekend, op verzoek van de Tweede Kamer in

2013 de huidige wet is geëvalueerd door de Commissie Dessens. Het lag niet voor de hand om reeds een integrale herziening van de huidige wet ter hand te nemen, zolang de huidige wet werd geëvalueerd en de uitkomsten daarvan nog niet bekend waren. Aansluitend is naar aanleiding van het kabinetsstandpunt over het rapport van de Commissie Dessens met uw Kamer overleg gevoerd. Alles overziend is de voorbereiding van het wetsvoorstel dan ook naar mijn mening op een voortvarende manier ter hand genomen, waarbij bovendien is voorzien in internetconsultatie en de uitvoering van een Privacy Impact Assessment (PIA). Zoals ik ook in de inleiding van de nota naar aanleiding van het verslag heb aangegeven ben ik uw kamer erkentelijk voor het feit dat aan een voortvarende behandeling wordt meegewerkt, zodat op korte termijn in een vernieuwde en toekomstvaste wet kan worden voorzien.

De leden van de D66-fractie constateren dat de regering bij de behandeling van de 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) heeft aangegeven dat internettaps steeds minder nuttige informatie opleveren als gevolg van versleuteling. In dit kader vragen deze leden waarom de regering van mening is dat ongerichte internettaps door de diensten wel nuttige informatie kunnen opleveren. Vooraleerst wil ik benadrukken dat het wetsvoorstel niet voorziet in het mogelijk maken van "ongerichte internettaps", maar van onderzoeksopdrachtgerichte interceptie. In het kader van het wetsvoorstel computercriminaliteit III gaf de regering aan dat de inzet van bevoegdheden zoals een telefoon-, e-mail-, of internettap geen resultaat biedt in gevallen waarin gebruik wordt gemaakt van moderne versleuteling. In dergelijke gevallen worden slechts gegevens verkregen waaruit de inhoud van de communicatie niet kan worden afgeleid. De opsporing zou daarom dringend behoefte hebben aan de mogelijkheid om de communicatie te kunnen onderscheppen voordat deze wordt versleuteld of nadat deze is ontsleuteld.
De inlichtingen- en veiligheidsdiensten nemen een unieke positie in. Zij dienen onder meer proactief (nog) ongekende dreigingen te onderkennen die onze nationale veiligheid bedreigen. Deze taak wijkt af van het reguliere reactieve opsporingswerk. De analyse van historische gegevens, voornamelijk zogenoemde metadata, is daarbij voor de inlichtingen- en veiligheidsdiensten een van de cruciale instrumenten. Essentiële metadata kunnen worden verkregen door de (onderzoeksopdracht)gerichte interceptie van communicatie waarvan de inhoud zelf versleuteld is.
Versleuteling van de inhoud van communicatie vormt ook voor de inlichtingen- en veiligheidsdiensten een uitdaging bij de vervulling van hun wettelijke taken. De opbrengst van de inzet van bevoegdheden gericht op het onderscheppen van communicatie over het internet rechtvaardigt deze inzet evenwel nog steeds. Daarnaast wijs ik op de bevoegdheid van de diensten om de encryptie in specifieke gevallen te doorbreken. Het staken van de inzet van deze bevoegdheden vanwege de mogelijkheid dat encryptie verhindert dat kennisgenomen kan worden van bepaalde informatie, acht ik niet verantwoord.

De leden van de ChristenUnie vragen zich af op welke wijze de Kamer zal worden geïnformeerd over de ontwikkelingen in het gebruik van de bepalingen rond interceptie van data nu het voorliggende wetsvoorstel techniekneutraal is vormgegeven. Het gebruik van nieuwe technologische toepassingen vond ook al plaats bij de meer techniek afhankelijke geformuleerde Wiv 2002. Een terecht zorgpunt zou zijn dat de diensten sinds 2002 geen gebruik gemaakt zouden hebben van nieuwe technologische

toepassingen bij de inzet van bijzondere bevoegdheden. Het toezichtsrapport van de CTIVD naar aanleiding van haar onderzoek naar de inzet van de afluisterbevoegdheid en van de bevoegdheid tot selectie van sigint door de AIVD (CTIVD-toezichtsrapport nr. 46) bijvoorbeeld, hierna ook aangehaald door de leden van de D66-fractie, bewijst dat de huidige toezichtspraktijk en toepassing van benodigde waarborgen al sinds 2002 functioneert. De toegepaste techniek is door de toezichthouder onderkend, de wijze waarop de toepassing feitelijk wordt gebruikt is onderzocht door de toezichthouder, over de toepassing is zowel in het openbaar als in de beslotenheid gerapporteerd aan de Tweede Kamer en de met de toepassing gepaard gaande aanvullende waarborgen zijn overgenomen in de werkwijze van de diensten. Deze leden vragen ten slotte of dit een bijzonder aandachtspunt moet zijn in het toezicht wat de CTIVD uitvoert op de uitoefening van de bevoegdheden. Ik onderschrijf de mening van de leden van de ChristenUnie-fractie dat de ontwikkelingen in het gebruik van de bepalingen rond interceptie van data een bijzonder aandachtspunt zouden moeten zijn van het toezicht van de CTIVD. Uiteraard is het aan de CTIVD zelf om te bepalen waarnaar zij binnen haar wettelijke taken onderzoek uitvoert.

1.3.2 Terroristische dreiging en ondersteuning krijgsmacht (§1.3.3 m.v.t.)

De leden van de D66-fractie vragen de regering om in een alinea en voor een ieder begrijpelijke taal uit te leggen wat gerechtvaardigde redenen zijn om een inbreuk te maken op iemands persoonlijke levenssfeer. Een inbreuk op de persoonlijke levenssfeer kan enkel worden gepleegd nadat is voldaan aan de wettelijke vereisten die de wet stelt aan deze inbreuk. De inbreuk moet noodzakelijk zijn voor de taakuitvoering van de diensten. Zo vereist de veiligheidstaak van de AIVD (de a-taak) dat een persoon of organisatie enkel kan worden onderzocht indien de doelen die zij nastreven, dan wel hun activiteiten aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat. Tevens dient de inzet van de bevoegdheid in verhouding te staan tot het doel en dient een qua privacy inbreuk lichter middel niet voorhanden te zijn. Voorts mag een bevoegdheid niet lager worden ingezet dan voor het bereiken van het doel noodzakelijk is. De uitoefening van een bevoegdheid moet voldoen aan diverse procedurele waarborgen. Een bevoegdheid kan niet eerder worden ingezet dan nadat op een verzoek om toestemming, waarin naast de zaken die uit artikel 29, tweede lid, van het wetsvoorstel voortvloeien ook is uiteengezet op welke wijze het verzoek voldoet aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, toestemming is verkreen op het juiste, door de wet aangegeven, niveau.

De aan het woord zijnde leden vragen zich daarnaast af of het mogelijk is dat jouw communicatie als bijvangst wordt verworven, verwerkt en/of geanalyseerd, hoe snel er dan in elk van deze stadia wordt achterhaald dat jouw data overbodige bijvangst zijn en tenslotte wat er vervolgens met deze date gebeurt. In het inlichtingen- en veiligheidsdomein is het verwerven van bijvangst onvermijdelijk. Dat geldt voor de klassieke middelen: indien met een camera de voordeur van een huis in de gaten wordt gehouden, dan registreert die camera ook talloze voorbijgangers. Ook bij onderzoeksopdrachtgerichte interceptie is het mogelijk dat de communicatie van een persoon op wie de interceptie zich niet richt wordt vergaard. Zodra dit wordt vastgesteld, schrijft de wet voor dat deze informatie niet verder wordt gebruikt, maar verwijderd en vernietigd.

1.3.3 Cybersecurity (§1.3.4. m.v.t.)

De leden van de D66-fractie vragen de regering om op technisch- en beleidsmatig niveau toe te lichten hoe dit wetsvoorstel het verminderen van cyberaanvallen gaat bewerkstelligen? In het antwoord op de vraag van de leden van de VVD-fractie bij paragraaf 1.3.1 heb ik toegelicht waarom onderzoeksopdrachtgerichte interceptie op de kabel een belangrijk middel is dat de bijdrage aan de veiligheid van Nederland en haar krijgsmacht in het cyberdomein aanzienlijk verhoogt.

Deze leden vragen de regering voorts of zij het met hen eens is dat het dichten (in plaats van het openhouden) van softwarekwetsbaarheden, het stimuleren van bedrijven om veiligere software te maken (bijvoorbeeld via software aansprakelijkheid), het investeren in goede cyberhygiëne, voorlichting om digitale vaardigheden onderdeel te maken van het curriculum en het stimuleren van hackers om kwetsbaarheden bij de maker van de software te melden, de beste manieren zijn om cyberaanvallen tegen te gaan? Ik onderschrijf dat de door de aan het woord zijnde leden genoemde maatregelen, van het wegnemen van kwetsbaarheden zoals in de brief over zero days is aangegeven tot aan de diplomatieke aanpak van cyberaanvallen, kunnen helpen (de effectiviteit van) cyberaanvallen te verminderen. Hierop wordt reeds ingezet door de Nederlandse regering. Echter zeker tegen zogenoemde advanced persistent threats van statelijke actoren is het niet afdoende en dienen inlichtingen- en veiligheidsdiensten op de wijze zoals hierboven beschreven te voorzien in de verdediging van het cyberdomein.

1.3.4 Internationale verantwoordelijkheid (§1.3.6 m.v.t.)

De leden van de D66-fractie delen met de regering dat het een bijzondere nationale verantwoordelijkheid met zich meebrengt dat Nederland een internationale hub voor datacommunicatie is, maar vrezen tegelijkertijd dat het voor onze regering en onze diensten erg verleidelijk wordt die "pot snoep" te openen. In die zin vragen deze leden zich af hoe de titel van deze paragraaf moet worden begrepen: een internationale verantwoordelijkheid om het internet veilig en vrij van technische ingrepen te laten zijn, of een internationale verantwoordelijkheid om data te 'oogsten' waar 'wij' goed bij kunnen en die dan te ruilen of te delen met andere landen. Ik wil graag op voorhand wegnemen dat de inlichtingen- en veiligheidsdiensten gericht zijn op een 'pot snoep' of het 'oogsten van data'. Voor een dergelijke benadering biedt het wetsvoorstel geen ruimte. Een dergelijk beeld komt ook zeker niet naar voren uit de rapporten van de CTIVD. Met het nemen van internationale verantwoordelijkheid wordt bedoeld dat het kabinet alles in het werk stelt om te voorkomen dat de Nederlandse infrastructuur wordt misbruikt door kwaadwillenden voor bijvoorbeeld het faciliteren van digitale aanvallen of het beramen van terroristische aanslagen.

Deze leden vragen de regering op welke wijze, anders dan met dit wetsvoorstel, zij aandacht besteedt aan een goede cyberpositie van Nederland. Nederland wil het digitale domein niet uitleveren aan kwaadwillende hackers en anderen die de digitale veiligheid bedreigen. Uw Kamer heeft op 22 november jl. de motie van het lid Belhaj (Kamerstukken II 2016/17, 34 550 X, nr. 35) aangenomen, waarin de regering wordt verzocht werk te maken van het versneld aantrekken van cyberreservisten bij Defensie. Conform de motie zal de regering de Kamer hierover informeren bij de Voorjaarsnota 2017. Voor de wijze waarop de regering aandacht geeft aan een goede cyberpositie, verwijs ik u naar de Nationale Cyber Security Strategie 2 en het bijbehorend

Actieprogramma 2014-2016 (26 643, nr. 291) en naar het jaarlijks onder coördinatie en verantwoordelijkheid van de staatssecretaris van Veiligheid en Justitie opgestelde Cyber Security Beeld Nederland en bijbehorende beleidsreactie (26 643, nr. 420, 5 september 2016).

1.4 Nadere achtergronden bij de ontwikkelingen die dit wetsvoorstel noodzakelijk maken

1.4.1 De dreiging die we niet kennen (§1.4.3 m.v.t.)

De leden van de D66-fractie vragen de regering nader toe te lichten hoe de analogie van het "waterfilter van het internet" waarover zij spreekt in de memorie van toelichting moet worden begrepen. Het filter is de selectie van bepaalde communicatie uit de te intercepteren datastroom. Stel dat de diensten weten dat persoon A vanuit Raqqa contact zoekt met geradicaliseerde personen in Nederland. Indien de datastroom tussen Raqqa en Nederland in interceptie kan worden gezet, dan kan op basis van technische kenmerken de communicatie behorend bij persoon A door middel van selectie uit de datastroom worden gefilterd.

1.5 Hoe heeft de regering het wetsvoorstel voorbereid?

De leden van de D66-fractie geven aan met grote belangstelling kennis te hebben genomen van de zienswijze van de CTIVD. Zij wijzen erop dat de CTIVD aanzienlijke fundamentele bezwaren plaatst bij het wetsvoorstel. Deze leden vragen of de regering de zienswijze van de CTIVD deelt? Ik deel de zienswijze van de CTIVD op veel punten (zoals versterking van de zorgplicht en de aanvulling wegingscriteria bij aangaan samenwerkingsrelatie met buitenlandse diensten, die in de nota van wijziging zijn opgenomen). Met het wetsvoorstel is naar mijn mening een goede balans is gevonden tussen uitoefening van de bevoegdheden enerzijds en bescherming van privacy en andere grondrechten anderzijds, waardoor de eventuele risico's van onderzoeksopdrachtgerichte interceptie worden ondervangen en goed toezicht mogelijk is op geautomatiseerde gegevensverwerking. Waar het gaat om het door de CTIVD opgebrachte punt van de rechtseenheid, verwijs ik naar hetgeen ik hierover verderop in deze nota ter zake opmerk.

Deze leden vragen voorts of de CTIVD tijdens het vormgeven van het wetsvoorstel haar zienswijze reeds naar voren heeft kunnen brengen. De CTIVD is – evenals de Nationale ombudsman – gevraagd om te reageren op het ontwerpwetsvoorstel zoals dat in consultatie is gegeven. Daarvan heeft zij gebruik gemaakt. In paragraaf 12.2 van de memorie van toelichting is uitvoerig ingegaan op de diverse in het kader van de consultatie uitgebrachte reacties, ook die van de CTIVD, en ook in hoeverre de diverse reacties aanleiding hebben gegeven om het wetsvoorstel aan te passen. Kortheidshalve wordt daarnaar verwezen. Voorts heeft de CTIVD indertijd een uitvoerige reactie op het advies van de Commissie Dessens gegeven. De leden van de fractie van D66 vragen voorts waarom bij het opstellen van het wetsvoorstel er niet voor is gekozen deze cruciale waarborgen die de CTIVD naar voren brengt meteen in het voorliggende wetsvoorstel op te nemen. Van de opmerkingen van de CTIVD hebben we telkens goede nota genomen en waar dat aan de orde was meegenomen bij de voorbereiding van het wetsvoorstel.

1.6. Wat verandert er met het nieuwe wetsvoorstel?

Door de leden van de fractie van de VVD is gevraagd of toegelicht kan worden hoe de werkwijze van de TIB en de ministeriële verantwoordelijkheid tot elkaar verhouden. Op deze kwestie is ook door de Afdeling advisering van de Raad van State ingegaan. In lijn met hetgeen in reactie daarop is gesteld, merk ik hierover het volgende op. De keuze voor een bindende toets door de TIB op een eerder door de voor de dienst verantwoordelijke minister verleende toestemming voor de inzet van een bijzondere bevoegdheid, doet naar mijn mening niet af aan de ministeriële verantwoordelijkheid. De beslissing om een onderzoek te starten door een van de diensten valt onder de volledige verantwoordelijkheid van de voor de dienst verantwoordelijke minister; dat is niet een besluit dat uitsluitend een juridisch oordeel vereist, maar samenhangt met beleidsmatige afwegingen. Die beslissing is niet onderworpen aan een toets van de TIB noch aan het rechtmatigheidstoezicht door de CTIVD. Het vervolgens uitvoeren van het onderzoek brengt met zich mee dat – afhankelijk van de onderzoeksvraag, de onderzoeksmogelijkheden e.d. - overgegaan dient te worden tot de inzet van bijzondere bevoegdheden. Daarvoor zal – tenzij er is voorzien in de mogelijkheid van mandaat – de toestemming van de minister dienen te worden verkregen. Daartoe wordt aan de minister een verzoek om toestemming te worden voorgelegd, waarbij door de diensten zal dienen te worden onderbouwd dat de inzet van de desbetreffende bijzondere bevoegdheid niet alleen noodzakelijk is, maar ook dat deze proportioneel (evenredigheid doel en middel) en subsidiair (van de beschikbare middelen het middel dat de minste inbreuk maakt). Uiteindelijk zal de gemaakte keuze voor de inzet van de bijzondere bevoegdheid de rechtmatigheidstoets dienen te doorstaan. Het gaat hier immers om toepassing van wettelijk vastgelegde eisen. Voor het uiteindelijk genomen besluit tot inzet van de bijzondere bevoegdheid – ook ingeval dat in mandaat is genomen - is de betreffende minister volledig verantwoordelijk. Voor zover er vervolgens een toets door de TIB wordt vereist, is dat een toets die door de wetgever in dit proces is voorzien. De wetgever aanvaardt en beoogt daarmee, dat indien de minister – naar het oordeel van de TIB - niet in staat is om de rechtmatigheid van een besluit (noodzaak, proportionaliteit en subsidiariteit) te onderbouwen, de uitoefening van een bijzondere bevoegdheid waarmee inbreuk op iemands grondrechten kan worden gemaakt, achterwege dient te blijven. De minister kan, ingeval de TIB de door de minister verleende toestemming onrechtmatig acht en deze daarmee komt te vervallen, overwegen een nieuw besluit nemen, waarbij gepoogd kan worden de door de TIB geconstateerde gebreken op het vlak van rechtmatigheid (zoals onvoldoende noodzaak aangetoond, disproportioneel of een te zwaar middel als er een lichter middel voorhanden is) weg te nemen. Of hij dat doet is zijn beslissing en ook daar is hij volledig voor verantwoordelijk; dus ook voor het nalaten daarvan. Uiteraard is de minister volledig verantwoordelijk voor de uiteindelijke uitvoering van de bijzondere bevoegdheid door de dienst.

Naar aanleiding van de vraag van de VVD of de TIB in staat zal zijn te oordelen over overwegingen rondom buitenlands beleid, bijvoorbeeld inzake het plaatsen van een tap, kan het volgende worden opgemerkt. De toestemming welke aan de TIB ter toetsing wordt voorgelegd, wordt verleend op basis van een door de betrokken dienst opgestelde motivering. In die motivering wordt ingegaan op aspecten als proportionaliteit en subsidiariteit en voorts waarom de uitoefening van de betreffende bijzondere bevoegdheid noodzakelijk is in het kader van een bepaald onderzoek passend binnen de

taakomschrijving en passend binnen de Geïntegreerde Aanwijzing. In die motivering zal dus afdoende moeten worden ingegaan op het onderzoek en waarom het op het buitenland gerichte onderzoek en de betreffende bijzondere bevoegdheid noodzakelijk is in het licht van de taakomschrijving en de Geïntegreerde Aanwijzing.

Tenminste twee van de drie leden van de TIB, waaronder de voorzitter, dienen tenminste zes jaar een rechterlijke functie te hebben vervuld en zijn dus ook bij uitstek geschikt in het afwegen van alle betrokken belangen. Verwacht mag daarom worden dat de leden van de TIB alle argumenten (en dus ook de genoemde noodzakelijkheidsafweging) op hun waarde zullen weten te schatten.
Voorts kan nog worden opgemerkt dat ingevolge het wetsvoorstel een derde lid in de TIB kan worden benoemd, die beschikt over technische deskundigheid en inzicht in veiligheidsrisico's. Hiermee wordt ook nog de specifieke inbreng van deze deskundigheid in de toets geborgd.

1.7 Wat gaan wij nu wel en niet doen in de praktijk?

De leden van de D66-fractie lezen dat er geen sprake van zal zijn dat een fors deel van de telecommunicatie van Nederlanders zal worden opgeslagen. Opslaan is, aldus deze leden, echter iets anders dan een tap op de kabel plaatsen om te bezien of op basis van een negatief filter data ter verwerving (en later verwerking en analyse) binnengehaald moeten worden. Zij vragen of opslaan in deze zin dient te worden geïnterpreteerd en, zo nee, waarom niet. Het antwoord op deze vraag is nee. Er is geen sprake van een tap op de kabel. In de antwoorden in de paragraaf over onderzoeksopdrachtgerichte interceptie (3.3.3.3.5) van deze nota wordt hier uitgebreid op ingegaan. Kort weergegeven betreft interceptie een specifieke datastroom die over enkele fibers van een kabel loopt. Van deze datastroom wordt op basis van uiterlijke kenmerken een groot deel van de data (via negatieve filters) afgebogen, zodat deze niet bij de diensten terechtkomt. Na deze reductie wordt data opgeslagen: de volledige resterende metadata en de inhoud enkel indien deze voldoet aan bepaalde (positieve) filters. Deze filters worden vastgesteld op basis van toestemming van de minister, waarop nog een rechtmatigheidstoets voor de TIB plaatsvindt.

Deze leden vragen wat de regering onder het begrip "bulk" verstaat en vraagt om hiervan een exacte definitie te geven uitgedrukt in hoeveelheid megabytes of in hoeveel personen wiens data daarin besloten ligt. Vanwege de onbepaaldheid ervan wordt het begrip 'bulk' niet in de wet, doch enkel in de memorie van toelichting gebruikt. In de wet wordt onderscheid gemaakt tussen geëvalueerde en ongeëvalueerde gegevens. De laatste categorie betreft gegevens die nog niet op relevantie voor de taakuitvoering zijn onderzocht. Een definitie in aantallen megabytes of personen acht ik in dit kader niet zinvol.

Daarnaast herinneren deze leden zich de Wet precursoren voor explosieven (Kamerstuk 34 289), waarin een meldingssysteem besloten zit voor verdachte verkopen van kunstmest. Deze leden begrijpen echter aan de hand van hetgeen in deze toelichting gesteld wordt, dat mocht er een grote hoeveelheid kunstmest verkocht worden aan, of ontvreemd door, een onbekend persoon, dat desondanks niet voor een daartoe relevant gebied bezien zal worden of, en zo ja wie, gecommuniceerd heeft over kunstmest (waarna ten behoeve van de verwerking onderscheid gemaakt kan worden tussen

landbouwers en degenen die niet in die zin beroepshalve dergelijke stoffen nodig hebben). Klopt dat?
Het verwerven van communicatie met als doel te bezien welke mensen op zoek zijn naar kunstmest kan nooit reden zijn om onderzoeksopdrachtgerichte interceptie in te zetten. De wet biedt geen basis voor het door de leden van D66 geschetste voorbeeld. Het verwerven van inlichtingen over ongekende dreigingen wordt niet op deze wijze ingevuld.

2. De diensten en de coördinatie tussen de diensten

De leden van de CDA-fractie merken op dat de Commissie Dessens in haar rapport heeft aangegeven dat de rol van de coördinator van de inlichtingen- en veiligheidsdiensten onvoldoende uit de verf komt. Zij vragen of de door de Commissie Dessens gesignaleerde problemen met betrekking tot de rol van de coördinator met het voorliggend wetsvoorstel zijn ondervangen.Ik verwijs voor wat betreft de beantwoording van deze vraag de leden van de CDA-fractie naar hetgeen hierna in paragraaf 2.2 van deze nota is gesteld.

2.1 De taken van de diensten (§2.2 m.v.t.)

De leden van de D66-fractie waarderen dat er een wettelijke grondslag voor het verrichten van "naslagen" in het voorliggende wetsvoorstel is opgenomen. Zij wijzen er terecht op dat de uitwerking daarvan, blijkens de artikelen 8, tweede lid, onder f, en 10, tweede lid, onder g, van het wetsvoorstel, plaatsvindt bij ministeriële regeling, Zij vragen of meer inzicht kan worden gegeven in de voorgenomen kring van personen die bevoegd is tot het doen van een verzoek tot naslag en ten aanzien van welke personen en onder welke omstandigheden dat verzoek kan worden gedaan. De hier bedoelde ministeriële regeling is in voorbereiding en zal in ieder geval de huidige praktijk van naslag, zoals onder meer kenbaar uit toezichtsrapporten van de CTIVD, codificeren. De inhoud van de ministeriële regeling is thans onderwerp van interdepartementaal overleg. Deze leden vragen voorts aan wie een instemmingsverklaring als bedoeld in artikel 63, tweede lid, onder b, gevraagd zal worden en hoe wordt bepaald wanneer dit de effectiviteit van het onderzoek als bedoeld in het derde lid zou kunnen schaden. Het vragen van een instemmingsverklaring is de norm. Enkel indien op voorhand verwacht kan worden dat het vragen van instemming de effectiviteit van het uitvoeren van het verzoek schaadt, bijvoorbeeld omdat het leidt tot vertraging die een gevaar voor het te beschermen belang betekent, kan hiervan worden afgezien. In de door deze leden geschetste casus zal het van de omstandigheden van het geval afhangen of een naslag gewenst is, hetgeen ter beoordeling aan de Minister-president, minister van Algemene Zaken is. Dat geldt evenzeer voor het antwoord op de vraag of wel of niet een instemmingsverklaring kan worden gevraagd.
De leden van de D66-fractie vragen ten slotte hoe vaak op dit moment naslag wordt verricht. Er worden nu door de AIVD zo'n 38.000 per jaar uitgevoerd. Ruim 99 % daarvan betreft naslagen naar aanleiding van de aanvraag van een nationaal visum. Voor de MIVD gaat het om enkele tientallen naslagen per jaar. Daarnaast worden de AIVD en MIVD incidenteel verzocht om in het kader van een specifiek evenement, zoals de National Security Summit in 2014, de aangemelde bezoekers na te slaan. Dit betreft enkele duizenden naslagen per keer.

2.2 De coördinatie van de taakuitvoering (§2.4 m.v.t.)

De leden van de SGP-fractie vragen zich af wat de precieze taak wordt van de coördinator. In paragraaf 2.2.1 van deze nota worden de vragen die deze leden ter zake stellen, in samenhang met de andere vragen van deze leden waar het gaat om de Geïntegreerde Aanwijzing (GA) beantwoord, zodat kortheidshalve daarnaar wordt verwezen.

2.2.1 Geïntegreerde aanwijzing (§2.4.3 m.v.t.)

De leden van de SGP-fractie vragen zich, onder verwijzing naar het voorstel van de Commissie Dessens om de rol van coordinator bij een driemanschap van de SG-en van AZ, Def en BZK te beleggen, af wat de precieze taak wordt van de coördinator. Daarbij vragen deze leden zich af in hoeverre het logisch is om deze taak bij een ander ministerie te beleggen dan een ministerie dat primair betrokken is bij de (nationale) veiligheid. In dit verband vragen de leden zich tevens af in hoeverre het logisch is om naast de Commissie Veiligheids- en Inlichtingendiensten (CVIN) nog een afzonderlijke coördinator te hebben. Deze leden vragen zich in dit kader af of het niet logischer zou zijn om deze CVIN te laten gelden als coördinerend orgaan, waarbij dan een voorzittersrol is weggelegd voor de coördinator vanuit Algemene Zaken. Tevens vragen de aan het woord zijnde leden zich af hoe de prioritering in de GA zich verhoudt tot de specifieke onderzoeksopdrachten door beide ministeries. De secretaris-generaal van het ministerie van Algemene Zaken (SG AZ) heeft het door de Commissie Dessens gesignaleerde probleem met betrekking tot de rol van de coördinator reeds binnen de WIV 2002 opgepakt. Op verzoek van de SG AZ heeft de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) plaats genomen in het Comité Verenigde Inlichtingendiensten Nederland (CVIN). De secretaris-generaal van het ministerie van Defensie is lid van het CVIN en heeft feitelijke deelname, doorgaans gemandateerd aan de Hoofddirectie Beleid.

Sinds 2015 wordt vooruitlopend op de nieuwe wet door de AIVD en MIVD gewerkt op basis van een Geïntegreerde Aanwijzing Inlichtingen- en Veiligheid. Hiervan maakt de voorheen separaat bestaande aanwijzing inlichtingentaak buitenland onderdeel uit. De geïntegreerde aanwijzing wordt opgesteld door een integraal overzicht van de behoeftes, zoals aangegeven door de behoeftestellers, af te zetten tegen de bij de diensten beschikbare capaciteit, waarna op ministerieel niveau in de Raad Inlichtingen en Veiligheid (RIV), onder voorzitterschap van de minister-president de weging van prioriteiten en toedeling van capaciteit wordt vastgesteld.
Het ambtelijk voorbereiden van een dergelijke aanwijzing vindt onder voorzitterschap van de coördinator van de inlichtingen- en veiligheidsdiensten plaats. De coördinator vervult hierbij een coördinerende rol tussen enerzijds de diensten (AIVD en MIVD) en anderzijds de behoeftestellers: het ministerie van Buitenlandse Zaken (BZ), het ministerie van BZK, het ministerie van Veiligheid en Justitie (V&J) en het ministerie van Defensie. De coördinator draagt zorg voor het goed verlopen van de informatie-uitwisseling tussen de betrokken partijen die verantwoordelijkheid dragen voor de veiligheid in Nederland en voor de veiligheid van Nederland(ers) in het buitenland. Naast de in de geïntegreerde aanwijzing opgenomen thema's hebben de inlichtingen- en veiligheidsdiensten capaciteit beschikbaar voor ad hoc verzoeken van de ministeries zoals bijvoorbeeld Requests for Information (RFI's). Gedurende het jaar draagt de coördinator er zorg voor dat de diensten periodiek rapporteren over de uitvoering van de geïntegreerde aanwijzing aan het CVIN en vervolgens aan de RIV. Indien de

ontwikkelingen noodzaken tot een heroverweging van in de geïntegreerde aanwijzing vastgelegde afspraken vindt nader overleg plaats op voorstel van de coördinator en/of op verzoek van de betrokken diensten in het CVIN, waarna zo nodig voorstellen ter besluitvorming aan de RIV worden voorgelegd. Voorts wordt vanuit het CVIN onder voorzitterschap van de coördinator waar relevant voorstellen gedaan aan de RIV voor eventuele beleidsmatige opvolging van inlichtingen van de inlichtingen- en veiligheidsdiensten.
Sinds maart 2015 vindt wekelijks een overleg plaats tussen de minister-president, de viceminister-president, de ministers van BZ, BZK, Defensie en V&J en de inlichtingen- en veiligheidsdiensten, NCTV en de politie over actuele kwesties die de nationale veiligheid of veiligheid van Nederlanders in het buitenland betreffen.
Alles bijeen kan derhalve gesteld worden dat de afgelopen jaren naar aanleiding van het advies van de Commissie Dessens intensiever inhoud is gegeven aan de rol van coördinator van de inlichtingen en veiligheidsdiensten. Die versterkte rolopvatting sluit goed aan bij de bij alle betrokken organisaties reeds gevoelde noodzaak om intensief en zo goed mogelijk samen te werken, gelet op de ernstige bedreigingen van onze veiligheid.
In onderhavig wetsvoorstel is de actieve coördinerende rol, die de SG AZ vervult, verder verduidelijkt en daarmee de thans goed lopende praktijk verankerd. Het toedelen van de coördinerende rol aan een orgaan, zoals door de leden van de SGP-fractie geopperd, zie ik niet als een verbetering ten opzichte van de huidige wijze van werken.

3. De verwerking van gegevens door de diensten

3.1 Algemeen

De leden van de PvdA-fractie vragen de regering of het juist is te veronderstellen dat de verzameling van bulkgegevens en de verdere verwerking en analyse daarvan een grote inzet en kennis van personeel zal vergen, of de diensten daar goed op zijn voorbereid en waaruit dat dan blijkt. Voor de beantwoording van deze vraag verwijs ik naar mijn eerdere antwoord op een soortgelijke vraag van de CDA-fractie in paragraaf 1 (Inleiding) van deze nota.

De leden van de SP-fractie lezen dat er geen verwerking plaatsvindt van gevoelige persoonsgegevens, waar het gaat om gegevens over godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid of seksueel leven. Deze leden vragen zich af waarom nationaliteit en burgerlijke staat hier niet onder vallen en waarom is gekozen voor de term "seksueel leven".
Noch in de huidige Wiv 2002 noch in andere bestaande wetten op het terrein van de verwerking van persoonsgegevens, zoals de Wet bescherming persoonsgegevens en de Wet politiegegevens, worden nationaliteit en burgerlijke staat als een gevoelig gegeven aan gemerkt. Maar ook in toekomstige Europese wetgeving op het terrein van verwerking van persoonsgegevens, te weten de Algemene verordening gegevensbescherming, worden nationaliteit en burgerlijke staat niet onder de bijzondere of gevoelige gegevens geschaard.
Naar aanleiding van de vraag van de SP-fractie waarom is gekozen voor de term "seksueel leven" merk ik op dat in de hier bovengenoemde wet- en regelgeving verschillende omschrijvingen worden gehanteerd. Bij het opstellen van het wetsvoorstel is er voor gekozen de bestaande terminologie uit de Wiv 2002 (welke aansluit bij de Wet bescherming persoonsgegevens en de Wet politiegegevens) te handhaven.

De leden van de SP-fractie vragen zich af waarom in artikel 25, tweede lid, van het wetsvoorstel, waarin is bepaald dat de betrokken minister een andere informatiebron als bedoeld in het eerste lid kan aanwijzen waaruit de dienst informatie kan verzamelen, niet is gekozen voor een wettelijke verankering en waarom er niet voor is gekozen om de TIB hier een rol in te geven. Uit oogpunt van toekomstbestendigheid van de wet is er voor gekozen deze mogelijkheid op te nemen. Het gaat bij artikel 25, eerste lid, om een algemene duiding van de type informatiebronnen waaruit de diensten kunnen putten, opgenomen naar aanleiding van een aanbeveling in de PIA. Zoals thans valt te overzien, dekt artikel 25, eerste lid, de lading. Niettemin valt niet uit te sluiten dat in de toekomst een nieuwe type informatiebron te raadplegen valt welke niet is beschreven in artikel 25, eerste lid. Om dan te voorkomen dat eerst artikel 25 moet worden aangepast alvorens van die informatiebron gebruikt kan worden gemaakt, is het tweede lid van artikel 25 opgenomen. Zoals ook in de memorie van toelichting is aangegeven, ligt het voor de hand vanuit de actieve inlichtingenplicht jegens het parlement dat deze omtrent een dergelijke beslissing wordt geïnformeerd. Voor alle duidelijkheid zij opgemerkt dat met artikel 25, tweede lid niet een nieuwe (nu nog niet te voorziene) bijzondere bevoegdheid in het leven kan worden geroepen. Daarvoor geldt nog steeds onverkort dat daarvoor eerst de wet moet worden gewijzigd. Zoals aangegeven gaat het in artikel 25 om een algemene duiding van de informatiebronnen. Het ligt dan ook niet in de rede om hier een rol te geven aan de Toetsingscommissie Inzet Bevoegdheden welke is belast met de toetsing van de door de betrokken minister verleende toestemmingen van een aantal ingrijpende bijzondere bevoegdheden.

De leden van de SP signaleren dat datamining en het gebruik van geautomatiseerde algoritmes afbreuk kan doen aan de betrouwbaarheid van gegevens en vragen of de regering wil reageren op de vraag waarom de aanbeveling in de PIA om een bepaling op te nemen in het wetsvoorstel over gegevensbescherming by design en by default niet is overgenomen.
De regering wijst op de algemene zorgplicht van de diensthoofden tot het bevorderen van technische, personele en organisatorische maatregelen. De zorgplicht in artikel 24 ten aanzien van de ontwikkeling van technische systemen legt een inspanningsverplichting bij de diensten neer om bij nieuw te ontwikkelen systemen ten behoeve van de verwerking van persoonsgegevens, waar mogelijk, zoveel mogelijk te handelen naar gegevensbescherming by design en by default. In artikel 24, tweede lid onder a, is opgenomen dat er voorzieningen door de diensten worden getroffen die de juistheid en volledigheid van gegevens die door de diensten worden verwerkt, bevorderd. Naar aanleiding van de zorgen die geuit zijn omtrent de geautomatiseerde gegevensverwerking door de diensten wordt via de nota van wijziging artikel 24, tweede lid, onderdeel a, uitgebreid, waardoor ook de kwaliteit van gegevensverwerking, waaronder de daarbij gehanteerde algoritmes en modellen, onder de wettelijke zorgplicht komen te vallen.

Bij het ontwerpen, aankopen en in gebruik nemen van technische systemen houden de diensten rekening met de beginselen van gegevensbescherming, zoals gegevensbescherming by design en by default. Gegevensbescherming by design houdt in dat de diensten bij de ontwikkeling van systemen het belang van privacy en gegevensbescherming inbouwen. Gegevensbescherming by default ziet erop dat systemen zo ontworpen en ingericht worden dat zo min mogelijk persoonsgegevens worden verwerkt.

Tot slot benadruk ik dat de CTIVD als onafhankelijke toezichthouder toegang heeft tot gegevensverwerkingsprocessen gedurende de gehele verwerkingscyclus. Als toezichthouder kan de CTIVD de rechtmatigheid van gegevensverwerking gedurende het gehele proces, inclusief het gebruik van algoritmes en modellen, beoordelen. Bovendien bestaat er altijd de mogelijkheid voor de CTIVD om medewerkers van de diensten om toelichting vragen. De voorgestelde aanpassing van de zorgplicht in artikel 24, tweede lid, onder a, zoals eerder in deze nota toegelicht, biedt de CTIVD aanvullende mogelijkheden om vanuit haar toezichtstaak toe te zien op de kwaliteit van de gegevensverwerking.

De leden van de SP-fractie lezen dat er een rechterlijke toets ingesteld wordt voor het gebruik van bevoegdheden bij journalisten en advocaten en vragen zich af waarom deze rechterlijke toets alleen bij advocaten en journalisten noodzakelijk en niet bij notarissen, artsen, geestelijken – en bijvoorbeeld ook bij Kamerleden? In het wetsvoorstel is inderdaad uitsluitend een specifieke regeling getroffen voor twee beroepsgroepen, te weten advocaten en journalisten, waarbij voorzien is in een rechterlijke toets. Zoals in paragraaf 3.3.2.5.3 van de memorie van toelichting is aangegeven, ligt aan de noodzaak tot het opnemen van een regeling voor de twee genoemde gevallen in beide gevallen een rechterlijke uitspraak ten grondslag. Voor het opnemen van een regeling voor andere beroepsgroepen (inclusief kamerleden), vergelijkbaar met die welke is getroffen voor journalisten en advocaten bestaat dan ook geen dwingendrechtelijke reden.

3.2 De algemene bepalingen inzake de verwerking van gegevens

3.2.1. Algemene eisen aan gegevensverwerking

De leden van de D66-fractie vragen de regering of zij het nodig acht via een wettelijke zorgplicht van de hoofden van de diensten vast te leggen dat er een schriftelijk gegevensbeschermingsbeleid komt en de nodige voorzieningen getroffen worden met betrekking tot het waarborgen van de kwaliteit en betrouwbaarheid van de gegevensvergadering, de gebruikte gegevens(bestanden), de toe te passen modellen, algoritmes, technieken en methode en de resultaten van de verwerking. Het lid Verhoeven heeft daartoe het amendement over de technische, personele en organisatorische maatregelen (Kamerstuk II 2016/17, 34 588, nr. 15) ingediend. Deze leden horen graag van de regering hoe zij, indien dit amendement aangenomen of overgenomen zou worden, invulling gaan gegeven aan dit gegevensbeschermingsbeleid. Ik heb eerder, naar aanleiding van een vergelijkbare vraag van de leden van de PvdA-fractie, aangegeven dat ik inmiddels van oordeel ben dat er inderdaad een vorm van een zorgplicht dient te worden opgenomen. Ik verwijs deze leden dan ook naar het gestelde in paragraaf 1.2.2 van deze nota.

De leden van de D66-fractie vragen zich voorts af welke standaarden de regering wil gaan hanteren voor de gebruikte modellen, algoritmes, technieken en de methode van verwerking, welke kans op fouten daarin bestaat en welke foutmarges de regering daarbij acceptabel acht. Ik wil hier als volgt op reageren. Uitkomsten van geautomatiseerde processen van gegevensverwerking vereisen gelet op het feit dat zij correlaties weergeven, en geen causale verbanden, altijd menselijke validatie of nadere weging. Het resultaat van de analyse is bovendien afhankelijk van de (kwaliteit van de) gehanteerde algoritmen en data. De mogelijkheid dat geautomatiseerde data-analyse

fouten kan bevatten die kunnen leiden tot verkeerde conclusies kan derhalve nooit worden uitgesloten.

Een belangrijke waarborg bij de geautomatiseerde verwerking van gegevens ligt in het vereiste van menselijke tussenkomst bij de geautomatiseerde data-analyse (artikel 60, derde lid, van het wetsvoorstel). Een menselijke afweging van het resultaat in het licht van andere onderzoeksgegevens is juist bij het werk van inlichtingen- en veiligheidsdiensten van het grootste belang. Het benutten van data-analyses betreft een activiteit waarbij voortdurend sprake is van weging, inschatting en interpretatie van onderzoeksresultaten in combinatie met elkaar en in het licht van de specifieke onderzoeksvraag. Hierbij wordt ook gekeken naar de foutmarge en de daarmee samenhangende betrouwbaarheid van de informatie. Waar het gaat om gegevensverwerking door de inlichtingen- en veiligheidsdiensten is in artikel 18, derde lid, van het wetsvoorstel als algemene eis toegevoegd, dat de gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt dienen te zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend. Tevens vloeit uit deze waarborg voort dat het verstrekken van data aan derden nooit geautomatiseerd zal gebeuren. Daar zit altijd een zorgvuldige menselijke afweging voor.

De leden van de D66-fractie vragen zich voorts af hoe het bovenstaande zich verhoudt tot andere diensten in Nederland en het buitenland. De activiteiten van de inlichtingen- en veiligheidsdiensten zijn vanwege de unieke taken en gerichtheid niet te vergelijken met die van andere instanties in Nederland. Voor zover mij bekend is de werkwijze van de Nederlandse diensten niet wezenlijk anders dan die van buitenlandse inlichtingen- en veiligheidsdiensten. Ik heb echter geen zicht op bijvoorbeeld standaarden e.d., waarop deze leden doelen, die door deze instanties worden gehanteerd.

Daarnaast vragen de aan het woord zijnde leden zich af hoe ten aanzien van de uitkomst van de verwerking en van de analyse duidelijk wordt gemaakt wat de kwaliteit van de broninformatie en die van de verwerking ervan is en wat de context van die informatie is. Zoals ik in de beantwoording hierboven reeds heb aangegeven, is in artikel 18, derde lid, van het wetsvoorstel als algemene eis opgenomen, dat de gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt dienen te zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend. De diensten kunnen in het kader van hun taakuitvoering gegevens verzamelen uit allerlei bronnen (open en gesloten, technisch en menselijk enz.). Niet elke bron en daarmee het aldus verkregen gegeven is echter zonder meer betrouwbaar. Bepaalde technische bronnen, zoals een gerichte tap op een target, zijn over het algemeen als erg betrouwbaar te kwalificeren. De kwalificatie van de betrouwbaarheid van gegevens verkregen van agenten of informanten wordt echter in belangrijke mate mede bepaald door de mate waarin de agent of informant als zodanig als betrouwbaar wordt beoordeeld; dat is afhankelijk van diverse factoren, zoals bijvoorbeeld dat verstrekte gegevens door gegevens uit andere bronnen worden bevestigd. Gelet op het gebruik dat van deze gegevens kan worden gemaakt – bijvoorbeeld als basis voor een mededeling als bedoeld in artikel 62 jo. 68 van het wetsvoorstel – en de gevolgen die dat kan hebben voor personen of organisaties waarop die gegevens betrekking hebben, is het dan ook van groot belang dat expliciet wordt vastgesteld wat de juistheid van die gegevens is.

Het toevoegen van een betrouwbaarheidsaanduiding of bronverwijzing geeft ook houvast bij de beoordeling van afgeleide gegevens die bijvoorbeeld volgen uit nadere analyse of samenvoeging van de oorspronkelijke gegevens. Tevens wordt gedocumenteerd welke analysemethoden zijn gebruikt, alsmede de betrouwbaarheid van deze methode. Het duiden van de betrouwbaarheids- of bronaanduiding van de programmatuur waarmee gegevensverzamelingen worden geanalyseerd behoort tot de kwaliteit van de bedrijfsvoering van de diensten. De diensten geven bij de programmatuur voor analyses de betrouwbaarheid en de bronaanduiding van de gegevensverzamelingen aan. Tevens is als extra waarborg opgenomen dat het bevorderen of treffen van maatregelen jegens een persoon uitsluitend naar aanleiding van geautomatiseerde data-analyse niet is toegestaan (artikel 60, derde lid). Zoals ik al aangaf in de beantwoording van eerdere vragen, blijft bij de analyses van gegevensverzamelingen de menselijke afweging essentieel en vereist.

De leden van de D66-fractie vragen zich af op welke wijze bijvoorbeeld de betrouwbaarheid van informatie automatisch wordt afgeschaald naarmate de tijd verstrijkt? De betrouwbaarheid van gegevens is van essentiële betekenis voor een goede taakuitvoering van de diensten en heeft dan ook – mede in het licht van het bepaalde in artikel 18, derde lid, van het wetsvoorstel – bij voortduring aandacht. Immers de betrouwbaarheid van de gegevens werkt door in de te maken analyses en de daarop te baseren vervolghandelingen. Ingevolge artikel 69, eerste lid, van het wetsvoorstel vindt de verstrekking van gegevens die meer dan tien jaar geleden zijn verwerkt niet plaats. Slechts in limitatief bepaalde gevallen kan daarvan worden afgeweken, waarbij altijd de mate van betrouwbaarheid en de ouderdom van gegevens dient te worden vermeld. Overigens wordt opgemerkt dat oudere gegevens niet automatisch minder waard of onjuist zijn. Voor de beoordeling of ISIS een operative naar het westen heeft gestuurd om een aanslag te plegen kan juist een database uit 2014 informatie geven die essentieel is voor een onderzoek naar dit target. Zo kan een oud adres waar deze operative in 2014 verbleef niet meer zichtbaar zijn in een database uit 2016 waardoor de diensten deze informatie zouden missen, terwijl dit adres een belangrijke aanwijzing in een onderzoek kan zijn. Het is van belang om bij de beoordeling van de gegevens en de correlatie aan andere gegevens duidelijk in beeld te houden dat het gegevens uit 2014 betreft. Voordat met de analyse iets gedaan wordt, moet immers een AIVD- of MIVD-medewerker het resultaat bekeken hebben. De presentatie ervan kan dan een groot verschil maken voor de wijze waarop de analist dat beoordeelt en meeneemt in zijn of haar afwegingen. De aan het woord zijnde leden verkrijgen tot slot graag enkele voorbeelden van hoe de informatie binnen een analyse-product vermeld wordt. Bij analyseproducten wordt de mate van betrouwbaarheid aangegeven van de informatie die tot de analyse heeft geleid. Dit wordt per informatiebron gedaan.

De leden van de SGP-fractie vragen zich af hoe wordt bepaald of gegevens relevant zijn voor enig lopend onderzoek en of gegevens die zijn verzameld alleen mogen worden gebruikt voor onderzoeken die op dat moment daadwerkelijk lopen of ook voor onderzoeken die op een later moment starten dan dat de gegevens zijn verzameld. Het onderzoek op relevantie vindt alleen plaats ten aanzien van de lopende onderzoeken. Indien binnen de bewaartermijn zich een nieuw onderzoek aandient waarvoor de gegevens kunnen worden gebruikt en de gegevens nog niet zijn vernietigd, mogen de gegevens ook voor het nieuwe onderzoek worden gebruikt. Indien dit laatste niet mogelijk zou zijn, kan de onwenselijke situatie ontstaan dat de diensten beschikken over

rechtmatig verkregen informatie over een dreiging tegen de nationale veiligheid, maar deze informatie niet mogen gebruiken ter afwending van de dreiging.

Deze leden vragen zich voorts af wat het verschil is tussen verwijderen, vernietigen en terstond vernietigen omdat in sommige artikelen wordt gesproken over terstond vernietigen en op andere plaatsen over vernietigen. Het door de leden van de SGP-fractie opgemerkte verschil tussen 'vernietigd' en 'terstond vernietigd' betreft een technische onvolkomenheid in de tekst van het wetsvoorstel. Deze zal bij nota van wijziging worden hersteld.

De leden van de SGP-fractie begrijpen dat de gegevens ten minste bewaard moeten blijven in een semi statisch archief zolang er de mogelijkheid van bezwaar of klacht is. Maar, zo vragen zij, is altijd duidelijk wanneer die periode begint en wanneer hij eindigt? Wat is in dat verband de precieze betekenis van het 'vernietigd worden' als dit niet terstond dient te gebeuren? Er staat bijvoorbeeld in de toelichting dat 'ten minste' gewacht wordt tot een rechtelijke uitspraak onherroepelijk is geworden. Met deze vraag duiden deze leden, voor zover ik kan overzien, op de situatie als beschreven in artikel 20, vijfde lid, van het wetsvoorstel. Zoals daar is aangegeven moet er sprake zijn van bijvoorbeeld een aanhangige klacht of een aanhangig bezwaar. Daarmee is duidelijk wanneer die periode begint (namelijk het moment van indiening van een klacht of van een bezwaar); het einde van de periode zal niet altijd op voorhand duidelijk zijn en is afhankelijk van het verloop van de desbetreffende procedure. Overigens wordt in artikel 20 niet de eis gesteld dat de gegevens terstond moeten worden vernietigd, mede in verband met het bepaalde in artikel 21 van het wetsvoorstel.

3.2.2 De kring van personen (§3.2.4 m.v.t.)

De leden van de D66-fractie lezen dat de verwerking van persoonsgegevens die betrekking heeft op de in artikel 19, derde lid, bedoelde kenmerken slechts plaatsvindt in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is Deze leden vragen de regering wat precies wordt bedoeld met het begrip onvermijdelijk. Deze leden vragen zich voorts af of uitgesloten kan worden dat betreffende andere gegevens slechts verwerkt worden met als doel de bedoelde kenmerken te kunnen verwerken en op welke wijze dit in de systematiek van het voorliggende wetsvoorstel is gewaarborgd. Zoals in de memorie van toelichting is aangegeven, is met het begrip 'onvermijdelijk' beoogd aan te geven dat bij de verwerking van een gegeven als hier bedoeld aan een zwaarder criterium dient te worden voldaan dan aan het aan artikel 18, eerste lid, van het wetsvoorstel neergelegde noodzakelijkheidscriterium. Bij het vastleggen van de hier bedoelde gegevens zullen de diensten dus extra terughoudend dienen te zijn. Bovendien mogen dergelijke gegevens slechts worden verwerkt in aanvulling op andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is; daarmee geldt voor de verwerking van gegevens betreffende deze kenmerken een "dubbel slot". De betekenis van het begrip onvermijdelijkheid, waarnaar deze leden vragen, laat zich naar mijn mening het beste verwoorden door het geven van een concreet voorbeeld. Het zal onvermijdelijk zijn om bijvoorbeeld de godsdienstige of levensovertuiging van personen te registreren in de gevallen dat antidemocratische, staatsgevaarlijke of antimilitaristische activiteiten worden ontplooid waarbij deze personen hun godsdienstige overtuiging als motief aanvoeren voor hun activiteiten.

Dit algemene vereiste van artikel 19 van het wetsvoorstel geldt voor alle processen die binnen de diensten plaatsvinden, dus ook de geautomatiseerde gegevensverwerkingen. Echter bij de verwerking van gegevens in algoritmes en modellen worden persoonsgegevens niet gewogen. Er worden enkel correlaties gelegd. Daarbij zullen geen correlaties worden gezocht op basis van de kenmerken uit artikel 19, derde lid, van het wetsvoorstel, tenzij deze verwerking in het kader van het onderzoek naar de nationale veiligheid onvermijdelijk is. Zo is het bijvoorbeeld bij onderzoek naar jihadistisch terrorisme onvermijdelijk dat vast wordt gelegd wat de godsdienstbeleving is van een bepaald target of targetorganisatie. Daarbij kan het van belang zijn welke extremistische geloofsvariant wordt aangehangen of welke radicale moskee wordt bezocht. Na de geautomatiseerde verwerking volgt menselijk tussenkomst die op de resultaten daarvan een weging uitvoert.

3.2.3 De verwijdering, vernietiging en overbrenging van gegevens (§3.2.5 m.v.t.)

De leden van de D66-fractie stellen dat artikel 20, derde lid, vrij categorisch de indruk wekt dat verwijderde gegevens vernietigd worden, behoudens wettelijke verplichtingen. Deze leden vragen zich af welke verplichtingen dit zijn, welke termijn geldt voor die vernietiging, wie kan besluiten verwijderde gegevens niet te vernietigen maar te her-activeren en hoe na her-activering de geldende bewaartermijnen doorwerken. De verplichtingen omtrent bewaren en vernietigen zijn omschreven in de Archiefwet 1995. De termijnen voor vernietiging verschillen per werkproces en zijn vastgelegd in de selectielijsten van de diensten zoals deze door de ministers zijn opgesteld en door de minister van OC&W zijn vastgesteld. De ministers kunnen besluiten tot de opschorting of omzetting van de vernietiging als voorgeschreven in de generieke selectielijsten. Het opnieuw gebruiken van verwijderde gegevens die nog niet zijn vernietigd, kan enkel op basis van redenen zoals in de wet beschreven. Ik verwijs ook naar mijn eerdere beantwoording van vragen van de leden van de SGP-fractie in paragraaf 3.2.1. Het opnieuw gebruiken van reeds verwijderde gegevens, kan aan de orde zijn, indien de gegevens op enig moment voor een ander, later opgestart onderzoek van belang blijken te zijn. Het is immers merkwaardig indien bij de dienst beschikbare en voor een onderzoek relevante gegevens niet daarvoor gebruikt zouden mogen worden. Wanneer na een dergelijk onderzoek de desbetreffende gegevens opnieuw worden verwijderd, zoals voorgeschreven in de wet, geldt de voor dat proces vastgestelde vernietigingstermijn opnieuw.

De leden van de D66-fractie vragen zich voorts af wanneer gegevens, gezien het doel waarvoor zij zijn verworven, hun betekenis verliezen. Bij de inzet van de onderzoeksopdrachtgerichte interceptie bestaat het doel per slot van rekening vaak uit het invullen van witte vlekken en het ondervangen van onbekende dreigingen. Men zou kunnen beargumenteren dat gegevens hun doel pas verliezen zodra vaststaat dat zij niet in verband te brengen zijn met een mogelijke dreiging van een persoon of instantie. Dat valt echter nooit met zekerheid te zeggen, waarmee de gegevens nooit hun betekenis zouden verliezen en artikel 20, eerste en derde lid, een lege letter in de wet zouden zijn. Deze leden vragen de regering of zij deze redenering kan uitsluiten. Een deel van de gegevens verkregen uit onderzoeksopdrachtgerichte interceptie zal worden geanalyseerd en een deel niet. Indien de gegevens worden geanalyseerd, kunnen ze worden beoordeeld als relevant of als niet relevant. Gegevens verkregen uit de onderzoeksopdrachtgerichte interceptie die na analyse als relevant zijn beoordeeld

worden bewaard en daarvoor geldt ook artikel 20. De niet relevant bevonden gegevens worden immers op grond van het bepaalde in artikel 48, vijfde lid, terstond vernietigd.

De leden van de D66-fractie hebben enige tijd geleden kennisgenomen van de ontwerpselectielijsten voor de overbrenging van gegevens uit de archieven van de Binnenlandse Veiligheidsdienst (BVD), AIVD en MIVD naar het Nationaal Archief. Deze leden vragen de regering om uit te leggen op welke wijze het voorliggende wetsvoorstel de vastgestelde selectielijsten zal beïnvloeden. Dit wetsvoorstel heeft geen invloed op de vastgestelde selectielijsten. Deze leden vragen voorts of op een andere manier invulling gegeven moet worden aan die lijsten teneinde voldoende informatie voor toekomstig (historisch) onderzoek te bewaren. Er is naar mijn mening geen reden om op een andere manier invulling te geven aan de selectielijsten dan wel deze anders in te richten. De selectielijsten zijn tot stand gekomen na een zorgvuldige procedure waarbij naast de betrokken departementen, de minister van OC&W, de algemeen rijksarchivaris en een extern deskundige op het terrein van de relatie tussen burger en overheid en de betekenis van overheidsinformatie voor deze relatie betrokken zijn. De belangen zoals genoemd in artikel 2, eerste lid, van het Archiefbesluit 1995 en die zien op het evenwicht tussen bewaren, overdragen en vernietigen, zijn daarbij betrokken en tegen elkaar afgewogen.

De leden van de GroenLinks-fractie vragen de regering of zij de mening deelt dat artikel 19 lid 1 onder e juncto artikel 19 lid 2 onder e met de toestemming voor het verwerken van gegevens "ter ondersteuning van een goede taakuitvoering door de dienst" niet een te ongeclausuleerde toestemming bevat die op vrijwel alle gegevens kan slaan. Deze leden vragen de regering in te gaan op de mate van proportionaliteit van deze bepalingen. De bevoegdheid om gegevens te verwerken ter ondersteuning van een goede taakuitvoering door de dienst, is reeds opgenomen in de huidige regeling in artikel 13 Wiv 2002. Bij het vastleggen van een dergelijk gegeven moet zowel in de huidige wet als in het wetsvoorstel worden voldaan aan de algemene eis uit artikel 18, eerste lid, dat het noodzakelijk is voor een goede uitvoering van de Wiv of de Wet Veiligheidsonderzoeken.

De leden van de GroenLinks-fractie vragen de regering een toelichting te geven op de schijnbare willekeur waarmee op sommige plaatsen van het voorliggende wetsvoorstel is bepaald dat gegevens terstond dienen te worden vernietigd en dat het woord 'terstond' op andere plaatsen ontbreekt. Zoals ik heb aangegeven in mijn beantwoording van een soortgelijke vraag van de leden van de fractie van de SGP-fractie onder 3.2.1, betreft het opgemerkte verschil tussen 'vernietigd' en 'terstond vernietigd' een technische onvolkomenheid in de tekst van het wetsvoorstel. Deze zal bij nota van wijziging worden hersteld.

3.2.4 Zorgplichten voor de diensthoofden (§3.2.6 m.v.t.)

De leden van de D66-fractie lezen dat het voorstel in de PIA om een bepaling op te nemen over gegevensbescherming by design en by default niet door de regering gevolgd wordt, maar dat zij volstaan met een algemene zorgplicht van de diensthoofden tot technische, personele en organisatorische maatregelen. Zij zouden het waarderen als de regering dit aspect van gegevensbescherming nader zou willen uitwerken. Ik merk hieromtrent het volgende op. Bij het ontwerpen, aankopen en in gebruik nemen van technische systemen houden de diensten rekening met de beginselen van

gegevensbescherming, zoals gegevensbescherming by design en by default. Gegevensbescherming by design houdt in dat de diensten bij de ontwikkeling van systemen het belang van privacy en gegevensbescherming inbouwen. Gegevensbescherming by default ziet erop dat systemen zo ontworpen en ingericht worden dat zo min mogelijk persoonsgegevens worden verwerkt. De zorgplicht in artikel 24 ten aanzien van de ontwikkeling van technische systemen legt een inspanningsverplichting bij de diensten neer om bij nieuw te ontwikkelen systemen ten behoeve van de verwerking van persoonsgegevens, waar mogelijk, zoveel mogelijk te handelen naar gegevensbescherming by design en by default. In artikel 24, tweede lid onder a, is opgenomen dat er voorzieningen door de diensten worden getroffen die de juistheid en volledigheid van gegevens die door de diensten worden verwerkt, bevorderd. Zoals eerder aangegeven wordt deze zorgplicht uitgebreid. Het beschermen van gegevens is inherent aan het werk van inlichtingen- en veiligheidsdiensten. Dit blijkt onder meer doordat de medewerkers van de diensten gescreend worden op het hoogste veiligheidsmachtigingsniveau, bij wet verplicht zijn tot geheimhouding en werken in beveiligde kantoren met zonering en functiescheiding, die conform de Wet bescherming staatgeheimen als verboden plaats zijn aangewezen. Ook het beginsel van need to know wordt door de diensten gehanteerd. Daarnaast werken de diensten met systemen conform de vereisten die in het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) zijn gesteld, hetgeen de diensten voorschrijft (persoons)gegevens te beveiligen op het allerhoogste niveau. De systemen zelf zijn en worden voorzien van standaardfunctionaliteiten zoals passend autorisatiebeleid, afscherming van informatie en actieve logging. De gebruikers van deze systemen hebben alleen toegang tot de informatie die voor hun taakuitvoering noodzakelijk is. Hiermee wordt tegemoet gekomen aan de invulling van gegevensbescherming by design.
Gegevensbescherming by default beoogt te bevorderen dat bij de technische inrichting van systemen, zowel in ontwerp als in standaardinstellingen, privacyinbreuken zoveel mogelijk worden voorkomen of beperkt. De verwerking van persoonsgegevens behoort tot de kerntaak van de diensten. Omdat de diensten niet van tevoren weten welke (persoons)gegevens in potentie relevant zijn in het kader van hun onderzoeken, is het onwenselijk systemen op voorhand zodanig te ontwerpen dat deze systemen by default een beperkende werking hebben bij het vinden van persoonsgegevens. Anders dan deze leden lijken te suggereren staat het gebruiksgemak niet voorop; het voldoen aan de wettelijke waarborgen staat voorop. Tot slot merk ik op dat de CTIVD als onafhankelijke toezichthouder toegang heeft tot gegevensverwerkingsprocessen gedurende de gehele verwerkingscyclus. Als toezichthouder kan ze de rechtmatigheid gedurende het gehele proces van gegevensverwerking beoordelen. Bovendien bestaat er altijd de mogelijkheid voor de CTIVD om medewerkers van de diensten om toelichting te vragen. De voorgestelde aanpassing van de zorgplicht in artikel 24, tweede lid, onder a, zoals eerder in deze nota toegelicht, biedt de CTIVD aanvullende mogelijkheden om vanuit haar toezichtstaak toe te zien op de kwaliteit van de gegevensverwerking.

3.3 De verzameling van gegevens

3.3.1 Algemene bepalingen inzake de verzameling van gegevens(§3.3.2 m.v.t.)

3.3.1.1 De informatiebronnen van de diensten (§3.3.2.1 m.v.t.)

De leden van de fractie van D66 merken op dat het hen opvalt dat in het eerste lid de woorden ‘in ieder geval’ is opgenomen, wat lijkt te impliceren dat er buiten de

ministeriële toestemming van het tweede lid vallende informatiebronnen zijn die niet expliciet in het eerste lid genoemd worden. Zij achten dit onwenselijk en stellen daartoe een amendement voor. Ik heb met de tekst van het eerste lid niet beoogd wat deze leden daarin lezen. Om misverstanden te voorkomen kunnen genoemde woorden dan ook vervallen. Ik ondersteun dan ook het amendement van het lid Verhoeven op dit onderdeel.

Naar aanleiding van de vraag van de leden van de D66-fractie aan wat voor een soort alternatieve informatiebronnen in artikel 25, tweede lid, moet worden gedacht, merk ik op dat naar thans valt te overzien artikel 25, eerste lid, de lading dekt. Het gaat in artikel 25, tweede lid om nieuwe nu niet te voorziene typen informatiebronnen. Het gaat bij artikel 25 om een algemene duiding van de type informatiebronnen waaruit de diensten kunnen putten. Om te voorkomen dat eerst artikel 25 moet worden aangepast alvorens van een informatiebron gebruikt kan worden gemaakt, is het tweede lid van artikel 25 opgenomen. Zoals ook in de memorie van toelichting is aangegeven, ligt het voor de hand vanuit de actieve inlichtingenplicht jegens het parlement dat deze wordt geïnformeerd omtrent een aanwijzing van een nieuwe niet onder artikel 25, eerste lid, vallende informatiebron.

Ik merk het volgende op naar aanleiding van de stelling van de D66-fractie dat voor nieuwe technische toepassingen van bijzondere bevoegdheden voor zover deze een substantiële en vergaande inbreuk op de persoonlijke levenssfeer kunnen maken, er sprake zou moeten zijn van de mogelijkheid tot debat hierover. Zoals ook elders in de nota naar aanleiding van het verslag aangegeven, benadruk ik dat indien een nieuwe bijzondere bevoegdheid in het leven wordt geroepen daarvoor eerst de wet moet worden gewijzigd. En daarmee dus ook eerst het parlement als medewetgever wordt betrokken. Wanneer het echter gaat om een bepaalde nieuwe technische toepassing welke volledig past binnen een bestaande wettelijk omschreven bijzondere bevoegdheid en de daarbij geregelde waarborgen ben ik er geen voorstander van de toepassing afhankelijk te maken van de mogelijkheid van een parlementair debat daarover en zo'n clausule wettelijk vast te leggen. Ik acht het uit oogpunt van het bieden van een zuiver en helder, maar ook slagvaardig wettelijk instrumentarium, onwenselijk dat er onduidelijkheid kan gaan ontstaan of wel of niet van gebruik kan worden gemaakt van een bestaande bijzondere bevoegdheid. Ik vestig er daarbij de aandacht op dat over de wijze waarop door de diensten gebruik wordt gemaakt van de bijzondere bevoegdheden gebruik wordt gemaakt, toezicht wordt gehouden door de CTIVD. Deze heeft hieraan de afgelopen jaren uitvoering gegeven door het uitbrengen van diverse uitgebreide toezichtsrapporten ten behoeve van het parlement.

3.3.1.2 Het onderzoek op relevantie van gegevens en de vernietiging van gegevens (§3.3.2.3 m.v.t.)

De leden van de D66-fractie lezen in artikel 27 een plicht voor de diensten om gegevens verkregen door uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5 zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven te onderzoeken. Deze leden vragen de regering aan te geven wat zij verstaan onder het begrip 'zo spoedig mogelijk' en welke termijn daaraan is gekoppeld. Het begrip 'zo spoedig mogelijk' drukt uit dat zodra de mogelijkheid redelijkerwijs bestaat de gegevens te onderzoeken op relevantie, dit dient plaats te vinden. Het is niet op voorhand vast te stellen wat 'zo spoedig mogelijk' in een specifiek geval betekent

aangezien er diverse factoren invloed hebben op een redelijke invulling van dit begrip. De normering dat zo spoedig mogelijk dient te worden onderzocht op relevantie geeft de CTIVD voldoende duidelijke handvatten in het licht van haar toezichthoudende taak.

De leden van de D66-fractie vragen met verwijzing naar een aantal casus naar de gehanteerde termijn voor het filteren van gegevens en daarbij gehanteerde algoritme. In het algemeen kan worden gesteld dat de diensten streven naar een zo nauwkeurig mogelijke analyse binnen de daarvoor beschikbare tijd. De keuze voor snelheid of nauwkeurigheid hangt, voorzover er sprake is van een keuze, evenwel af van het type onderzoek en het spoedeisend karakter daarvan. Een uitspraak over een redelijke termijn voor de beoordeling van relevantie voor een specifieke activiteit is op voorhand echter niet te geven.

De leden van de D66-fractie vragen zich af onder welke omstandigheden het hebben van onvoldoende vertaalcapaciteit reden kan zijn om tot verlenging van de bewaartermijn als bedoeld in artikel 27 over te gaan. Voorts vragen deze leden zich af of en op welke wijze dit gebrek aan vertaalcapaciteit invloed kan hebben op de proportionaliteit van de inzet van een bijzondere bevoegdheid. Onder de omstandigheden voor een verlenging wordt in de memorie van toelichting onder 3.3.2.3 genoemd een grote hoeveelheid gegevens die binnen de gestelde termijn niet kan worden verwerkt of het ontbreken van voldoende vertaalcapaciteit. De norm is dat indien de diensten niet verwachten de te verwerven gegevens te kunnen verwerken, de inzet niet proportioneel zal zijn en dus achterwege moet blijven. Echter indien bijvoorbeeld vertaalcapaciteit nu ontbreekt maar reeds wordt voorzien dat deze binnen afzienbare termijn beschikbaar komt, kan er alsnog reden bestaan tot inzet over te gaan. Dan zal bij de toetsing van de noodzakelijkheid en proportionaliteit van het verlengen of hernieuwen van de inzet van bijzondere bevoegdheden hierbij nadrukkelijk worden stilgestaan.

De leden van de ChristenUnie-fractie constateren dat advocaten in artikel 27 (terecht) worden beschermd tegen doorbreking van vertrouwelijke communicatie. Deze leden vragen de regering of is overwogen om een bredere verschoningsgrond op te nemen in de wet en niet, waarom daarvan is afgezien. Meer specifiek vragen de aan het woord zijnde leden de regering of zij heeft overwegen de regeling in artikel 27 voor de communicatie tussen advocaten en cliënten ook van toepassing te verklaren op journalisten. Daarbij verwijzen deze leden naar de zorgen die zijn geuit door de Studiecommissie Journalistieke Bronbescherming. Ik wijs deze leden er graag op dat niet alleen in artikel 27 van het wetsvoorstel, maar ook in artikel 30, maatregelen zijn opgenomen in verband met de bescherming van vertrouwelijke communicatie als hier bedoeld; aldaar strekt de regeling bovendien niet alleen uit tot advocaten, maar ook tot journalisten. De reden waarom de regeling is beperkt tot deze twee beroepsgroepen is eerder toegelicht in reactie op vragen van de leden van de SP-fractie. Ook verderop in deze nota naar aanleiding van het verslag wordt, in reactie op vragen van de leden van de D66-fractie, nog stilgestaan bij de reden waarom in het wetsvoorstel niet ook een regeling voor andere verschoningsgerechtigden, zoals artsen, notarissen en reclasseringsmedewerkers, is opgenomen. Ik zou deze leden graag daarnaar willen verwijzen, nu daar ook de door hen gestelde vragen worden beantwoord. Deze stelden tevens de vraag of overwogen is de in artikel 27 opgenomen regeling voor communicatie tussen advocaten en cliënten ook van toepassing te verklaren op journalisten. Invoeren van een vergelijkbare bijvangstregeling voor journalisten zal in de praktijk niet mogelijk zijn. Voor de uitvoerbaarheid van een dergelijke regeling zou – anders dan bij het direct

inzetten van bevoegdheden op journalisten om hun bronnen te achterhalen - essentieel zijn dat de diensten kunnen onderkennen wanneer de persoon waarmee een target in contact staat een journalist is van wie het target als bron functioneert. In tegenstelling tot advocaten, voor wie regels gelden voor het lidmaatschap van de Orde van Advocaten, vormen journalisten niet een afgebakende en daarmee te herkennen beroepsgroep. Daarmee zou de voorgestelde regeling onuitvoerbaar zijn en dat vormt voor mij reeds voldoende reden deze niet in de wet op te nemen. Tevens wijs ik erop dat het te beschermen rechtsgoed in het geval van journalisten wezenlijk verschilt van dat van advocaten. Bij advocaten gaat het om de bescherming van de communicatie als zodanig tussen de advocaat en zijn cliënt, opdat de cliënt, ook al is hij een target van de dienst, niet in zijn recht zal worden geschaad. Verdachten en andere procespartijen dienen een eerlijk proces te krijgen en in dit verband is van belang dat zij zich in vertrouwen kunnen wenden tot een advocaat. Bij journalisten gaat het om de bescherming van het recht van de journalist dat zijn bronnen niet worden achterhaald. De inzet van een bijzondere bevoegdheid op een target, niet zijnde die journalist, omdat het target daartoe aanleiding geeft, doet daaraan niets af. Er bestaat geen bijzondere bescherming voor een target om in vertrouwen met een journalist te kunnen communiceren.

De leden van de ChristenUnie-fractie constateren dat in artikel 27 van het wetsvoorstel de rechtbank den Haag beoordeelt of de gegevens terstond moeten worden vernietigd. Zij vragen hoe dat precies bij de rechtbank wordt vormgegeven. Gebeurt dat door een enkelvoudige of meervoudige kamer. Voor de goede orde merk ik allereerst op dat ingevolge artikel 27, tweede lid, de rechtbank niet beoordeelt of de gegevens terstond moeten worden vernietigd, maar of er toestemming kan worden verleend om de gegevens verder te verwerken voor het onderzoek in welk kader de gegevens zijn verworven. Indien de toestemming niet wordt verleend verbindt de wet daar het rechtsgevolg aan dat ze terstond dienen te worden vernietigd. Voor de beoordeling van de verzoeken om toestemming – onder de huidige wet beperkt tot het mogen openen van brieven en andere geadresseerde zendingen – zijn door de rechtbank Den Haag twee rechter-commissarissen aangewezen, die ieder voor zich (dus niet als collectief) de verzoeken om toestemming beoordelen. Naar verwachting kan onder de werking van de nieuwe wet met deze twee rechter-commissarissen worden volstaan.

De leden van de ChristenUnie-fractie vragen of de regering uiteen kan zetten hoe in het voorliggende wetsvoorstel gewaarborgd is dat bij gegevensverzameling niet-relevante data direct wordt verwijderd en vragen zich tevens af waarom de regering een jaar nodig heeft om verzamelde gegevens op hun relevantie te beoordelen. Zoals eerder aangegeven is ‘terstond’ inmiddels ingevoegd in de wet bij nota van wijziging. In de wet is daarmee gewaarborgd dat niet-relevante gegevens terstond worden vernietigd. Dat wil zeggen dat zij in tegenstelling tot verwijderde gegevens nimmer meer kunnen worden gebruikt voor enig onderzoek van de dienst. De gegevens zijn definitief en onomkeerbaar uit de systemen en de gegevensdragers waarop ze zijn vastgelegd verdwenen. Alleen het deel van de gegevens waarvan de relevantie niet kan worden vastgesteld of die niet op relevantie is onderzocht, wordt eerst na afloop van deze periode vernietigd. Deze leden vragen zich voorts af hoe inhoudelijk de relevantietoets is die moet plaatsvinden? De toets op relevantie is een inhoudelijke toets waarbij onder meer wordt gekeken of de gegevens in positieve zin bijdragen aan het onderzoek, alsook of die gegevens bepaalde vragen negatief kunnen beantwoorden, hypothesen kunnen ontkrachten of anderszins van doorslaggevend belang zijn.

De leden van de GroenLinks-fractie geven aan dat zij positief zijn over de uitzondering die in artikel 27, tweede lid, is gecreëerd voor communicatie tussen advocaten en hun cliënten. Wel vragen deze leden zich af of een soortgelijke uitzondering niet op zijn plaats is voor communicatie tussen journalisten en hun bronnen, evenals de communicatie tussen artsen en patiënten. Deze leden vragen of de regering het met hen eens is dat het wenselijk is om aan artikel 27, tweede lid, toe te voegen dat bij algemene maatregel van bestuur groepen kunnen worden aangewezen die tevens onder de regeling komen te vallen. Ik ben verheugd dat de leden van de GroenLinks-fractie positief zijn over de uitzondering die in artikel 27, tweede lid, van het wetsvoorstel is gecreëerd voor communicatie tussen advocaten en hun cliënten. Ik heb eerder aangegeven dat ik bezwaar heb tegen uitbreiding van deze regeling tot journalisten. Voor een vergelijkbare regeling voor de communicatie tussen artsen en patiënten zie ik voorts geen aanleiding. Ik verwijs hiervoor naar hetgeen ik verderop in deze nota in antwoord op vragen van de leden van de fractie van D66 heb geantwoord, waar het gaat om de positie van verschoningsgerechtigden in algemene zin. De suggestie van de leden van de GroenLinks-fractie om aan artikel 27, tweede lid, de mogelijkheid toe te voegen om bij algemene maatregel groepen aan te wijzen die tevens onder de regeling komen te vallen, wijs ik af. De regeling van artikel 27, tweede lid, staat namelijk niet op zichzelf en heeft een relatie met hetgeen in artikel 30, tweede en derde lid, van het wetsvoorstel is bepaald. In artikel 30, tweede en derde lid, wordt een regeling getroffen voor de inzet van bijzondere bevoegdheden op journalisten onderscheidenlijk advocaten; artikel 27, tweede lid, bestrijkt de situatie dat bij de uitoefening van bijzondere bevoegdheden jegens een andere persoon gegevens worden verkregen die betrekking hebben op de vertrouwelijke communicatie van een advocaat en diens cliënt. Met een aanvulling van artikel 27, tweede lid, kan aldus niet worden volstaan. Dan zou ook in de sfeer van artikel 30 een voorziening moeten worden getroffen. Ik zie echter geen aanleiding om voor andere groepen een vergelijkbare voorziening te treffen.

3.3.1.3 Het toestemmingsregime voor bijzondere bevoegdheden (§3.3.2.5 m.v.t.)

3.3.1.3.1 De inhoud van een verzoek om toestemming (§3.3.2.5.2 m.v.t.)

De leden van de D66-fractie lezen alleen voorbeelden van wat onvoldoende concreet is als omschrijving van het onderzoek waarvoor de bijzondere bevoegdheid uitgeoefend wordt en vragen de regering om voorbeelden te noemen van de soort dreiging en de targetgroep die wel voldoende concreet zijn om te kunnen leiden tot toestemming en een positief rechtmatigheidsoordeel. Voorbeelden van voldoende concrete soorten dreiging of targetgroepen die voor de dreiging zorgen, zijn bijvoorbeeld:
- uit onderzoek blijkt dat leden van een jihadistische cel actief zijn in Nederland. Om deze dreiging te duiden, zal de betrokken dienst een of meerdere (bijzondere) bevoegdheden op (al dan niet) verschillende leden van deze cel inzetten, teneinde in kaart te brengen of zij een aanslag willen plegen in Nederland, in het Westen, of willen uitreizen naar een strijdgebied zoals Syrië om deel te nemen aan de gewapende strijd.
- de AIVD of MIVD ontvangt een melding van een Nederlands bedrijf uit de vitale sector dat er malware is aangetroffen op de R&D-afdeling. De AIVD of MIVD start een onderzoek op om te onderzoeken of hier sprake is van digitale spionage door een statelijke actor. Indien dat het geval is zal worden onderzocht welke gegevens

onttrokken zijn aan deze afdeling, wat de schade is voor de nationale veiligheid, en welke statelijke actor hiervoor verantwoordelijk is.
- uit een onderzoek naar massavernietigingswapens ontstaat het vermoeden dat een bedrijf in Nederland dual use goederen levert aan een land dat zich bezighoudt met het vervaardigen van massavernietigingswapens. Om deze dreiging te kunnen duiden, zullen bijzondere bevoegdheden worden ingezet om de levering door dit bedrijf in kaart te kunnen duiden en vast te stellen of inderdaad sprake is van de levering van dual use goederen.
- een specifieke eenheid van een vijandige buitenlandse strijdkracht is actief in een gebied waar Nederlandse militairen actief zijn. Er zullen bijzondere bevoegdheden worden ingezet om de dreiging die vanuit deze eenheid uitgaat richting de aanwezige Nederlandse militairen tijdig te onderkennen.

Op de vraag hoe de regering invulling geeft aan de doelbinding is in de toelichting aangegeven dat de proportionaliteitstoets en subsidiariteitstoets tevens onderdeel uitmaken van de algehele beoordeling bij de aanvraag om een verzoek om toestemming voor de inzet van een bijzondere bevoegdheid. Met de verwijzing naar het CTIVD-rapport nr. 35 (aanbeveling 11.11 en 11.12) is opgenomen hoe in het geval van verlenging van een verzoek invulling aan deze toets wordt gegeven.
In artikel 26 van het wetsvoorstel wordt een regeling gegeven voor het bij de uitoefening van bevoegdheden toe te passen afwegingskader. Het gaat dan met name om de zogeheten subsidiariteits- en proportionaliteitstoets. Deze criteria zijn in de jurisprudentie van het EHRM ontwikkeld en indertijd in de Wiv 2002 toegespitst op de bijzondere bevoegdheden gecodificeerd (artikel 31 en 32 Wiv 2002); in de toezichtspraktijk van de CTIVD vormen deze criteria, naast andere, een belangrijke toetssteen. In artikel 26, eerste lid, van het wetsvoorstel is de subsidiariteitstoets uitgewerkt. Zoals uit de opsomming van de bevoegdheden in artikel 25 blijkt komen de diensten – mede afhankelijk van de aan de orde zijnde taak - diverse mogelijkheden toe tot het verzamelen van gegevens. Welke gegevens de diensten noodzakelijk achten te verzamelen zal in de praktijk primair worden bepaald door het onderzoeksonderwerp, het doel van het onderzoek, de reeds beschikbare informatie en dergelijke. Afhankelijk van het verloop van het onderzoek en de gegevens die daarin beschikbaar komen, zal telkens dienen te worden bezien welke informatie nog ontbreekt en op welke wijze de ontbrekende informatie zou kunnen worden verzameld. Het is met andere woorden een dynamisch proces. Voorts zijn ook aspecten als urgentie mede bepalend bij de te maken keuze. Bij de te maken toets op grond van artikel 26, eerste lid, spelen deze factoren allemaal een rol. Echter uiteindelijk zal die bevoegdheid (of combinatie van bevoegdheden) dienen te worden gekozen die voor de betrokkene – dat wil zeggen degene jegens wie de bevoegdheid wordt ingezet – het minste nadeel oplevert. Wanneer bijvoorbeeld de diensten de noodzakelijke gegevens kunnen verkrijgen door degene die toegang heeft tot de gegevens erom te vragen, zal voor dit middel worden gekozen. Dan kan en zal de inzet van een zwaardere bevoegdheid als het binnendringen in een geautomatiseerd werk achterwege blijven. Min of meer in het verlengde van het bepaalde in het eerste lid bepaalt artikel 26, vierde lid, dat een bevoegdheid onmiddellijk wordt gestaakt, indien het doel waartoe de bevoegdheid is uitgeoefend is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan. De proportionaliteitseis heeft zijn neerslag gekregen in artikel 26, tweede en derde lid: de uitoefening van een bevoegdheid dient achterwege te blijven, indien de uitoefening ervan voor betrokkene een onevenredig nadeel in vergelijking met daarmee na te streven doel oplevert; de uitoefening dient evenredig te zijn aan het daarmee beoogde

doel. Tevens vragen de aan het woord zijnde leden om een overzicht van alle aanbevelingen van de CTIVD om de inzet en toepassing van selectie bij SIGINT te verbeteren.
Voor een integraal overzicht van alle aanbevelingen van de CTIVD verwijs ik naar de respectievelijke rapporten en mijn reactie die aan uw Kamer is gezonden.

De leden van de SGP-fractie hebben een aantal vragen gesteld met betrekking tot de omschrijving van het doel van het vragen van toestemming voor gebruik van een bijzondere bevoegdheid. Ik ben het met deze fractie eens dat per geval kan verschillen hoe concreet de omschrijving en motivering van een verzoek om toestemming tot inzet van een bijzondere bevoegdheid kan zijn. Wel zal altijd aan alle in artikel 29, tweede lid, gestelde voorwaarden moeten worden voldaan. In reactie op een vraag van deze fractie kan worden bevestigd dat het denkbaar is dat sprake kan zijn van een ingewilligd verzoek in de situatie van een concreet doel, maar waarbij de precieze personen nog onduidelijk zijn. Gedacht kan worden aan een tap op een nummer waarvan het gerede vermoeden bestaat dat dit wordt gebruikt in extremistische kringen, maar waarvan op dat moment de identiteit van de precieze gebruiker(s) nog onbekend is. Voorts valt te denken aan de observatie van een pand ten aanzien waarvan aanwijzingen bestaan dat daar activiteiten plaatsvinden welke een gevaar vormen voor de nationale veiligheid. Uiteraard dient er dan een zo concreet mogelijke beschrijving plaats te vinden van het onderzoek waarvoor de betreffende bijzondere bevoegdheid dient te worden uitgeoefend en voorts een omschrijving van het met de uitoefening van de betreffende bevoegdheid beoogde doel. Daarnaast zal de reden moeten worden toegelicht waarom uitoefening van de bijzondere bevoegdheid noodzakelijk wordt geacht. Wanneer meer bekend wordt over de identiteit van de gebruikers zal dan in een verlengingsverzoek hierop vervolgens nader moeten worden ingegaan.

3.3.1.3.2 Toestemmingsverlening in bijzondere gevallen (§3.3.2.5.3 m.v.t.)

De leden van de D66-fractie begrijpen niet waarom de bescherming van verschoningsgerechtigden zich beperkt tot advocaten en journalisten en vragen de regering deze keuze – mede in het licht van de adviezen van de KNB en de Raad voor de Rechtspraak – nader toe te lichten. Ik heb eerder in antwoord op vragen van de leden van de SP-fractie reeds kort uiteengezet dat de reden waarom er uitsluitend voor journalisten en advocaten een regeling is opgenomen, voortvloeit uit rechterlijke uitspraken die daartoe noopten. Dat is ook in de memorie van toelichting toegelicht. Aangezien in de internetconsultatie door meerdere respondenten aandacht is gevraagd voor de positie van verschoningsgerechtigden is daaraan in paragraaf 12.2.7 van de memorie van toelichting (blz. 242 e.v.) nader bij stilgestaan. In de context van de werkzaamheden van inlichtingen- en veiligheidsdiensten bestaat een verschoningsrecht als zodanig niet; en daarmee ook niet de figuur van de verschoningsgerechtigde. Ergo: het feit dat iemand in de strafvorderlijke context als verschoningsgerechtigde wordt aangemerkt, betekent niet dat men automatisch ook in de context van inlichtingen- en veiligheidsdiensten op een bijzondere positie kan beroepen. Daar zullen specifieke redenen aan ten grondslag moeten liggen. Waar het gaat om journalisten en advocaten is aangegeven dat uit de ter zake geldende jurisprudentie kan worden opgemaakt dat beide beroepsgroepen een belangrijke functie vervullen in het kader van het borgen van belangrijke aspecten van onze democratische rechtsstaat. Bescherming van de bron van een journalist is van essentiële betekenis om te garanderen dat bronnen zich niet bezwaard voelen om met de pers samen te werken bij het informeren van het publiek

over zaken van publiek belang. De vertrouwelijkheid van de communicatie tussen een advocaat en diens cliënt en het in dat kader aan de advocaat toegekende verschoningsrecht moet worden moet worden geplaatst in de sleutel van het grondwettelijke recht op een eerlijk proces. Los van de eis dat er rechterlijke toestemming moet zijn om bijzondere bevoegdheden op een advocaat in te kunnen zetten, is in dit kader met name ook de in artikel 66, derde lid, van het wetsvoorstel van belang: het verstrekken van door de diensten verwerkte gegevens welke betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt aan het openbaar ministerie, is daarbij ook onderworpen aan voorafgaande toestemming van de rechtbank Den Haag. Waar het gaat om andere beroepsgroepen aan wie in het kader van strafvordering het verschoningsrecht toekomt, is met name stilgestaan bij artsen en geestelijken. Deze nemen de lichamelijke en geestelijke verzorging van hun cliënten voor hun rekening en in dat verband is weliswaar ook sprake van vertrouwelijke communicatie, maar niet vergelijkbaar met die van journalisten en advocaten. Dit geldt evenzeer voor de door de leden van de D66-fractie genoemde voorbeelden van notarissen en reclasseringsmedewerkers. Gelet op het voorgaande lijkt mij dat niet volgehouden kan worden dat sprake is van een arbitraire keuze. Ik wil er ten slotte nog op wijzen dat de belangen van die andere beroepsgroepen – gelijk de belangen van normale burgers – onder de werking van de regeling zoals voorzien in onderhavig wetsvoorstel niet onbeschermd zijn: ingeval van inzet van bijzondere bevoegdheden, waarvoor de toestemming van de minister is vereist (zoals interceptie van communicatie, binnendringen in geautomatiseerde werken e.d.), dient voorafgaand aan de uitvoering daarvan de door de minister verleende toestemming eerst nog onderworpen te worden aan een rechtmatigheidstoets door de TIB. De TIB is een onafhankelijke instantie, waarvan de toets materieel gezien zeker niet onderdoet voor die van de rechter.

De leden van de D66-fractie zijn van mening dat de bescherming voor journalisten nog enkele te dichten gaten kent en heeft daartoe een amendement ingediend. Allereerst menen de leden van de D66-fractie dat de bescherming zoals genoemd voor advocaten in artikel 27, tweede lid ook voor journalisten moet gelden. Verder vragen deze leden waarom ten nadele van de bronbescherming van journalisten wordt afgeweken van de door het EHRM gehanteerde definitie van een journalist en waarom de bescherming enkel geldt voor gegevens die ter openbaarmaking verkregen zijn. De voorgestelde uitbreiding van de regeling in artikel 27, tweede lid, tot journalisten, zoals neergelegd in het amendement van lid Verhoeven (Kamerstukken II 2016/17, 345 88, nr. 10) op onderdeel I, ondersteun ik niet. Voor een nadere toelichting hierop verwijs ik naar mijn eerdere antwoorden op vragen van leden van de ChristenUnie-fractie. Wat de definitie van journalist betreft merk ik het volgende op. Het gaat hierbij niet zozeer om de definitie van journalist, maar veeleer om dat van de bron. Zoals in de memorie van toelichting op het voorstel van wet tot wijziging van de Wiv 2002 in verband met bronbescherming van journalisten (kamerstukken II 2014/15, 34 027, nr. 3, blz. 7) is aangegeven, is daarbij begripsmatige aansluiting gezocht bij de omschrijving van het begrip bron die in het wetsvoorstel bronbescherming in strafzaken (Kamerstukken II 2014/15, 34 032) wordt gehanteerd. Dat wetsvoorstel is bij uw Kamer aanhangig en voor zover ik kan overzien wordt een vergelijkbare wijziging als thans door het lid Verhoeven wordt voorgesteld in dat kader niet gedaan. Om deze reden kan ik het voorgestelde amendement op dit onderdeel niet steunen.

De leden van de D66-fractie hebben de regering enkele vragen gesteld met betrekking tot het besluit van de regering om geen systeem van "nummerherkenning" in te voeren. In verband met de aard van de te beschermen belangen in het kader van de nationale veiligheid kan op voorhand geen communicatie worden uitgesloten van de bevoegdheden van de diensten. Targets zou daarmee een mogelijkheid worden geboden om hun communicatie in de uit te sluiten categorie te laten vallen. Het systeem van "nummerherkenning" zoals is vormgegeven in de opsporingspraktijk, en welke tot doel heeft dat van bepaalde communicatie op geen enkele wijze kennis kan worden genomen, acht de regering daarom onverantwoord. Er is dan ook geen aanleiding geweest de technische mogelijkheden daartoe te onderzoeken of te bespreken met de Nederlandse Orde van Advocaten. Ik benadruk dat wel van belang is dat tijdig door de diensten wordt onderkend dat een target contact heeft met zijn advocaat, zodat deze gegevens niet worden uitgewerkt voordat toestemming is verkregen van de rechtbank Den Haag. Momenteel laat ik onderzoeken of aan dit belang in meer geautomatiseerde vorm door middel van een aangepast systeem van nummerherkenning gestalte kan worden gegeven in de operationele praktijk.

De leden van de SGP-fractie stellen vast dat de regering heeft afgezien van een wettelijke definitie van het begrip journalist om hiermee aan te sluiten bij de ontwikkeling van de jurisprudentie door het EHRM en vragen de regering of het mogelijk is om hier nadere duiding aan te geven. Dat is mogelijk. Zoals bekend is thans bij de Tweede Kamer tevens een wetsvoorstel aanhangig tot wijziging van de huidige wet in verband met bronbescherming van journalisten (Kamerstukken II 2014/15, 34 027); de daarin voorziene regeling is – deels aangepast – in huidig wetsvoorstel geïncorporeerd. In de memorie van toelichting van dat wetsvoorstel is uitvoerig bij de betekenis van het begrip journalist stilgestaan. Nu ik in de memorie van toelichting op onderhavig wetsvoorstel niet verder ben in ingegaan op de betekenis van het begrip journalist, terwijl dit wel een wezenlijk element vormt voor de uitleg van de wettelijke regeling ter zake, zal ik de kernelementen van hetgeen in de toelichting op eerdergenoemd wetsvoorstel ter zake is gesteld hierna vermelden. Allereerst moet geconstateerd worden dat het EHRM zelf nog geen definitie heeft gegeven van de beroepsgroep of personen die als "journalisten" kunnen worden gekenschetst. Wel verwijst het in dit verband geregeld (onder meer in zijn uitspraak in de Telegraafzaak en Sanomazaak) naar een Aanbeveling van de Raad van Ministers van de Raad van Europa, Recommendation No. R(2000)7 on the rights of journalists not to disclose their sources of informations. Deze aanbeveling omschrijft journalist als «any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication». Eenzelfde onderscheid wordt in iets andere bewoordingen gehanteerd in de Nederlandse context door journalisten zelf. De Nederlandse Vereniging van Journalisten (NVJ) en de Raad voor de Journalistiek beschouwen allebei in artikel 4 van hun statuten als journalist «degene die, hetzij in dienstverband, hetzij als zelfstandige, er zijn hoofdberoep van maakt mede te werken aan de redactionele leiding of redactionele samenstelling van: a. een dagblad, nieuwsblad, huis-aan-huisblad, tijdschrift of nieuwssite, voor zover de inhoud daarvan bestaat uit nieuws, foto's en andere illustraties, verslagen of artikelen; (...); c. programma's, die worden verspreid door radio, televisie of internet, voor zover deze bestaan uit nieuws, rapportages, beschouwingen of rubrieken van informatieve aard; (...)». De voorgestelde regeling sluit met het gebruik van het begrip «journalist» in de zin van «beroepsmatige berichtgever» aan bij zowel het Raad van Europa begrippenkader («professionally» of «regularly engaged») als bij de beschrijving die de Nederlandse beroepsgroep zelf hanteert

(«hoofdberoepsmatig» of «regelmatig en tegen betaling»). Het gaat daarbij dus om een ieder die zich hoofdberoepsmatig (en daarmee vanzelfsprekend ook tegen betaling), danwel niet-hoofdberoepsmatig doch regelmatig tegen betaling, bezighoudt met het verzamelen, verspreiden of publiceren van informatie ten behoeve van het publieke debat, ongeacht de aard van het gebruikte medium (oude en nieuwe media) en ongeacht de aard van zijn rechtspositionele status (zzp-er, in vaste dienst, deelcontract e.d.). Deze toespitsing op «beroepsmatige berichtgeving» betekent materieel gezien een dubbel criterium: het moet gaan om journalistieke handelingen waarmee wordt mede gewerkt aan de redactionele leiding of de redactionele samenstelling van publiciteitsmedia en er moet sprake zijn van een vorm van «betaling» waartegen die handelingen worden ondernomen. Het begrip «betaling» moet in dit kader echter ruimer worden uitgelegd dan uitsluitend als «financiële vergoeding». In het Explanatory Memorandum bij de Aanbeveling van de Raad van Europa wordt aangegeven dat de journalist «some form of remuneration» voor zijn of haar werk ontvangt. Dat gaat verder dan louter een financiële vergoeding en omvat ook andere tegenprestaties. Te denken valt aan bepaalde voorzieningen of faciliteiten die als tegenprestatie voor de verrichte journalistieke werkzaamheden aan de betrokkene worden verstrekt, maar ook aan vergoedingen in de vorm van een abonnement op het periodiek waarin de publicatie(s) van betrokkene wordt opgenomen. Er dient echter wel een duidelijke relatie te bestaan met de door betrokkene geleverde (of te leveren) prestatie en voorts dient de tegenprestatie in economische zin waardeerbaar te zijn. Tot slot merk ik op, dat het enkele feit dat iemand bijvoorbeeld twittert, een blog of een vlog erop na houdt, deze nog niet tot journalist maakt.

3.3.1.3.3 De verslaglegging inzake de uitoefening van bevoegdheden tot verzamelen van gegevens (§3.3.2.5.4 m.v.t.)

De leden van de D66-fractie vragen de regering hoe een verschoningsgerechtigde, ten aanzien van wie de rechtbank toestemming heeft verleend tot inzet van een bijzondere bevoegdheid, erachter komt dat een dienst het vertrouwelijk karakter van de communicatie met een of meerdere cliënten c.q. bronnen geschaad heeft. Deze leden vragen zich af op welke wijze de regering voornemens is om daar zoveel mogelijk openheid in te betrachten. In artikel 59 is bepaald dat vijf jaar na de beëindiging van een bijzondere bevoegdheid zoals bedoeld in de artikelen 44, eerste lid, 47, eerste lid, alsmede artikel 58 eerste lid, voor zover is binnengetreden in een woning zonder toestemming van de bewoner, en daarna telkens eenmaal per jaar, wordt onderzocht of de persoon ten aanzien van wie één van deze bijzondere bevoegdheden is uitgeoefend (in casu de verschoningsgerechtigde), daarvan verslag kan worden gebracht. Indien dit mogelijk is, geschiedt dit zo spoedig mogelijk. Indien het uitbrengen van een verslag niet mogelijk is wordt de CTIVD daarvan gemotiveerd op de hoogte gesteld.

3.3.2 Toetsingscommissie inzet bevoegdheden (§3.3.3 m.v.t.)

Door de leden van alle aan het woord zijnde fracties zijn vragen gesteld omtrent de nieuw in te stellen Toetsingscommissie inzet bevoegdheden (hierna; TIB), die een belangrijke rol krijgt in het autorisatieproces voor de inzet van die bijzondere bevoegdheden waarvoor de voor de desbetreffende dienst verantwoordelijke minister – zonder de mogelijkheid van mandaat - toestemming dient te verlenen. Uit de gestelde vragen blijkt dat er nog onduidelijkheid bestaat over diverse aan de TIB verbonden aspecten.

De leden van de VVD-fractie vragen of gereageerd kan worden op de vrees dat de TIB onderbedeeld is en over te weinig know how, kennis en kunde beschikt. Ik kan deze vrees wegnemen. De TIB zal komen te bestaan uit een drietal leden. Dat aantal komt overeen met het huidige aantal leden van de CTIVD. Van de TIB dienen ten minste twee leden ervaring te hebben als rechter. De keuze voor een meerderheid aan leden met rechterlijke ervaring is ingegeven door het feit dat de toets die de TIB moet verrichten een rechtmatigheidstoets is, waarmee rechters immers van huis uit vertrouwd zijn. Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is er in het voorliggende voorstel in voorzien dat binnen de TIB ook een lid kan worden benoemd met bijvoorbeeld expertise op het vlak van inlichtingen- en veiligheidsdiensten en/of technologische ontwikkelingen. Bij het selecteren en benoemen van de leden van de TIB, waarbij de Tweede Kamer een belangrijke rol speelt (voor de TIB geldt immers dezelfde benoemingsprocedure als voor de CTIVD), zullen dit belangrijke aandachtspunten dienen te zijn. Er wordt aldus gekozen voor een gespecialiseerde commissie, waarin kennis en expertise wordt gebundeld. In paragraaf 3.3.3.1 van de memorie van toelichting is dit nog nader uitgewerkt, zodat kortheidshalve daarnaar wordt verwezen. De TIB krijgt voorts een eigen secretariaat, waarin al naar gelang de behoefte voorzien kan worden in de voor de ondersteuning bij de taakuitvoering van de TIB benodigde know how, kennis en expertise. Ik heb er alle vertrouwen in dat de TIB in de loop van de tijd de benodigde kennis en expertise zal hebben opgebouwd. Ook de CTIVD is indertijd vanuit het niets opgebouwd en heeft zich tot een gezaghebbende instantie weten te ontwikkelen.
Tot slot vragen de leden van de fractie van de VVD een toelichting te geven op de onafhankelijkheid van de TIB. De TIB zal een bij de wet ingestelde commissie zijn, met een wettelijk vastgelegde taak en daarbij behorende bevoegdheden (ook waar het gaat om het verkrijgen van voor die taakuitoefening benodigde informatie), die zelfstandig haar werkwijze zal kunnen bepalen en daarbij van niemand instructies zal kunnen ontvangen. Over de wijze waarop ze haar taak vervult zal zij jaarlijks een openbaar jaarverslag dienen uit te brengen (artikel 35, derde lid, jo. 132 van het wetsvoorstel). Voor de benoeming van de leden van de TIB (bij koninklijk besluit) is de procedure die geldt voor de benoeming van leden van de CTIVD van overeenkomstige toepassing verklaard, waarbij een belangrijke rol voor de Tweede Kamer is weggelegd. Naar mijn mening kan op grond van de wijze waarop de TIB in het wetsvoorstel is geregeld, er dan ook geen enkele twijfel over de onafhankelijkheid van die commissie bestaan.

De leden van de fractie van de SP vragen waarom er voor gekozen is de TIB alleen een marginale toets vooraf te laten doen op de inzet van bijzondere bevoegdheden. Ik wil hierbij graag de suggestie wegnemen dat de TIB alleen een marginale toets verricht. De TIB heeft ingevolge artikel 32, tweede lid, van het wetsvoorstel tot taak de rechtmatigheid van de door de minister verleende toestemming voor de uitoefening van een bijzondere bevoegdheid te toetsen. Deze rechtmatigheidstoets omvat een toets op noodzakelijkheid, proportionaliteit en subsidiariteit. Binnen deze rechtmatigheidstoets geldt voor de TIB geen beperking en hieraan kan zij deze dus op eigen wijze invulling geven. Het is dus niet zo dat men bijvoorbeeld slechts moet toetsen of de wettelijke (procedure)voorschriften in acht zijn genomen en of – ingeval er sprake is van de nodige beleidsvrijheid - de minister in redelijkheid tot het besluit had kunnen komen. De TIB zal hetzelfde feitencomplex als de minister krijgen voorgelegd en de in dat kader beoogde bevoegdheidsuitoefening in zijn volle omvang aan een rechtmatigheidstoets kunnen onderwerpen. Waar het gaat om de vraag van deze leden naar de gekozen samenstelling van de TIB en waarom specifiek is gekozen voor een commissie van drie personen,

wordt verwezen naar hetgeen eerder in reactie op vergelijkbare vragen van de leden van de fracties van de VVD en de PvdA is gesteld. De leden van de SP-fractie vragen ten slotte of – naar aanleiding van de kritiek van de Afdeling advisering van de Raad van State – nader ingegaan kan worden op de wijze waarop de verhouding tussen de TIB, als toetser vooraf, en de CTIVD, als toetser achteraf, wordt vorm gegeven. Voorts vragen zij of de regering ook ziet dat hier spanningen kunnen ontstaan. Zoals in reactie op het advies van de Afdeling advisering ter zake is gesteld (Kamerstukken II, 2016/17, 34 588, nr. 4, p. 24 en 25) en dat ook heeft geleid tot aanvulling van de memorie van toelichting op dat punt (Kamerstukken II, 2016/17, 34 588, nr. 3, p. 52), vervullen de TIB en de CTIVD ieder een verschillende rol in een verschillende fase van de taakuitvoering van de diensten. De CTIVD houdt toezicht tijdens en achteraf op de rechtmatige uitvoering van de wet en behandelt klachten hierover, terwijl de TIB een bindende toets uitvoert voorafgaand aan de inzet van bepaalde bijzondere bevoegdheden. Nu de toets op de rechtmatigheid van het door de minister genomen besluit voorafgaand aan de inzet van een bijzondere bevoegdheid exclusief bij de TIB is belegd, brengt dat met zich mee dat de CTIVD de rechtmatigheid van dat (door de TIB geaccordeerde) besluit in beginsel dient te respecteren; Indien de CTIVD in het kader van haar toezicht op de uitvoering van een dergelijk besluit constateert dat het door de minister genomen besluit en het voor toetsing aan de TIB voorgelegde besluit is gebaseerd op onvolledige of onjuiste informatie, kan zij dit als bevinding aan de minister rapporteren. De minister zal dan dienen te bezien of er aanleiding bestaat de eerder verleende toestemming in te trekken en eventueel een nieuw besluit te nemen dat vervolgens (opnieuw) aan de TIB – voorafgaand aan de uitvoering ervan – wordt voorgelegd. Een handelwijze zoals hiervoor geschetst, waarbij over en weer ieders positie en rol wordt gerespecteerd, moet er naar mijn mening toe leiden dat er van spanningen tussen beide instanties geen sprake hoeft te zijn en zij elkaar juist kunnen versterken.

De leden van de CDA-fractie vragen of er in verband met de voorziene toetsing door de TIB nader ingegaan kan worden op het vraagstuk van de ministeriële verantwoordelijkheid voor de diensten en de parlementaire controle daarop. Op het vraagstuk van de ministeriële verantwoordelijkheid ben ik eerder in reactie op een vergelijkbare vraag van de leden van de fractie van de VVD ingegaan, zodat ik kortheidshalve daarnaar verwijs. Waar het gaat om de parlementaire controle op de (voor de) diensten (verantwoordelijke minister) en de introductie van de TIB wil ik het volgende opmerken. De parlementaire controle blijft intact. De introductie van de TIB draagt er naar mijn overtuiging aan bij dat de kwaliteit – in termen van rechtmatigheid – van de besluitvorming van de minister waar het gaat om de (voorgenomen) uitvoering van bijzondere bevoegdheden ook bij de modernisering van de bevoegdheden gewaarborgd blijft, hetgeen naar mijn mening ook zijn weerslag zal krijgen in de toezichtsrapportages van de CTIVD, die uiteindelijk de Kamer bereiken en in het kader van de parlementaire controle van de Kamer van de activiteiten van de inlichtingen- en veiligheidsdiensten sinds jaar en dag een belangrijke rol spelen. Daarnaast zal ook de TIB jaarlijks voor 1 mei een openbaar verslag van haar werkzaamheden dienen uit te brengen, dat ook aan beide Kamers der Staten-Generaal wordt aangeboden. Naast de toezichtsrapportages en het jaarverslag van de CTIVD komt aldus voor het parlement een extra bron van informatie beschikbaar inzake de wijze waarop de wet door de diensten wordt uitgevoerd.

De leden van de CDA-fractie constateren dat het naast elkaar bestaan van de TIB en de CTIVD de vraag oproept hoe de werkzaamheden van beide organen op elkaar moet worden afgestemd. Zij wijzen er in dit verband op dat de CTIVD constateert, dat het wetsvoorstel niet voorziet in waarborgen ten behoeve van een uniforme en consistente rechtstoepassing. Hoe wordt, aldus de aan het woord zijnde leden, in de nieuwe wet uniforme en consistente rechtstoepassing geborgd? Ik wijs er allereerst op dat zowel de TIB als de CTIVD onafhankelijke instanties zijn, ook ten opzichte van elkaar en dat van afstemmen van werkzaamheden in dat opzicht geen sprake kan zijn; dat staat juist haaks op die onafhankelijkheid. Iets anders is, en daarvoor vragen deze leden – in navolging van de CTIVD – terecht aandacht, dat het wel wenselijk is dat er sprake is van een uniforme en consistente rechtstoepassing. Immers niemand, de burger voorop, is erbij gebaat dat twee onafhankelijke instanties bij de uitleg van de wet op een en hetzelfde onderdeel tot twee verschillende oordelen komen. Dat het wetsvoorstel niet voorziet in een bepaling, zoals door de CTIVD is voorgesteld, waarbij zowel de TIB als de CTIVD wordt opgedragen de rechtseenheid te bevorderen, verzet zich er naar mijn mening niet tegen dat beide instanties overleg hebben over de wijze waarop bepaalde wettelijke bepalingen dienen te worden uitgelegd. Echter, zoals de voorzitter van de CTIVD ook tijdens het gesprek met uw Kamer op 13 december 2016 aangaf, zonder dat daarbij een van beide de ander kan voorschrijven hoe de uitleg in een voorkomend geval zal moeten zijn; dan wordt de een immers bovengeschikt aan de ander en is er van onafhankelijkheid geen sprake meer.

De leden van de GroenLinks-fractie zijn positief over de keuze van de regering om de toetsing van de inzet van bijzondere bevoegdheden vóóraf en achteraf bij verschillende organen te beleggen. Wel hebben zij zorgen over de toerusting van de nieuw in te stellen TIB en vragen de regering een onderbouwing te geven van de geraamde €1 miljoen voor de TIB, de toegang die zij indien noodzakelijk zullen hebben tot nadere informatie van de veiligheidsdiensten en een appreciatie van de mate waarin de regering deze middelen en toegang voldoende acht om effectief en adequaat controle te kunnen uitvoeren. Voor de financiële onderbouwing wordt verwezen naar de beantwoording van de vragen van de leden van de D66-fractie in paragraaf 7.1.1 van deze nota.

De leden van de GroenLinks-fractie vragen de regering waarom zij niet heeft gekozen om in plaats van het creëren van een aparte toetsingscommissie de toetsing ex ante te beleggen bij rechters in functie. Deze leden vragen of deze optie de onafhankelijkheid van de toetsing niet beter zou garanderen. De toets door de TIB doet in termen van onafhankelijkheid niet onder voor de situatie dat de toets zou worden uitgevoerd door rechters in functie. De leden van de TIB worden benoemd door middel van een met waarborgen omklede procedure die gelijk is aan die van de leden van de CTIVD. De TIB staat volledig los van de betrokken departementen en zal voor twee derde bestaan uit leden die ten minste zes jaar beschikken over rechterlijke ervaring. De TIB voldoet daarmee volledig aan de eisen die ingevolge het EVRM en de daarmee samenhangende jurisprudentie worden gesteld. De Afdeling Advisering van de Raad van State onderkent dat het wetsvoorstel met de invoering van de TIB in formele zin voldoet aan de jurisprudentie van het EHRM, waar het gaat om de daarin geformuleerde wenselijkheid van een voorafgaande, onafhankelijke en bindende juridische toetsing. De keuze voor de TIB – in plaats van rechters in functie - is voorts ingegeven door het volgende. Een deel van de inzet van bijzondere bevoegdheden heeft betrekking op het buitenland en niet-Nederlanders. Het is maar zeer de vraag of een Nederlandse rechter zich bevoegd zal achten ten aanzien van zulke inzet van bijzondere bevoegdheden. Om deze reden is in

een aantal landen ook voorzien in een speciale commissie (en dus niet in een toets door rechters in functie) voor de inzet van bijzondere bevoegdheden betreffende het buitenland. Daarbij komt dat, zoals eerder aangestipt, ingevolge het wetsvoorstel een derde lid in de TIB kan worden benoemd, die beschikt over technische deskundigheid en inzicht in veiligheidsrisico's. Hiermee wordt ook nog de specifieke inbreng van deze deskundigheid in de toets geborgd. Ook dit pleit voor een aparte gespecialiseerde toetsingscommissie.

Deze leden vragen voorts waarom de regering ervoor heeft gekozen om het oordeel van de CTIVD bij de toetsing achteraf niet bindend te laten zijn. De huidige praktijk, waarin de CTIVD niet bindende adviezen geeft, functioneert goed. Ik wijs hier ook op de opvatting van de voorzitter van de CTIVD, zoals geuit in het gesprek dat de vaste commissie voor Binnenlandse Zaken op 13 december 2016 met de CTIVD heeft gehad, en waarbij deze zelf nadrukkelijk aangaf geen bindend oordeel te willen geven. Hij acht het gezag van de oordelen van de CTIVD voldoende.

Deze leden vragen de regering daarnaast waarom zij situaties voorziet waarin het oordeel van de CTIVD niet opgevolgd zou moeten kunnen worden. Zij vragen de regering bij haar antwoord de reactie van de CTIVD op dit punt te betrekken. In het verleden is het voorgekomen dat de betrokken minister het oordeel van de CTIVD niet volgde, omdat bijvoorbeeld de minister het oordeel niet deelde of de gevolgen die eruit voortvloeiden niet verantwoord vond met het oog op de nationale veiligheid. De minister dient dan in de reactie aan het parlement gemotiveerd aan te geven waarom een oordeel van de CTIVD niet wordt opgevolgd, zodat het parlement de minister hierop desgewenst kan aanspreken. De opvatting van de voorzitter van de CTIVD over de onwenselijkheid van bindend toezicht door de CTIVD, zoals ik die hierboven heb weergegeven, is hiermee in lijn.

De leden van de GroenLinks-fractie vragen ten slotte of de CTIVD in het nieuwe stelsel ook kan ingrijpen gedurende de uitvoering van een bevoegdheid van de diensten, teneinde te voorkomen dat onrechtmatig gebruik van bevoegdheden lang kan voortduren. Die mogelijkheid is er zeker, zij het dat die niet de vorm van een bindend oordeel heeft. Zo heeft de CTIVD (afdeling toezicht) de bevoegdheid om de minister gevraagd of ongevraagd in te lichten en te adviseren aangaande de door de CTIVD/afdeling toezicht geconstateerde bevindingen. Dat kan dus ook betrekking hebben op een door de CTIVD bevonden onrechtmatig gebruik van bevoegdheden. De minister kan een dergelijke bevinding niet negeren. Daarbij komt dat de CTIVD de minister kan vragen om een of beide kamers der Staten-Generaal de inlichtingen of adviezen ter kennis te brengen, waarbij de procedure inzake toezichtsrapportages (artikel 113 van het wetsvoorstel) van overeenkomstige toepassing is (artikel 97, derde lid, onder b, van het wetsvoorstel).

De leden van de SGP-fractie vragen of een nadere beschouwing kan worden gegeven op de vraag hoe wordt voorkomen dat – kort gezegd – de toets van de TIB vertragend gaat werken, terwijl ook voorkomen moet worden dat de zelfstandige verantwoordelijkheid van de minister wordt uitgehold door een zeer uitvoerige toetsing die ook nog eens bindend is. Aangaande de opmerking dat de ministeriële verantwoordelijkheid zou worden uitgehold verwijs ik graag naar mijn beantwoording op soortgelijke vragen van de leden van de VVD-fractie in paragraaf 1.6. Ik ben het met deze leden eens dat voorkomen moet worden dat de toets door de TIB vertragend gaat werken bij het

inzetten van noodzakelijke geachte bijzondere bevoegdheden door de AIVD en MIVD in het kader van hun onderzoeken. In artikel 36, tweede lid, is daartoe bepaald dat het oordeel van de TIB zo spoedig mogelijk dient te worden uitgebracht. Maar ook ben ik van mening dat de TIB op een adequate wijze de aan haar opgedragen taak moet kunnen vervullen. Er zal dan ook een goede modus moeten worden gevonden tussen enerzijds de belangen van de dienst en anderzijds die van de TIB waar het gaat om de toetsing van aan haar voorgelegde besluiten. Daarbij spelen naar mijn mening een aantal zaken een belangrijke rol, zoals de zorg voor een zowel in kwantitatief als kwalitatief ondersteuning van de TIB, een goede spreiding in tijd van de ter toetsing aan de TIB voor te leggen besluiten (zie ook hetgeen ik eerder in antwoorden op vragen van de leden de PvdA-fractie heb gesteld) en een tijdige aanlevering van eventueel additioneel door de TIB gevraagde informatie. Ik ga er voorts van uit dat na een opstartfase waarin ervaring wordt opgebouwd met het toetsingsproces de te verrichten toets binnen een aanvaardbare termijn kan plaatsvinden. Daarmee kom ik tegelijk op de vraag van deze leden of een indicatie te geven is van de termijn. Naar mijn mening moet daarbij onderscheid worden gemaakt tussen nieuwe verzoeken tot toestemming en aanvragen tot verlenging van een bestaande inzet. Ik kan me goed voorstellen dat de toets bij nieuwe verzoeken iets meer tijd in beslag zal nemen dan ingeval sprake is van verlenging van een bestaande inzet. Een duur van maximaal twee werkdagen lijkt me redelijk, maar dit acht ik ook een kwestie die tezijnertijd met de voorzitter en leden van de TIB nader dient te worden besproken. Voor alle gevallen geldt uiteraard dat het oordeel van de TIB zo spoedig mogelijk wordt uitgebracht, conform artikel 36, tweede lid, van het wetsvoorstel.

De leden van de SGP-fractie geven voorts aan dat het hen opvalt dat in artikel 99 van het wetsvoorstel een algemene bepaling is opgenomen over de verenigbaarheid van functies. Zij stellen voorts dat hier geen nadere duiding aan is gegeven dan dat de leden van de TIB geen onderdeel uit mogen maken van de CTIVD en andersom. Moet – aldus deze leden – bijvoorbeeld iedere rijksambtenaar per definitie als niet geschikt gezien worden voor de invulling van deze functie? En geldt dit ook voor bijvoorbeeld burgemeesters of commissarissen van de Koning? Ik merk allereerst op dat de in artikel 99, achtste lid, opgenomen regeling, overeenkomt met de regeling die thans reeds is opgenomen in artikel 65, zevende lid, Wiv 2002, waar het gaat om de leden van de CTIVD. De regeling inzake de (on)verenigbaarheid van betrekkingen, die is neergelegd in artikel 99, achtste lid, voor leden van de CTIVD, maar die van overeenkomstige toepassing is op de TIB (zie artikel 33, vierde lid, van het wetsvoorstel), behelst een algemeen geformuleerde norm, waaraan ieder voorkomend geval zal moeten worden getoetst. Deze norm heeft een duurzaam karakter, dat wil zeggen dat die niet alleen van toepassing is op bijvoorbeeld het moment dat iemand in aanmerking wenst te komen voor het lidmaatschap van de TIB of de CTIVD maar ook indien deze inmiddels lid is van de TIB of de CTIVD en een andere betrekking wenst te aanvaarden. Het gaat hierbij telkens om de vraag of de gelijktijdige uitoefening van verschillende betrekkingen ongewenst is met het oog op een goede vervulling van de functie van lid van de CTIVD of de TIB of op de handhaving van de onpartijdigheid en onafhankelijkheid of van het vertrouwen daarin. Het is dus niet zo dat iedere rijksambtenaar als per definitie ongeschikt moet worden gezien. Indien deze voldoet aan de overige eisen die aan het vervullen van het lidmaatschap van de TIB of CTIVD worden gesteld, kan deze zeer wel in aanmerking komen voor vervulling van de desbetreffende functie, echter indien uit de toets blijkt dat de betrekking die hij thans vervult daarmee onverenigbaar is zal deze een keus moeten maken: of de bestaande betrekking neerleggen of afzien van de functie

in de TIB of CTIVD. Dat geldt evenzeer voor burgemeesters of commissarissen van de Koning. Deze afweging zal ook telkens gemaakt moeten worden indien een lid van de TIB of CTIVD een andere betrekking ambieert en deze gelijktijdig/naast die van lid van de TIB of CTIVD wenst uit te oefenen. Hier ligt dus ook een verantwoordelijkheid voor het (kandidaat) lid van de TIB of de CTIVD. In artikel 100, aanhef en onder c, van het wetsvoorstel is tot slot bepaald dat bij koninklijk besluit, op voordracht van de betrokken ministers gezamenlijk, ontslag wordt verleend aan een dergelijk lid, bij de aanvaarding van een betrekking als bedoeld in artikel 99, achtste lid.

De leden van de SGP-fractie wijzen er op dat de TIB bestaat uit drie personen die voor een periode van zes jaar (met de mogelijkheid van verlenging) worden benoemd. In verband hiermee vragen zij of dit betekent dat mogelijk na zes of twaalf jaar de drie vacatures tegelijkertijd vrijkomen en of dit wel wenselijk is. Zou er niet gekozen moeten worden voor verschillende termijnen om de kwaliteit te handhaven en de overdracht beter mogelijk te maken? Deze leden hebben theoretisch gezien gelijk dat de door hen geschetste situatie zich zou kunnen voordoen. Ook bij de CTIVD, waarvoor dezelfde regeling geldt, zou dit voor kunnen komen. De praktijk laat echter zien dat de kans daarop klein is. Wel is het zaak om in voorkomend geval de benoemingsprocedure voor nieuwe leden tijdig in gang te zetten, zodat er geen gat valt tussen de beëindiging van het lidmaatschap van de bestaande leden en het aantreden van de nieuwe leden. Daar ligt zowel voor de Tweede Kamer als de regering een belangrijke verantwoordelijkheid, gelet op de rol die beiden in het benoemingsproces vervullen. De door de leden van de SGP-fractie voorgestelde oplossing kan op zich een bijdrage leveren om een scenario als door deze leden geschetst te voorkomen, maar ik zie daartoe geen aanleiding. Deze leden vroegen voorts of de termijn van zes jaar bij vervanging opnieuw begint te lopen. Dat is juist. Tot slot merk ik op dat het secretariaat van de TIB, dat een belangrijke ondersteunende rol zal spelen, een belangrijke bijdrage zal leveren aan het behoud van continuïteit en het borgen van de kwaliteit van de werkzaamheden van de TIB. De leden van de SGP-fractie vragen ten slotte in hoeverre de eis van bijvoorbeeld onpartijdigheid en onafhankelijkheid ook gelden voor de bemensing van het secretariaat en of dit ook geldt voor de eis van de Nederlandse nationaliteit. De personen die bij het secretariaat worden aangesteld dienen te worden aangemerkt als ambtenaar in de zin van de Ambtenarenwet en leggen in verband daarmee de eed of belofte af, waarbij hij onder meer zweert of belooft dat hij zich onder meer aan de gedragsregels inzake integriteit houdt; in dat kader zweert of belooft de ambtenaar onder meer dat hij zich gedraagt zoals een goed ambtenaar betaamt, zorgvuldig, onkreukbaar en betrouwbaar is en niets zal doen dat het aanzien van het ambt schaadt. Waar het gaat om de eis van de Nederlandse nationaliteit, wordt opgemerkt dat de functies bij de TIB (zowel die van de leden als van de ambtelijke ondersteuning) zullen worden aangewezen als vertrouwensfuncties als bedoeld in de Wet veiligheidsonderzoeken. Artikel 125e, eerste lid, van de Ambtenarenwet, bepaalt dat voor de vervulling van een vertrouwensfunctie slechts degene in aanmerking komt die Nederlander is.[4]

3.3.2.1 Algemeen (§3.3.3.1 m.v.t.)

De leden van de D66-fractie spreken hun verwondering erover uit dat de regering aanvankelijk als zorgpunt heeft uitgesproken dat met een onafhankelijke bindende toets

[4] Degene die geen Nederlander is, kan niettemin worden aangesteld wanneer het dienstbelang dat bepaaldelijk vordert. Toepassing van deze uitzondering is bij de CTIVD en TIB niet aan de orde.

vooraf geen invulling meer gegeven zou kunnen worden aan de ministeriële verantwoordelijkheid, terwijl men daar nu juist wel voor kiest. Op welke wijze, zo vragen de hier aan het woord zijn de leden, komt die verantwoordelijkheid onder het voorgestelde systeem tot uiting. Voorts vragen deze leden of de indruk juist is dat de regering nog steeds niet geheel achter de invoering van de TIB staat, maar dat dit omwille van het draagvlak voor het wetsvoorstel wel onderdeel van hebben gemaakt. Ik zou hier als volgt op willen reageren. Het is op zich juist dat aanvankelijk – zie het in consultatie gegeven ontwerp-wetsvoorstel – het standpunt is ingenomen, dat de invoering van een bindende rechtmatigheidstoets als door de Commissie Dessens was voorgesteld zich slecht zou verdragen met de ministeriële verantwoordelijkheid; als alternatief is toen een zogeheten heroverwegingsplicht voorgesteld. Naar aanleiding van hetgeen in de consultatie naar voren is gebracht, is opnieuw bij dit standpunt stilgestaan en heeft dat geleid tot een heroverweging die zijn beslag heeft gekregen in onderhavig wetsvoorstel. Daar liggen beide in de memorie van toelichting aangegeven redenen (zie paragraaf 3.3.3) aan ten grondslag en niet alleen, zoals deze leden met hun vraagstelling suggereren, het verwerven van draagvlak. De ontwikkeling in de jurisprudentie van het EHRM gaat, zoals gesteld, onmiskenbaar in de richting van een (vorm van een) bindende toets door een onafhankelijke instantie en dit gegeven kan niet veronachtzaamd worden; met onderhavig wetsvoorstel wordt namelijk niet alleen beoogd een toekomstvast kader te bieden voor de taakuitvoering van de diensten, maar ook een EVRM-proof stelsel voor de langere termijn. Waar het gaat om het vraagstuk van de ministeriële verantwoordelijkheid is vervolgens in reactie op het advies van de Afdeling advisering van de Raad van State zowel in het nader rapport als in de memorie van toelichting nader uiteengezet hoe de ministeriële verantwoordelijkheid in dit kader dient te worden beschouwd. Een belangrijk element daarin vormt het feit dat het uiteindelijk de wetgever is, die de bevoegdheidsuitoefening van de minister normeert en daarmee ook de grens van de ministeriële verantwoordelijkheid bepaalt.

De leden van de D66-fractie vragen tot slot op welke wijze dat vertrouwen moet scheppen dat de verantwoordelijke ministers er straks op een goede en constructieve wijze mede zorg voor gaan dragen dat de TIB snel gezag en kennis opbouwt om goed en geloofwaardig te kunnen toetsen. Deze leden kunnen er van op aan dat waar de regering een bijdrage kan leveren aan opbouw van kennis en gezag van de TIB, deze bijdrage – rekening houdend met de onafhankelijke status van de TIB – zal worden geleverd. Ik wijs erop dat kennis en gezag niet alleen daar afhankelijk van is, maar ook van de personele samenstelling van de TIB. In de benoemingsprocedure is, zoals bekend, een belangrijke rol voor de Tweede Kamer weggelegd.

De leden van de fractie van de ChristenUnie vragen welke scenario’s voor het toezicht allemaal door de minister zijn overwogen en welke vielen af en om welke redenen. Bij het voorbereiden van het wetsvoorstel is het bestaande toezichtstelsel, waarbij de CTIVD is belast met het toezicht op de rechtmatige uitvoering van de Wiv 2002 en de Wet veiligheidsonderzoeken alsmede als klachtadviesinstantie optreedt, als startpunt genomen. Naar aanleiding van de evaluatie van de Wiv 2002 door de Commissie Dessens, waarbij de commissie in paragraaf 5.5 (Extern toezicht op de inzet van bijzondere bevoegdheden) van haar evaluatierapport uitvoerig is ingegaan op diverse toezichtsvarianten, heeft het kabinet besloten het voorstel van deze commissie om de CTIVD te belasten met een onmiddellijke toets en een bindend rechtmatigheidsoordeel met betrekking tot een aantal bijzondere bevoegdheden, af te wijzen. In het kabinetsstandpunt dat naar aanleiding van dit evaluatierapport is uitgebracht, is dat

nader gemotiveerd (Kamerstukken II 2013/14, 33 820, nr. 2). Wel is in het kabinetsstandpunt de aanbeveling van de commissie overgenomen om de CTIVD als een (zelfstandige) onafhankelijke klachtbehandelaar te positioneren. Daarbij is tevens aangegeven dat het idee van de commissie om eventueel te voorzien in een aparte klachtenkamer ook in de door het kabinet voorgestane variant mogelijk een oplossing zou zijn, indien de bezwaren tegen de voorgestane invulling te groot zouden worden bevonden. Daar is later ook daadwerkelijk invulling aan gegeven door te voorzien in twee aparte afdelingen bij de CTIVD, één voor toezicht en één voor klachtbehandeling (en de behandeling van vermoedens van misstanden). In het Algemeen Overleg dat vervolgens naar aanleiding van het kabinetsstandpunt met betrekking tot het rapport van de Commissie Dessens op 16 april 2014 is gehouden, is – voor zover hier relevant – door het kabinet in aanvulling daarop voorgesteld om de oordelen die de CTIVD zou gaan uitspreken in het kader van klachtbehandeling een bindend karakter te geven; dit vanuit de wens om het stelsel EVRM-proof te doen zijn. Daarnaast is in het Algemeen Overleg door het kabinet aangekondigd dat, nu een bindend rechtmatigheidstoezicht als door de Commissie Dessens wordt voorgesteld, wordt afgewezen, ter versterking van het toezicht op de toestemmingverlening door de CTIVD te voorzien in een zogeheten heroverwegingsplicht. Aan de hand van deze standpuntbepaling is vervolgens gewerkt aan een uitwerking in wettelijke regeling ter zake. Bij dit alles is met name de uitspraak van het EHRM in de Kennedy-zaak als referentiekader gebruikt, nu het beoogde stelsel op onderdelen overeenkomsten vertoonde met het Britse stelsel dat door het EHRM in een uitspraak uit 2010 als EVRM-proof werd beoordeeld. In het Britse stelsel was namelijk niet voorzien in een vorm van rechterlijke toets vooraf, ook niet in een bindende toets achteraf, maar wel in een bindende klachtbehandeling door het Investigatory Powers Tribunal. Uiteindelijk heeft een en ander zijn beslag gekregen in het ontwerp-wetsvoorstel dat in juli en augustus 2015 in consultatie is gegeven. Om redenen zoals uiteengezet in paragraaf 12.2.3 van de memorie van toelichting is na afloop van de internetconsultatie besloten de heroverwegingsplicht te vervangen door een bindende toets door een nieuw in te stellen, onafhankelijke instantie, te weten de TIB. Dat zou dan een toets zijn op een eerder door de minister verleende toestemming; dus niet een toestemming, zoals wel is voorzien door de rechtbank ingeval het gaat om de uitoefening van de bijzondere bevoegdheid tot het openen van brieven, en de inzet van bijzondere bevoegdheden jegens advocaten en journalisten in de in het wetsvoorstel beschreven gevallen. Op de vraag van deze leden of door de regering is overwogen het toezicht vooraf zoveel mogelijk neer te leggen bij een college van gespecialiseerde rechters, kan worden opgemerkt dat de optie van een rechterlijke toets vooraf wel aan de orde is geweest, maar daarbij tegelijkertijd ook die van een ander onafhankelijk college (waarvoor in de jurisprudentie van het EHRM ook ruimte bestaat) is betrokken. De optie van een bindende toets vooraf door de CTIVD is in de loop van het wetgevingsproces ook aan de orde geweest, maar het onderbrengen van zowel een (bindende) ex ante toets als een ex post toezichtstaak bij de CTIVD, zou, meer nog dan nu blijkbaar al het geval is waar het gaat om toezicht en klachtbehandeling, de vraag inzake een onbevooroordeelde en onpartijdige oordeelsvorming op kunnen roepen. Bij een dergelijke keuze zou het bovendien aangewezen zijn om de bindende klachtbehandeling bij een andere, nieuw in te richten instantie onder te brengen. Nu ook de voorzitter van de CTIVD al eerder te kennen had gegeven een dergelijke ex ante toets niet te willen, is die optie al snel komen te vervallen. De optie van een rechterlijke toets vooraf is dus aan de orde geweest maar uiteindelijk afgewezen, omdat een substantieel deel van de inzet van bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten betrekking op het buitenland en de persoonlijke levenssfeer van niet-

Nederlanders. Een Nederlandse rechter zal zich niet bevoegd achten zich over deze inbreuk uit te spreken, omdat deze zich strikt genomen niet beperkt tot de Nederlandse jurisdictie. Zie in dit verband ook hetgeen in paragraaf 3.3.3.1 daaromtrent is gesteld. Dat daar waar het gaat om journalisten en advocaten wel voor is gekozen, hangt samen met het feit dat voor journalisten reeds een wetsvoorstel tot wijziging van de Wiv 2002 bij de Tweede Kamer aanhangig was, waarbij – ter opvolging van de uitspraak van het EHRM in de zogeheten Telegraafzaak - voorzien was in een rechterlijke toets ingeval de diensten een bijzondere bevoegdheid jegens journalisten zouden willen inzetten met het oog op het achterhalen van bronnen. Daar is vervolgens voor de beroepsgroep advocaten bij aangesloten. De beslissing over de invoering van de TIB is pas begin 2015 genomen.
Waar het gaat om de suggestie van het aanstellen van een 'public advocate' binnen de toezichtsstructuur merk ik, in aanvulling op hetgeen ik eerder in antwoord op vragen van leden van de D66-fractie heb gesteld, op, dat ik daar geen aanleiding toe zie. Ik ga er vanuit dat zowel de TIB als de CTIVD in het kader van de aan hen opgedragen taak, in staat zijn om bij de afweging van de in geding zijnde belangen het burgerperspectief adequaat te betrekken.

3.3.2.2 De instelling, taakstelling en samenstelling van de TIB (§3.3.3.2 m.v.t.)

De leden van de PvdA-fractie vragen of de TIB steeds als college beslist, dan wel of ook individuele leden van de TIB kunnen beslissen. Op grond van de voorgestelde regeling zal de TIB als college beslissen. Dat neemt niet weg, zoals ook in de memorie van toelichting (p. 54) is betoogd, dat de commissie de voorbereiding van het oordeel over een ter toetsing voorgelegd besluit kan toedelen aan een lid van de TIB. Het is echter aan de TIB om daar zelf afspraken over te maken. In artikel 35, eerste lid, van het wetsvoorstel is bepaald dat de TIB voor haar werkzaamheden een reglement van orde dient op te stellen, dat in de Staatscourant wordt geplaatst. Ik neem aan dat daarin wordt aangegeven op welke wijze zij intern de toetsing inricht. Op de vraag van deze leden of er de mogelijkheid bestaat om bij de TIB ook plaatsvervangende leden te benoemen, merk ik op dat het wetsvoorstel daarin niet voorziet. Er wordt van uitgegaan dat de TIB met drie leden en voldoende secretariële ondersteuning de aan haar opgedragen taak in beginsel moet kunnen uitvoeren. Daarbij is het wel van belang dat er sprake zal zijn van een in tijd gelijkmatig aanbod van te toetsen besluiten. Dat is niet alleen van belang om de werkzaamheden van de TIB beheersbaar te houden, maar ook de diensten hebben daar een duidelijk belang bij: immers, zolang de TIB een besluit tot inzet van een bijzondere bevoegdheid niet heeft kunnen toetsen zal deze – behoudens spoedgevallen – nog niet kunnen worden ingezet. Indien op enig moment zou blijken dat de TIB in de voorgestelde omvang (en samenstelling) haar taak niet naar behoren kan vervullen, dan zal daar een oplossing voor moeten worden gevonden. Introductie van de mogelijkheid tot het benoemen van plaatsvervangende leden vergt dan wel wetswijziging. De leden van de PvdA-fractie wijzen er voorts op dat de Raad voor de Rechtspraak (hierna: RvdR) aandacht vraagt voor het belang om "inkapseling" van de leden van de TIB te voorkomen. De RvdR acht het om die reden van belang dat wordt vastgesteld dat de leden niet worden herbenoemd. Het belang van het voorkomen van "inkapseling" wordt door mij gedeeld, maar anders dan de RvdR ben ik niet bevreesd dat dit zal gebeuren; ik zie ook niet in waarom in dat kader zou moeten worden afgezien van de mogelijkheid van (eenmalige) herbenoeming van leden van de TIB. Ook de leden van de CTIVD kunnen (eenmaal) worden herbenoemd en in de praktijk is dat ook een aantal keren gebeurd; ik heb niet de indruk dat de CTIVD – ongeacht de mogelijkheid van

herbenoeming – zich als toezichthouder heeft laten "inkapselen". Ik heb er alle vertrouwen in dat de onafhankelijke TIB zich dan ook niet in zal laten kapselen. De leden van de PvdA-fractie wijzen verder op het feit dat de RvdR nog meerdere vragen heeft over de omvang van de werkzaamheden, de vormgeving en de bemensing van de TIB. Deze leden vragen of hierover meer helderheid kan worden geboden. Een aantal van de door de RvdR opgeworpen kwesties zijn reeds hiervoor in antwoord op vragen van de leden van de fractie van de VVD aan de orde geweest. Dat betreft in ieder geval de verhouding van het oordeel van de TIB tot de ministeriële verantwoordelijkheid alsmede de samenstelling van de TIB en de benodigde expertise en ervaring. De vraag van de RvdR of is overwogen de TIB als een zelfstandige en onafhankelijke commissie te positioneren binnen de CTIVD kan ontkennend worden beantwoord. Een dergelijke constructie zou bovendien het eventuele en naar mijn mening onterechte negatieve beeld dat sommigen reeds hebben over de onafhankelijkheid en onbevooroordeeldheid van de CTIVD, die bestaat uit twee afdelingen (toezicht en klachtbehandeling) die in volstrekte onafhankelijkheid van elkaar de aan hen opgedragen taken zullen gaan vervullen, alleen maar versterken. Daar is de TIB noch de CTIVD bij gebaat. De leden van de PvdA-fractie vragen voorts – onder verwijzing naar de hoorzitting die de Tweede Kamer heeft gehouden en de daar ingebrachte position papers – naar de effectiviteit van de TIB; zij geven aan de zorgen van de RvdR in dat kader te delen. Meer in het bijzonder lijkt het hier te gaan om de vraag of de TIB aan het verzoek van de dienst en de toestemming van de minister kan opmaken of terecht gebruik is gemaakt van de bevoegdheid en of de TIB wel over voldoende informatie beschikt om dat te kunnen beoordelen. Allereerst wordt opgemerkt dat de TIB niet hoeft te beoordelen of terecht gebruik is gemaakt van de bevoegdheid, maar juist dient te oordelen of er gebruik gemaakt mag worden van een bevoegdheid waarvoor de minister toestemming heeft verleend. Voor dat laatste krijgt de TIB de beschikking over alle informatie die ook aan de minister is overgelegd in het kader van diens besluitvorming. Dat omvat in ieder geval de informatie die ingevolge artikel 29, tweede lid, van het wetsvoorstel in het verzoek om toestemming dient te worden opgenomen, inclusief de gemaakte afweging inzake noodzakelijkheid, proportionaliteit en subsidiariteit. In beginsel moet dat voor de te verrichte toets door de TIB voldoende zijn; hetgeen hier van de TIB wordt gevraagd wijkt in essentie niet af van wat bijvoorbeeld een rechter-commissaris doet indien deze een machtiging wordt gevraagd voor de inzet van bepaalde bijzondere opsporingsmethoden en waarbij deze ook "slechts" over de vordering van de officier van justitie beschikt. Mocht de TIB echter menen dat de ter beschikking gestelde informatie (nog) onvoldoende is voor een goede oordeelsvorming, dan heeft men de bevoegdheid om aanvullende informatie bij de minister op te vragen en deze is verplicht deze te verstrekken (artikel 36, eerste lid, van het wetsvoorstel). Voor deze taak is het niet nodig dat de TIB rechtstreeks toegang wordt verleend tot alle informatie die bij de diensten berust; het gaat immers telkens om een eenmalige toets aan de hand van een concreet verzoek. Rechtstreekse toegang tot bij de diensten berustende informatie is echter wel essentieel voor een goede taakvervulling door de CTIVD die toezicht houdt op de rechtmatige uitoefening van bijzondere bevoegdheden; dat heeft immers niet per definitie het karakter van een eenmalige toets op een bepaald moment, maar kan juist de uitoefening van een bijzondere bevoegdheid over een langere tijdspanne omvatten (monitoring). Zo wordt door de CTIVD de uitoefening van de bijzondere bevoegdheid tot interceptie van communicatie doorlopend gemonitored. Alles overwegende zie ik dan ook geen aanleiding om de voorgestelde regeling inzake de TIB ter zake aan te passen.

De leden van de PvdA-fractie wijzen erop dat de Raad voor de Rechtspraak de suggestie doet om de TIB als zelfstandige en onafhankelijke commissie binnen de CTIVD te positioneren en vraagt de regering om hierop in te gaan. Met het oog op de hierboven gegeven motivering acht ik de suggestie om de TIB als zelfstandige en onafhankelijke commissie binnen de CTIVD te positioneren onwenselijk.

De leden van de D66-fractie vragen waarom de leden van de TIB, voor zover rechterlijke ervaring vereist is, afkomstig moeten zijn uit de rechterlijke macht, en niet mede geworven kunnen worden onder de raadsheren bij de Afdeling bestuursrechtspraak van de Raad van State. Deze leden vragen zich voorts af aan wat voor expertise gedacht wordt voor het derde lid van de TIB. Wat het eerste punt betreft, ben ik het met deze leden eens dat ook bijvoorbeeld leden van de Afdeling bestuursrechtspraak van de Raad van State, maar ook leden van het College van Beroep voor het bedrijfsleven en leden van de Centrale Raad van Beroep, in aanmerking moeten kunnen komen voor benoeming in de TIB. In de bij deze nota gevoegde nota van wijziging wordt dan ook voorzien in aanpassing van artikel 33, tweede lid, van het wetsvoorstel. De mogelijkheid om een derde lid, niet zijnde een persoon met rechterlijke ervaring, te kunnen benoemen is geopend naar aanleiding van het advies van de Afdeling advisering van de Raad van State. Aldus wordt de mogelijkheid geopend een lid te benoemen die over de eventueel benodigde technische deskundigheid en inzicht in de veiligheidsrisico's beschikt. Deze deskundigheid kan natuurlijk ook reeds voorhanden zijn bij een persoon met rechterlijke ervaring die in de TIB wordt benoemd; in dat geval wordt de aanwezigheid van dergelijke kennis en expertise binnen de TIB langs die weg geborgd.

Deze leden vragen zich voorts af welke omvang het secretariaat zal hebben, en of de TIB net als de CTIVD ondersteunt zal worden door een team van onderzoekers- en juristen. Zo ja, welk budget staat daartegenover? Vragen betreffende het secretariaat heb ik hierboven reeds beantwoord. Voor het antwoord over het budget verwijs ik naar hetgeen ik in paragraaf 7.1.1 van deze nota heb gesteld.

3.3.2.3 De toetsing door de TIB (§3.3.3.3 m.v.t.)

De leden van de D66-fractie vragen zich af hoe het selectiecriterium "meest inbreuk makend op de persoonlijke levenssfeer" precies is toegepast. Zij vragen of er ter zake nota's beschikbaar zijn waarin de bevoegdheden volgens die meetlat beoordeeld zijn en waarbij is gekeken welke bevoegdheid wel en niet daaronder moest vallen? Zo ja, zouden deze nota's voor de Kamer beschikbaar zijn en, zo neen, hoe heeft die weging dan wel plaatsgevonden? Het selectiecriterium "meest inbreukmakend op de persoonlijke levenssfeer", of zoals het in de memorie van toelichting is gesteld "in potentie meest inbreuk makend op de persoonlijke levenssfeer", is aangewend om te bepalen voor welke bijzondere bevoegdheden de eis van toestemming van de minister zou moeten gelden (zonder de mogelijkheid van mandaat). Dit criterium heeft altijd een zeker arbitrair karakter. Dit is ook bij de totstandbrenging van de huidige wet onderkend. Zo is indertijd op vragen van leden van de fractie van het CDA gesteld "Alvorens meer concreet in te gaan op de vragen van deze leden, merken we het volgende op. In algemene zin geldt dat de toestemming voor de inzet van bijzondere bevoegdheden dient te worden genomen op het voor de desbetreffende bijzondere bevoegdheid meest in aanmerking komende niveau dat in de hiërarchie van de organisatie voldoende hoog is, en waarbij tevens rekening wordt gehouden met de eis dat de flexibiliteit van de inzet van dergelijke bevoegdheden op adequate wijze wordt gegarandeerd waardoor een

effectieve en tijdige taakuitvoering van de dienst mogelijk is. Hoewel naar ons oordeel het moeilijk is om in theoretische zin een rangorde aan te brengen tussen de verschillende bijzondere bevoegdheden waar het gaat om de mate van ingrijpendheid in de persoonlijke levenssfeer van burgers, hetgeen dan min of meer automatisch gevolgen zou dienen te hebben voor de vaststelling van het niveau waarop toestemming dient te worden verleend (hoe ingrijpender de bevoegdheid, hoe hoger in de organisatie de functionaris dient te worden aangewezen die voor de toepassing daarvan toestemming dient te verlenen), bestaat er naar ons oordeel wel een zekere consensus dat de uitoefening van bepaalde bevoegdheden – in het bijzonder die bevoegdheden die raken aan meer specifiek in de Grondwet uitgewerkte grondrechten, zoals die welke in artikel 12 en 13 zijn neergelegd – toestemming op hoger niveau vereisen dan de uitoefening van andere bevoegdheden."[5] Dat geldt in algemene zin ook voor de keuzes die zijn gemaakt in onderhavig wetsvoorstel (en die voortborduren op reeds in de huidige wet neergelegde keuzes van de wetgever), waarbij de keuze om in een bepaald geval de beslissing omtrent de uitoefening van een bepaalde bijzondere bevoegdheid – bijvoorbeeld het binnendringen in een geautomatiseerd werk – op het niveau van de minister te leggen, ook de resultante van een politiek en maatschappelijk debat ter zake kan zijn. In het ontwerp-wetvoorstel dat in consultatie is gegeven, is er indertijd vervolgens voor gekozen om alle bijzondere bevoegdheden waarvoor de minister toestemming zou moeten geven onder het heroverwegingsstelsel te brengen; dat stelsel is vervangen door een toetsing door de TIB zonder dat opnieuw expliciet is stilgestaan bij de vraag welke bijzondere bevoegdheden nu wel of niet ter toetsing aan de TIB zouden moeten worden voorgelegd. Notities waarin expliciet per bijzondere bevoegdheid een weging is gemaakt naar mate van ingrijpendheid op de persoonlijke levenssfeer zijn dan ook niet voorhanden.

Naar aanleiding van de vraag van de leden van de D66-fractie hoe de oordeelsvorming binnen de TIB zal plaatsvinden, merk ik op dat de TIB steeds als college zal dienen te beslissen of een door de minister verleende toestemming voor de uitoefening van een bepaalde bijzondere bevoegdheid rechtmatig kan worden geacht. Het wetsvoorstel voorziet er niet in dat dit oordeel aan een afzonderlijk lid van de TIB kan worden opgedragen. Op de vraag of de TIB bij unanimiteit of bij meerderheid besluit, laat het wettelijk stelsel alle ruimte voor de mogelijkheid van meerderheidsbeslissingen. De eis van unanimiteit is immers niet gesteld.

De leden van de fractie van D66 wijzen er vervolgens op dat de TIB geen volledige toegang heeft tot de systemen van de AIVD en MIVD, hetgeen de CTIVD wel heeft. Deze leden vragen in verband daarmee welke ruimte de regering gaat bieden aan het inwinnen van nadere informatie door de TIB, indien zij daar behoefte aan heeft. In artikel 36, eerste lid, van het wetsvoorstel is bepaald dat ten behoeve van de toetsing door de TIB de minister het aan de toestemming ten grondslag liggende verzoek alsmede diens besluit verstrekt. Desgevraagd verstrekken de ministers aan de TIB alle inlichtingen en verlenen haar alle overige medewerking die zij voor een goede uitoefening van haar taak noodzakelijk acht. In het wetsvoorstel is – anders dan bij de CTIVD – er niet in voorzien dat men ook informatie kan inwinnen bij derden. Gelet op de taak van de TIB acht ik het ook niet noodzakelijk dat men bij externe deskundigen nog nadere informatie kan inwinnen, mede om de benodigde vertrouwelijkheid en snelheid te garanderen. Het is de verantwoordelijkheid van de betreffende minister om de TIB te

[5] Kamerstukken II 1999/2000, 25 877, nr. 8, p. 45 e.v.

voorzien van alle relevante informatie die de TIB nodig heeft en nodig acht om tot oordeelsvorming te komen. Indien de TIB twijfelt over noodzaak, proportionaliteit en subsidiariteit zal men ter zake nader uitsluitsel dienen te verkrijgen bij de verantwoordelijke minister; indien deze de twijfel door het verstrekken van nadere informatie niet kan doen wegnemen, dan zal de TIB daar de conclusie aan moeten verbinden die zij meent daaraan te moeten verbinden. Als dat leidt tot een negatief – met redenen omkleed (artikel 36, derde lid) - oordeel van de TIB en de toestemming van de minister daarmee komt te vervallen, is het aan de minister om te beslissen of het besluitvormingstraject opnieuw wordt ingezet, waarbij hij de redenen waarom de TIB toestemming heeft geweigerd kan betrekken. Daar komt ten slotte bij, dat,ingeval de TIB externe deskundigen – bijvoorbeeld aanbieders van communicatiediensten – bij diens oordeelsvorming gaat betrekken, dit met zich meebrengt dat door de TIB met die derden staatsgeheime informatie (target, toe te passen bevoegdheid en andere informatie) zal moeten worden gedeeld; dat achten we zeer onwenselijk en zonder een wettelijke regeling die dat expliciet toelaat zou dat neerkomen op schending van de wettelijke plicht tot geheimhouding. De TIB moet zelf over de benodigde kennis en expertise beschikken om de aan haar opgedragen taak te kunnen verrichten. Min of meer in het verlengde van het voorgaande ligt de vraag van deze leden hoe binnen de toetsing van de TIB invulling kan worden gegeven aan het tegenspraak-principe door het inpassen van een publieksadvocaat. Het opnemen van een dergelijke persoon bij de TIB is bij de uitwerking van de voorstellen voor een TIB niet aan de orde geweest en derhalve ook niet overwogen. Anders dan bij het openen van de mogelijkheid tot het raadplegen van externe deskundigen, zou, ingeval de introductie van een dergelijke persoon binnen de TIB zou worden overwogen, deze een wettelijk geregelde status moeten krijgen; aanwijzing als vertrouwensfunctie is dan ook aangewezen. Nu echter de introductie van een dergelijke persoon, wat mij betreft, niet aan de orde is, kan de beantwoording van de vragen inzake de benodigde ervaring c.q. achtergrond voor een dergelijke functie en de daarmee samenhangende kosten achterwege blijven.

Tot slot stellen de leden van de fractie van D66 enkele vragen omtrent de opgenomen voorziening voor het in gevallen van onverwijlde spoed inzetten van een bevoegdheid alvorens de toestemming van de TIB is verkregen. Een voorziening waarvan ze aangeven dat ze begrijpen dat die is voorzien. Zij maken zich echter zorgen dat de gevolgen van een onterecht beroep op de spoedvoorziening niet in de wet zijn vastgesteld, maar ter beoordeling van de TIB staan. Om te voorkomen dat deze route ter omzeiling van de waarborgsystematiek gebruikt gaat worden, zou er duidelijkheid moeten bestaan over welke gevolgen daaraan verbonden dienen te worden voor de gegevens die zijn verzameld voorafgaand aan het oordeel van de toetsingscommissie. Zij geven voorts aan een exacte motivatie te verlangen waarom niet wettelijk is uitgesloten dat de inlichtingen- en veiligheidsdiensten kunnen worden beloond voor het omzeilen van de wet. Ik ben het niet met de opvatting van deze leden eens, dat de in artikel 37 opgenomen regeling voor spoedgevallen door de diensten zou kunnen worden gebruikt om de waarborgsystematiek te omzeilen. Bovendien zijn het dan niet zozeer de diensten die dan de waarborgsystematiek – in de termen van de leden van de D66-fractie – "zouden omzeilen" maar de ministers, immers die moeten in voorkomend geval al wel toestemming hebben verleend voor de uitoefening van de bijzondere bevoegdheid en er bovendien mee hebben ingestemd dat reeds voorafgaand aan de toets door de TIB met de uitoefening van de bijzondere bevoegdheid een aanvang kan worden gemaakt. De diensten zullen dan ook eerst de eigen minister daarvan dienen te overtuigen. Daarnaast voorziet de spoedregeling als zodanig ook in een aantal waarborgen, welke ertoe

bijdragen dat deze niet ingezet wordt in gevallen waarbij geen sprake is van een spoedgeval. Zo moet allereerst de toestemming van de minister onverwijld worden voorgelegd aan de TIB. Ten tweede moet het gebruik van de spoedvoorziening afzonderlijk worden gemotiveerd. Ten derde dient te TIB in haar oordeelsvorming de toepassing van de spoedvoorziening te betrekken. Vanwege het feit dat de toestemming onverwijld moet worden voorgelegd en ik er van uitga dat in dergelijke gevallen de TIB met voorrang naar dergelijke toestemmingen zal kijken, zal de tijdwinst van het gebruik van een spoedvoorziening beperkt zijn en alleen van belang zijn in echte spoedsituaties. De oordeelsvorming van de TIB kan vervolgens verschillende uitkomsten hebben: (1) de toestemming zelf is ten onrechte verleend, in welk geval ingevolge het derde lid alle reeds verzamelde gegevens dienen te worden vernietigd, (2) de toestemming was terecht en het beroep op spoed ook, waarbij de reeds verzamelde gegevens verder gebruikt mogen worden en (3) de toestemming is weliswaar terecht verleend, maar er was geen reden voor een beroep op de spoedvoorziening. In dat laatste geval, waarvoor artikel 37, vierde lid, een voorziening geeft, is het inderdaad aan de TIB gelaten om te bepalen welke gevolgen daaraan verbonden dienen te worden waar het gaat om de reeds verzamelde gegevens. Dit lijkt mij een alleszins redelijke gang van zaken, waarbij rekening kan worden gehouden met de bijzondere omstandigheden van het geval. Hier moet, rekening houdend met het belang van de nationale veiligheid, ruimte zijn voor maatwerk door de TIB. Het voorstel van de leden van de fractie van D66 om alle verworven gegevens terstond te vernietigen, eventuele verwerkingen ongedaan te maken en analyses voor zover gemaakt op grond van die verwerving en/of verwerking ongedaan te maken voor dat deel en dit ongeacht of de inzet onrechtmatig was, of dat enkel de betoonde haast dat was, schiet zijn doel voorbij. Tot slot wil ik nog opmerken dat een eventueel oneigenlijk gebruik van de spoedvoorziening door de minister niet onopgemerkt zal blijven. De TIB dient immers omtrent haar werkzaamheden jaarlijks een openbaar verslag uit te brengen. Het ligt voor de hand dat daarbij ook ingegaan wordt op de toepassing van de spoedvoorziening. Dit verslag wordt aangeboden aan de beide kamers der Staten-Generaal die vervolgens de minister aan de hand daarvan ter verantwoording kan roepen. Ook de CTIVD die toezicht houdt op de uitvoering van de bijzondere bevoegdheden kan daaromtrent haar bevindingen aan de minister mededelen, al dan niet met het verzoek dit door te zenden aan de beide kamers, of in een toezichtsrapportage daaromtrent rapporteren.

De leden van de fractie van de ChristenUnie vragen of de TIB straks toegang heeft tot alle relevante informatie die nodig is om tot een goed en onafhankelijk advies te komen. Ik merk allereerst op dat de TIB niet met een advies komt, maar met een bindend oordeel. Op de vraag inzake de benodigde informatie verwijs ik deze leden naar hetgeen eerder in reactie op vragen van de leden van de D66-fractie is geantwoord. Ik constateer overigens dat ook experts – zie de reacties op het toezichtstelsel in brede zin en de interpretatie van de jurisprudentie van het EHRM ter zake – niet tot een eensluidende opvatting ter zake komen.
Tot slot vragen de leden van deze fractie op welke wijze en in welke mate informatie over het voorafgaande toezicht openbaar gemaakt zal worden. Worden, aldus de aan het woorden zijnde leden, het aantal afgewezen en toegewezen verzoeken tot toestemming openbaar gemaakt. De TIB heeft, evenals de CTIVD, de plicht om jaarlijks voor 1 mei een openbaar verslag van werkzaamheden uit te brengen (artikel 35, derde lid, jo. 132 van het wetsvoorstel). Daarbij is bepaald dat artikel 12, derde en vierde lid, van het wetsvoorstel van overeenkomstige toepassing is verklaard. Ingevolge artikel 12, derde lid, dient vermelding van in ieder geval de gegevens die zicht geven op door de dienst

aangewende middelen in concrete aangelegenheden, door de diensten aangewende geheime bronnen en het actuele kennisniveau van de dienst achterwege te blijven. Gegevens die zicht geven op de mate waarop door de dienst van een bepaalde bijzondere bevoegdheid gebruik wordt gemaakt, geven zicht op door de diensten aangewende geheime bronnen en worden als staatsgeheim aangemerkt. Dit is dus een kritische ondergrens die de TIB bij de verantwoording van haar werkzaamheden in acht heeft te nemen. Dat laat naar mijn oordeel nog voldoende ruimte om – met inachtneming van het bepaalde in artikel 12, derde lid - op een adequate wijze te rapporteren over de door de TIB verrichte voorafgaande toets op door de minister verleende toestemmingen voor de inzet van bijzondere bevoegdheden.

3.3.3 De bevoegdheden inzake de verzameling van gegevens (§3.3.4 m.v.t.)

3.3.3.1 Het stelselmatig verzamelen van gegevens over personen uit open bronnen (§3.3.4.2 m.v.t.)

De leden van de D66-fractie merken op dat expliciet wordt vastgelegd dat het toegestaan is om stelselmatig gegevens te verzamelen over personen uit open bronnen. Deze leden wijzen op het feit dat niet alles wat op het internet staat waar is en vragen de regering op welke wijze wordt geborgd dat hetgeen het algoritme uit die open bronnen bijeenbrengt ook daadwerkelijk een weergave van de werkelijkheid is. Daarnaast vragen deze leden zich af hoe een "open bron" afgebakend is. Het gegeven dat zoekslagen op internet niet per definitie op waarheid berustende feiten opleveren is mij bekend. Dit geldt (in meer of mindere mate) ook voor het door de diensten door middel van de inzet van inlichtingenmiddelen verwerven van gegevens. Niet elke bron van de diensten (open en gesloten, technisch en menselijk enz.) en daarmee de op basis van deze bron verkregen gegevens, wordt als zonder meer betrouwbaar beschouwd. De diensten zullen dan ook altijd trachten gegevens nader te verifiëren, bijvoorbeeld door deze op basis van informatie uit andere bronnen te bevestigen. Zowel de huidige wet als het wetsvoorstel vereisen dat gegevens die door de diensten worden verwerkt zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend.
Met open bron wordt geduid op een voor eenieder toegankelijke informatiebron, bronnen die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan. Open bronnen vormen één van de in artikel 25 genoemde categorieën gegevens. De door de D66-fractie geschetste voorbeelden betreffen geen open bronnen en worden dat evenmin door de inzet van een bijzondere bevoegdheid.

De leden van de D66-fractie hebben gevraagd hoe de bevoegdheid tot het stelselmatig uit open bronnen verzamelen van gegevens over personen te vergelijken is met de bevoegdheid tot het observeren en volgen van personen. Over het algemeen zal het verzamelen van persoonsgegevens uit open bronnen (zoals kranten, tijdschriften, (het openbare deel van het) internet) niet tot een noemenswaardige inbreuk op iemands privacy leiden, maar dat wordt anders als dit op een stelselmatige wijze plaatsvindt. Ik acht het daarom noodzakelijk in artikel 38 van het wetsvoorstel een expliciete grondslag voor het stelselmatig uit open bronnen verzamelen van gegevens omtrent personen op te nemen, inclusief toestemmingsregime. Dit zal veelal historische gegevens betreffen, bijvoorbeeld de berichten die door een onderzoekssubject werden gepost of diens profiel op een bepaald sociaal medium. Deze bevoegdheid zal bijvoorbeeld gedurende een veiligheidsonderzoek worden ingezet om een zo volledig mogelijk beeld te verkrijgen van

de persoon die een vertrouwensfunctie binnen de Nederlandse overheid ambieert. Deze (algemene) bevoegdheid dient te worden onderscheiden van de (bijzondere) bevoegdheid tot het observeren en volgen van personen zoals deze in artikel 40 van het wetsvoorstel wordt geregeld. Hierbij zal het veelal gaan om toekomstgerichte activiteiten: welke handelingen zal het onderzoekssubject in het reële dan wel digitale domein ontplooien? Bij observeren en volgen conform artikel 40 gaat het om het feitelijk waarnemen van een persoon of een situatie. Het doel is primair om vast te stellen wat iemand gaat doen. Er wordt geen onderscheid gemaakt tussen het observeren en volgen van gedragingen in het fysieke dan wel digitale domein. Voor beide middelen geldt dat een voorafgaande toets dient plaats te vinden ten aanzien van noodzakelijkheid, proportionaliteit en subsidiariteit in het verzoek tot toestemming en dat toestemming dient te worden verleend door de betrokken minister of het diensthoofd, met de mogelijkheid van ondermandaat. Beiden kunnen voor een periode van ten hoogste drie maanden worden ingezet en kunnen op verzoek worden verlengd.

De leden van de GroenLinks-fractie hebben gevraagd of het raadplegen van eenieder toegankelijke bronnen niet zo laagdrempelig mogelijk moet worden ingericht, teneinde te voorkomen dat zwaardere bevoegdheden worden ingezet om hetzelfde doel te bereiken. De diensten zijn op grond van het voorgestelde artikel 25 bevoegd tot (onder andere) het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen. Naar aanleiding van het Privacy Impact Assessment is in artikel 38 van het wetsvoorstel voorzien in een regeling voor het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen. Vanwege het stelselmatige karakter van deze bevoegdheid en de implicaties die dat heeft voor de privacy van de betrokken persoon is bepaald dat de uitoefening van deze bevoegdheid slechts is toegestaan met toestemming van de voor de dienst verantwoordelijke minister of namens deze het hoofd van de dienst (met de mogelijkheid van ondermandaat). De geuite vrees dat zwaardere, bijvoorbeeld bijzondere, bevoegdheden door de diensten zouden worden ingezet om dergelijke informatie te verwerven acht ik ongegrond, nu deze nimmer de subsidiariteitstoets zouden doorstaan.

3.3.3.2 De raadpleging van informanten (§3.3.4.3 m.v.t.)

De leden van de D66-fractie geven aan uit het voorliggende wetsvoorstel te begrijpen dat informanten ook rechtstreeks en geautomatiseerd geraadpleegd kunnen worden. Deze leden vragen zich af hoe die bevoegdheid, zoals neergelegd in artikel 39, zich verhoudt tot de bevoegdheid tot het binnendringen in een geautomatiseerd werk en tot het interceptiestelsel. Klopt het, aldus deze leden, dat een eerste verschil gelegen is in het feit dat in tegenstelling tot hacken en interceptie de informatie bewust en op vrijwillige basis verstrekt wordt? Hoe is in dat geval in het voorliggende wetsvoorstel die vrijwilligheid daadwerkelijk gewaarborgd? Deze leden zien het juist dat artikel 39 ook de mogelijkheid expliciteert dat ingeval door een informant wordt meegewerkt aan een verzoek tot verstrekking van gegevens, dat dat ook via de weg van het verlenen van rechtstreeks geautomatiseerde toegang tot die gegevens kan. Dit alles echter op basis van vrijwilligheid en ook ter discretie van de informant. Dit kan niet worden afgedwongen. Deze situatie is te onderscheiden van de toepassing van het binnendringen van een geautomatiseerd werk en de interceptie van communicatie, omdat het daarbij gaat om bijzondere bevoegdheden die jegens het target op een heimelijke wijze worden ingezet en waarbij in sommige gevallen, zoals bij interceptie, er een verplichting tot medewerking bestaat die strafrechtelijk is gesanctioneerd.

De leden van de D66-fractie zijn in dit kader ook benieuwd of het doen van een verzoek op grond van artikel 39 is uitgesloten, indien ook de mogelijkheid openstaat betreffende informatie te verkrijgen op grond van de bevoegdheden opgenomen in de paragrafen 3.2.5.5 en 3.2.5.6 van de memorie van toelichting. Op welke wijze komt de gedachte dat de route van de sterkste waarborg gekozen wordt, indien gekozen kan worden tussen verschillende bevoegdheden die tot zelfde informatie leiden, in het wetsvoorstel tot uitdrukking? Bij de inzet van bevoegdheden wordt steeds die bevoegdheid gebruikt die proportioneel en subsidiair is. Als een middel ingezet kan worden dat minder nadeel oplevert voor betrokkene, dan zal dat gebruikt worden door de diensten conform het vereiste van artikel 26. In artikel 39 ligt een bevoegdheid die net als de bijzondere bevoegdheden onderworpen is aan de vereisten van noodzaak, proportionaliteit en subsidiariteit. Het is echter geen bijzondere bevoegdheid en de inzet ervan zal in het algemeen als minder inbreukmakend kunnen worden gezien.

De leden van de GroenLinks-fractie hebben gevraagd de keuze voor de bevoegdheid tot het rechtstreekse toegang verschaffen tot de geautomatiseerde gegevensbestanden van bestuursorganen en andere organisaties nader te onderbouwen. In artikel 39, derde lid, van het wetsvoorstel is bepaald dat aan een verzoek om gegevensverstrekking kan worden voldaan door het verlenen van rechtstreeks geautomatiseerde toegang tot de desbetreffende gegevens dan wel door het verstrekken van geautomatiseerde gegevensbestanden. De genoemde rechtstreekse toegang –die louter op vrijwillige basis kan worden overeengekomen – is met name van belang in de gevallen waarbij het voorzienbaar is dat in het kader van een goede taakuitvoering het wenselijk is dat de diensten structureel de beschikking hebben over (actuele) gegevens die bij een persoon of instantie beschikbaar zijn. Een voorbeeld hiervan vormt de toegang binnen het kader van de CT Infobox tot de daarvoor in aanmerking komende gegevens bij de aangesloten partners ten behoeve van de samenwerking in de CT Infobox. Er is voorzien in nadere regelstelling bij of krachtens algemene maatregel van bestuur waar het gaat om de te treffen technische en organisatorische maatregelen inzake rechtstreeks geautomatiseerde toegang. Evenals het huidige artikel 17 Wiv 2002 wordt deze bevoegdheid beschouwd als een algemene bevoegdheid tot het verwerven van gegevens, welke – zoals iedere bevoegdheid - dient te voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De CTIVD kan ingeval een dergelijke rechtstreeks geautomatiseerde toegang is gerealiseerd erop toezien dat aan de wettelijk gestelde eisen ter zake wordt voldaan.

3.3.3.3 De bijzondere bevoegdheden tot verzameling van gegevens door diensten (§3.3.4.4 m.v.t.)

De leden van de D66-fractie lazen in het evaluatierapport van de Commissie Dessens de aanbeveling om de indringendheid van kennisname van communicatie, en niet meer het transportmedium of de stand der techniek, bepalend te laten zijn voor de toestemmingsvereisten en het toezicht op rechtmatigheid. Deze leden krijgen de indruk dat dit wel is gepoogd, maar niet is gelukt. De leden van de D66-fractie vragen de regering daarom om een gedetailleerde analyse van de manier waarop met technologische ontwikkelingen, die een diepgaander en indringender gebruik van bijzondere bevoegdheden mogelijk maakt, omgegaan zal worden. De technologische ontwikkelingen, voornamelijk in het kabelgebonden domein, in combinatie met het dreigingsbeeld stellen de diensten voor grote uitdagingen. Dergelijke ontwikkelingen zijn nu al van groot belang voor de goede taakuitvoering door de diensten, en zullen in de

toekomst een belangrijk aandachtspunt blijven. Het feit dat de makers van de huidige wet nooit rekening hebben kunnen houden met deze nieuwe realiteit, vormt een belangrijke reden om de Wiv 2002 te herzien.

Het is een gegeven dat de diensten, met inachtneming van het wettelijk kader, bij de inzet van bijzondere bevoegdheden de mogelijkheden die nieuwe technologische toepassingen bieden, benutten. Indien zij dat niet zouden doen, heeft dat ernstige gevolgen voor de informatiepositie van de diensten. Voor zover het ontwikkelingen betreft die een diepgaandere en indringendere gebruik van bijzondere bevoegdheden mogelijk maakt, zal altijd sprake zijn van ministeriële toestemming, waarbij in de aanvraag daarvoor een toets op noodzaak, subsidiariteit en proportionaliteit zal plaatsvinden. Vervolgens geldt in geval van bijzondere bevoegdheden, zoals onder andere onderzoeksopdrachtgerichte interceptie, gerichte interceptie en bij het binnendringen van een geautomatiseerd werk, altijd een voorafgaande rechtmatigheidstoets door de TIB met bindend oordeel. Ook kan de CTIVD toezicht houden tijdens (en na) het in het kader van de inzet van een bijzondere bevoegdheid toepassen van een dergelijke nieuwe technologie.

Deze leden vragen zich voorts af of er technische hulpmiddelen zijn, al dan niet aan het internet gekoppeld, waarvan de regering bereid is op voorhand het hacken of aftappen ervan uit te sluiten? Ik ben geen voorstander van het aanleggen van een limitatieve lijst van technische hulpmiddelen die uitgesloten moet worden. Juist omdat niet te voorspellen is welke technologische ontwikkelingen zich in deze snel veranderende omgeving de komende jaren zullen voordoen acht ik het bij voorbaat uitsluiten van technische hulpmiddelen onverantwoord. Het doel van het wetsvoorstel is immers om een zo techniekonafhankelijk kader te bieden. Voorts staat het naar mijn mening het recht op lichamelijke integriteit van personen buiten twijfel en zal de inzet van een bijzondere bevoegdheid die daar een inbreuk op maakt niet voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Van een dergelijke inzet kan dus nu of in de toekomst geen sprake zijn.

Voorts waren de leden van de D66-fractie enige tijd geleden verbaasd door het CTIVD-toezichtsrapport nr. 46 waaruit bleek dat de AIVD een nieuwe specifieke technische toepassing van de afluisterbevoegdheid gevonden had. De Kamerleden zijn vertrouwelijk geïnformeerd door de CTIVD over deze onderzoeksmethode, maar deze leden vragen zich af of dergelijke toepassing niet door de regering gemeld had moeten worden. Een regeling daarvoor heeft het lid Verhoeven van de D66-fractie opgenomen in het amendement over de informatiebronnen waaruit de diensten gegevens kunnen verzamelen (Kamerstukken II 2016/17, 34 588, nr.9). Deze leden vragen of de regering het uitgangspunt deelt dat bijzondere bevoegdheden die door de diensten ingezet worden op zijn minst bij de Kamer bekend moeten zijn, dat over de inzet ervan en bijhorende waarborgen een debat gevoerd moet worden, dat een nieuwe meer vergaande invulling van een bevoegdheid feitelijk op een nieuwe bevoegdheid neerkomt en dat daarbij een nieuwe afweging moet plaatsvinden van de bijhorende waarborgen en toetsing aan subsidiariteit en proportionaliteit? Ik deel het uitgangspunt dat de bijzondere bevoegdheden die door de diensten kunnen worden ingezet bij het parlement bekend moeten zijn en dat over de inzet ervan en de benodigde waarborgen een open debat gevoerd kan worden. Sterker nog: als het gaat om *bijzondere bevoegdheden*, zijn die in de Wiv limitatief vastgelegd en een nieuwe *bijzondere bevoegdheid* zou dan ook eerst wettelijk geregeld moeten worden. Het betoog dat een nieuwe meer vergaande

invulling van een (bestaande) bijzondere bevoegdheid feitelijk neerkomt op een nieuwe bevoegdheid deel ik niet. De bevoegdheid wordt begrensd door de wet zoals wij die met elkaar vastleggen. Een technische toepassing die ingezet kan worden in het kader van de uitvoering van die wettelijk vastgelegde bijzondere bevoegdheid zal vervolgens afgewogen worden langs de waarborgen zoals vastgelegd in de wet, waarbij zoals altijd de reguliere toets aan noodzakelijkheid, proportionaliteit en subsidiariteit plaatsvindt. Voorts merk ik op, dat, als het gaat om de concrete werkwijze waarmee de diensten uitvoering geven aan deze bevoegdheden, het niet past om voorafgaand aan het gebruik ervan de Tweede Kamer in het openbaar te informeren en daarover een open debat te voeren. Juist deze technische toepassingen raken de kern van de werkwijze, de modus operandi, van de inlichtingen- en veiligheidsdiensten. Die zijn als staatsgeheim gekwalificeerd. Indien deze werkwijzen in de openbaarheid worden gebracht, kunnen de targets van de diensten immers hun voordeel hiermee doen door daarop hun gedrag aan te passen. Het door het lid Verhoeven ingediende amendement, waarbij verplicht wordt om een nieuwe specifieke technische toepassing van een bijzondere bevoegdheid die een substantiële en vergaande inbeuk op de persoonlijke levenssfeer kan inhouden – al dan niet vertrouwelijk- aan beide Kamers der Staten-Generaal te melden, ontraad ik. Het door de leden aangehaalde voorbeeld inzake CTIVD toezichtsrapport nr. 46 bewijst dat de huidige toezichtspraktijk en toepassing van benodigde waarborgen al sinds 2002 functioneert. De toegepaste techniek is door de toezichthouder onderkend, de wijze waarop de toepassing feitelijk wordt gebruikt is onderzocht door de toezichthouder, over de toepassing is zowel in het openbaar als in de beslotenheid gerapporteerd aan de Tweede Kamer en de met de toepassing gepaard gaande aanvullende waarborgen zijn overgenomen in de werkwijze van de diensten. Ik zie dan ook geen aanleiding om in dit proces wijzigingen aan te brengen.

De leden van de D66-fractie hebben een groot aantal vragen gesteld over het departementale proces met betrekking tot het verlenen van ministeriële toestemming voor de inzet van bijzondere bevoegdheden. Ik reageer daarop als volgt.
De inzet van bijzondere bevoegdheden wordt op meerdere momenten vooraf getoetst. Binnen de AIVD en MIVD vindt de primaire toets plaats van de noodzaak van het inzetten van een bijzondere bevoegdheid, alsmede de toets van proportionaliteit en subsidiariteit. De diensten maken de initiële afweging of inzet van een bijzondere bevoegdheid nodig is of niet. De beoordeling vindt plaats door het team of bureau dat overweegt de bijzondere bevoegdheid in te zetten, de juridische afdeling van de dienst en de directie. Er zijn derhalve meerdere functionarissen betrokken bij de advisering van de aanvraag.
Indien de minister van Defensie toestemming dient te verlenen, wordt nadat binnen de MIVD de aanvraag voor toestemming is getoetst en akkoord is bevonden, deze voorgelegd aan de secretaris-generaal (SG) van het ministerie van Defensie. Afhankelijk van de aard van de bijzondere bevoegdheid en het onderzoek beslaat het verzoek tot instemming gemiddeld meerdere pagina’s aan motivering en toelichting. De Directie Juridische Zaken (DJZ) van het ministerie van Defensie verricht voor de secretaris-generaal de juridische toets. Naast toetsing aan de beginselen van proportionaliteit en subsidiariteit wordt gekeken of de grondslag voor de bevoegdheid juist is en of wordt voldaan aan de wettelijke eisen. Binnen DJZ is één functionaris belast met het toetsen van de lasten waarbij voorzien is in een achtervang. Binnen het bureau SG beoordeelt eveneens één functionaris de lasten en deze kunnen dan naar de secretaris-generaal en de minister.

Indien de minister van Binnenlandse Zaken toestemming dient te verlenen wordt de aanvraag, nadat deze binnen de AIVD is getoetst door de eigen afdeling Juridische Zaken en akkoord is bevonden door de directeur-generaal van de AIVD, voorgelegd aan de minister. De directeur-generaal van de AIVD en de minister van BZK hebben regelmatig contact, waarbij ook de voorhanden lasten worden besproken en de minister vervolgens besluit. Wanneer de minister van BZK het bij de beoordeling van een last noodzakelijk acht, kan hij een beroep doen op ondersteuning van de secretaris-generaal en een ondersteunend cluster.

De leden van de fractie van D66 vragen voorts naar de bijzondere bevoegdheden waarvoor de minister persoonlijk toestemming dient te verlenen – onder de huidige wet en onder het wetsvoorstel – en de mogelijkheden van mandaat. Waar het gaat om het verlenen van toestemming voor de inzet van bijzondere bevoegdheden is op basis van de huidige Wiv 2002 aan de minister voorbehouden het verlenen van toestemming voor de inzet van een gerichte tap, de selectie van ongericht ontvangen etherverkeer aan de hand van identiteitsgegevens, een nummer als bedoeld in artikel 1.1, onder bb van de Telecommunicatiewet, danwel enig technisch kenmerk of zo'n selectie aan de hand van trefwoorden. Voorts wanneer het inzet van een bijzondere bevoegdheid betreft binnen een woning. Ten aanzien van het verlenen van toestemming met betrekking tot de bevoegdheid tot observatie, de inzet van agenten, het doorzoeken van besloten plaatsen en gesloten voorwerpen en de bevoegdheid tot hacken laat de Wiv 2002 mandaat toe. Op grond van artikel 19, tweede lid, van de huidige Wiv 2002 kan het hoofd van een dienst aan hem ondergeschikte ambtenaren bij schriftelijk besluit aanwijzen die de toestemming namens hem kunnen verlenen. De wet biedt hier derhalve de mogelijkheid tot ondermandaat. Ondermandatering heeft plaatsgevonden in het Mandaatbesluit bijzondere bevoegdheden AIVD 2015 respectievelijk de Mandaatregeling Defensie Wiv 2002. Ingevolge de Mandaatregeling Defensie Wiv 2002 is het verlenen van toestemming aan de minister van Defensie voorbehouden indien de toestemming in het concrete geval voor de eerste keer wordt verleend of de inzet principieel of politiek gevoelig van aard is.
Ingevolge het Mandaatbesluit BZK 2012 wordt aan het diensthoofd mandaat verleend ten aanzien van aangelegenheden die behoren tot het werkterrein van het diensthoofd en die, onverminderd het bepaalde in dit besluit, redelijkerwijs niet behoren te worden voorgelegd aan een hoger bevoegd gezag.
Anders dan in de huidige wet is bepaald, is – met uitzondering van de toestemmingverlening in bijzondere gevallen (artikel 30) – bij iedere bijzondere bevoegdheid aangegeven welke persoon of instantie bevoegd is toestemming te verlenen voor de uitoefening van de desbetreffende bijzondere bevoegdheid alsmede of en, zo ja, in hoeverre de mogelijkheid tot mandaat bestaat. Hierbij zij verwezen naar bijlage 3 van de memorie van toelichting waarin schematisch is aangegeven wanneer uit de wet voortvloeit dat een toestemming voor uitoefening van een bijzondere bevoegdheid door de minister zelf moet worden verleend en wanneer het wetsvoorstel ruimte biedt voor mandaat. In hoeverre ook daadwerkelijk gebruik zal worden gemaakt van een mandaatmogelijkheid zal worden bezien bij het opstellen van een nieuwe mandaatregeling.

Voor wat betreft de vraag van de leden van de D66-fractie naar de ontwikkeling van het aantal verzoeken om ministeriële toestemming kan ik in het openbaar geen mededeling doen. Voor het beeld inzake de inzet over de afluisterbevoegdheid door de AIVD wordt verwezen naar de CTIVD-rapporten nr. 40 en nr. 46.

3.3.3.3.1 Agenten (§3.3.4.4.3 m.v.t.)

De leden van de D66-fractie lezen dat diensten natuurlijke personen onder een dekmantel van een aangenomen identiteit en hoedanigheid mogen inzetten. Deze leden vragen zich af of weleens een bestaande identiteit wordt aangenomen. Zo nee, zo vragen deze leden, waarom is dit dan niet uitgesloten in het voorliggende wetsvoorstel? Zo ja, welke afweging wordt hierbij gemaakt? Op welke wijze wordt te zijner tijd de nagespeelde persoon daarvan op de hoogte gesteld? Hoe wordt gemonitord welke effecten dit kan hebben? Bestaat er een recht op schadevergoeding? Zo ja, hoe wordt dat gegeven het geheime karakter van een agentenoperatie geëffectueerd? Ik antwoord op deze vragen als volgt. Wanneer de inlichtingen- en veiligheidsdiensten natuurlijke personen onder een dekmantel van een aangenomen identiteit en hoedanigheid inzetten, wordt daarvoor een nieuwe identiteit ontworpen. Het gebruik van een bestaande identiteit kan het risico van persoonsverwisseling doen ontstaan, en dit is zowel vanuit het oogpunt van rechtmatigheid als vanuit operationeel perspectief onwenselijk. Evenwel valt niet uit te sluiten dat zich een bijzonder geval aandient waarin een identiteit dient te worden aangenomen die geheel, deels of overwegend samenvalt met een bestaand persoon. In dat geval zal worden overwogen of dit voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Er zal bijvoorbeeld sprake moeten zijn van een concrete en acute dreiging die niet op een andere manier kan worden weggenomen. De nagespeelde persoon zal hiervan enkel op de hoogte kunnen worden gesteld indien dit de wettelijk te beschermen belangen van het actueel kennisniveau, de werkwijze en bronnen niet in gevaar brengt. In ieder geval zal een verplichting op de diensten rusten om eventuele negatieve effecten of schade voor de nagespeelde persoon zoveel als mogelijk te beperken of weg te nemen. De CTIVD kan hierop toezicht uitoefenen en erover rapporteren aan het parlement.

De leden van de SP-fractie hebben diverse vragen gesteld over de wenselijkheid om journalisten en hulpverleners te kunnen inzetten als agent. Het uitgangspunt is en moet blijven dat de diensten zich voor de uitvoering van hun wettelijke taken kunnen richten tot eenieder die zou kunnen beschikken over de noodzakelijke gegevens. Op dit principe een beperking aanbrengen acht ik onverantwoord. Zo is goed denkbaar dat juist een hulpverlener van een geradicaliseerd persoon te horen kan krijgen welke geweldsdaad deze van plan is te plegen of dat juist een persoon die ook journalistieke activiteiten verricht zich in een uitzonderlijk geval in een positie bevindt om informatie te verkrijgen over een regime dat bezig is met de verwerving van massavernietigingswapens. Dan moeten de diensten de mogelijkheid hebben deze persoon in te zetten als agent. Niemand kan worden verplicht om te functioneren als informant of agent. Informanten en agenten helpen de diensten bij de uitvoering van hun wettelijke taken op basis van vrijwilligheid.

3.3.3.3.2 Onderzoek van besloten plaatsen, van gesloten voorwerpen, aan voorwerpen en DNA-onderzoek (§3.3.4.4.4 m.v.t.)

De leden van de SP-fractie vragen om een nadere toelichting op de keuze om bij DNA-onderzoek niet te kiezen voor een actieve notificatieplicht. Ik verwijs deze leden graag naar hetgeen in paragraaf 3.4 van deze nota naar aanleiding van het verslag, in reactie op vragen van de leden van de D66-fractie, in meer algemene zin wordt gesteld inzake

onder meer de reikwijdte van de notificatieplicht. De hier aan het woord zijnde leden vragen voorts waar zij aan moeten denken bij het terugplaatsen van een voorwerp dat DNA-materiaal bevat. Gelet op de afscherming van de modus operandi van de diensten, kan ik niet tot in detail ingaan op vragen omtrent in welke situaties voorwerpen wel of niet zullen worden teruggeplaatst. Wel kan ik in zijn algemeenheid aangeven dat terugplaatsing door de diensten achterwege blijft indien er geen redelijk belang mee is gediend: hierbij moet met name worden gedacht aan het belang van de eigenaar van het meegenomen voorwerp. Terugplaatsing zal tevens achterwege blijven indien dit in strijd zou zijn met een goede taakuitvoering door de dienst, bijvoorbeeld indien de gerede verwachting bestaat dat hiermee de operatie wordt onderkend.

De leden van de D66-fractie constateren dat het wetsvoorstel een expliciete basis gaat bieden voor het verrichten van DNA-onderzoek aan celmateriaal gericht op de vaststelling en de verificatie van de identiteit van een persoon. Zij stellen vast dat daarmee wordt tegemoet gekomen aan CTIVD-rapport nr. 42, waarin geconcludeerd wordt dat hiervoor een expliciete wettelijke basis nodig is. Ze vragen echter of aan alle aanbevelingen in de volle breedte is voldaan. Zij achten de waarborgen in de wet slechts procedureel van aard (toestemming minister) maar de CTIVD wijst op waarborgen voor gebruik en toegang tot derden. Welke materiële waarborgen bestaan er, zo vragen deze leden. Voorts zijn deze leden benieuwd naar de voorgenomen inhoud van de voor te hangen algemene maatregel van bestuur. In artikel 43 van de Wiv is omschreven voor welk doel (identificatie en verificatie) DNA-celmateriaal mag worden onderzocht en onder welke voorwaarden. Voor het onderzoek moet toestemming zijn verleend door de minister naar aanleiding van een verzoek daartoe. Het derde lid van artikel 43 beschrijft aan welke (aanvullende) voorwaarden het verzoek moet voldoen. Voor de verdere verwerking van de resultaten van het onderzoek is eveneens toestemming van de minister vereist naar aanleiding van een daartoe strekkend verzoek dat eveneens moet zijn gespecificeerd. Naar mijn oordeel is daarmee voldaan aan de eis dat een voldoende specifieke wettelijke grondslag wordt gegeven voor verstrekking aan derden van onderzoeksresultaten. Het betreft geen uitputtende regeling, enerzijds omdat die niet is vereist en anderzijds met het oog op de uiteenlopende gevallen in de praktijk en de mate van gedetailleerdheid ook niet zinvol is om dit in de wet zelf uitputtend te omschrijven.
Waar het gaat om de voorziene algemene maatregel van bestuur, die zoals door deze leden is aangegeven is onderworpen aan een voorhangprocedure, kan ik melden dat – in lijn met de delegatiegrondslag – daarin nadere regels worden gesteld inzake de bemonstering, het administreren van de uitoefening van de bevoegdheid tot DNA-onderzoek (ook met het oog op interne verantwoording en effectief toezicht door de CTIVD), de profilering van celmateriaal, de registratie en vergelijking van DNA-profielen (met name de inrichting van een DNA-profielenregistratie) alsmede nadere regels inzake de verdere verwerking van de in het kader van DNA-onderzoek verkregen gegevens. Omtrent de ontwerp-algemene maatregel van bestuur vindt interdepartementaal overleg plaats. De in artikel 43 neergelegde normen in combinatie met de inhoud van genoemde algemene maatregel van bestuur brengen naar mijn oordeel met zich mee dat het DNA-onderzoek van adequate materiële waarborgen is voorzien.

De leden van de D66-fractie hebben diverse vragen gesteld over de bruikbaarheid van de resultaten van onderzoek naar vingerafdrukken in de praktijk en hoe dit zich verhoudt tot andere vormen van onderzoek aan een voorwerp, gericht op de vaststelling van de identiteit van een persoon, meer specifiek in relatie tot het gebruik van DNA materiaal.

Het op heimelijke wijze op locatie zichtbaar maken van vingerafdrukken kan in de operationele praktijk van de diensten veel gecompliceerder blijken te zijn dan het veiligstellen van celmateriaal, met name wanneer die vingerafdrukken zich niet op een makkelijk (tijdelijk) verwijderbaar voorwerp bevinden, maar bijvoorbeeld op een meubelstuk of een deurkozijn. In dergelijke gevallen is voor het zichtbaar maken in de regel poeder of een chemische behandeling noodzakelijk. De behandelde voorwerpen moeten na onderzoek gereinigd worden, hetgeen niet altijd mogelijk is in de praktijk van de inlichtingen- en veiligheidsdiensten. Ten tweede kunnen vingerafdrukken in principe alleen zichtbaar worden gemaakt op voorwerpen die niet poreus zijn, een glad oppervlak hebben en groot genoeg zijn om een vingerafdruk op te plaatsen. Ten derde is een zichtbaar gemaakt vingerafdrukspoor niet altijd geschikt voor identificatie. Het spoor moet aan de kwaliteitseisen voldoen (er moeten 12 dactyloscopische punten in het spoor aanwezig zijn). Ten vierde is het onderling vergelijken van aangetroffen vingerafdrukken in verschillende onderzoeken niet altijd mogelijk, als je niet beschikt over een 10-vingerafdrukkenblad van een target. Er wordt immers niet altijd een afdruk van dezelfde vinger aangetroffen. Het heimelijk veiligstellen van celmateriaal is eenvoudig uit te voeren en laat geen sporen na. Als bij een DNA-onderzoek een DNA-profiel wordt verkregen, krijg je altijd hetzelfde DNA-profiel: of dit nu afkomstig is van speeksel, huidepitheel, etc. Daardoor is de vergelijking altijd mogelijk. De betrouwbaarheid van een sample is bij een DNA-onderzoek eenvoudiger te controleren door op verschillende tijdstippen en verschillende locaties celmateriaal veilig te stellen. In tegenstelling tot vingerafdrukken zal altijd hetzelfde DNA-profiel worden teruggevonden en kan dit aan het onderzoekssubject worden gekoppeld. Vanzelfsprekend houden de diensten altijd rekening met de mogelijkheid dat targets in het kader van hun veiligheidsbewustzijn valse sporen achterlaten: of het nu technische gegevens (bijvoorbeeld online activiteiten op een zeker moment), valse vingersporen of DNA-sporen betreft. Dit kan niet door een wettelijke regeling worden ondervangen, maar door gedegen onderzoek.

De leden van de fractie van D66 vragen voorts hoe het vierde en het vijfde lid van artikel 42 van de Wiv zich tot elkaar verhouden. Tevens vragen zij waarom er voor is gekozen dit in twee afzonderlijke leden onder te brengen. De verhouding tussen het vierde en het vijfde lid van artikel 42 van het wetsvoorstel is de volgende: in het vierde lid wordt de toestemming om gebruik te maken van de bevoegdheid tot binnentreden (en doorzoeken) exclusief toegekend aan de minister. Dit is nodig in verband met het grondwettelijk geregelde huisrecht dat specifiek ziet om het binnentreden van een woning zonder de toestemming van de bewoner. Ingevolge het eerste lid van artikel 12 van de Grondwet is een dergelijk binnentreden alleen toegestaan aan hen die daartoe bij of krachtens de wet zijn aangewezen. In verband daarmee wordt in de Wiv een grondslag gegeven voor het binnentreden zonder de toestemming van de bewoner wanneer de minister (bij uitsluiting van anderen) daarvoor (schriftelijk) toestemming heeft gegeven. Anders dan bij het optreden op grond van het strafrecht, waar in het kader van een gerechtelijk vooronderzoek een bevel tot binnentreden en doorzoeking moet zijn afgegeven door de rechter-commissaris of de officier van justitie, is in het kader van de Wiv de toestemming vereist van de minister. Aldus is een waarborg gecreëerd tegen binnentreden door weliswaar bevoegde personen in gevallen waarin een expliciet in het concrete geval gegeven toestemming ontbreekt. Het vijfde lid ziet op de verkrijging van de toestemming die in het vierde lid is omschreven. De bevoegdheid om besloten plaatsen te doorzoeken is, met het oog op het voorgaande, met bijzondere waarborgen omgegeven. Het daartoe strekkende verzoek kan in dat geval slechts worden gedaan door het hoofd van de dienst onder specificatie van het woonadres.

Omdat de toestemming en het verzoek daartoe zien op twee duidelijk verschillende aspecten van de doorzoeking is er voor gekozen om deze aspecten in afzonderlijke leden onder te brengen.

De leden van de D66-fractie hebben meerdere vragen gesteld over het terugplaatsen van aangetroffen en meegenomen voorwerpen. Ik verwijs deze leden graag naar hetgeen ik hiervoor in reactie op vragen van de leden van de SP-fractie heb gesteld.

De leden van de GroenLinks-fractie zijn kritisch op het voornemen van de regering om een aparte DNA-database aan te leggen voor de veiligheidsdiensten De leden van de GroenLinks-fractie vragen de regering waarom het niet mogelijk is om op het gebied van DNA-onderzoek een samenwerking plaats te laten vinden met de politie. Deze leden vragen tevens of het risico van een eigen DNA-database van de diensten niet kan zijn dat dit materiaal wordt onttrokken aan de strafrechtketen, en derhalve niet kan worden gebruikt in strafprocessen. De inlichtingen- en veiligheidsdiensten maken in het kader van de bevoegdheden op het gebied van DNA-onderzoek gebruik van de diensten en expertise van het Nederlands Forensisch Instituut en van gecertificeerde laboratoria. In Nederland is vanuit rechtsstatelijk oogpunt gekozen voor een scheiding tussen inlichtingen- en veiligheidsdiensten enerzijds en opsporing en strafvordering anderzijds. DNA-onderzoek door de AIVD en de MIVD kan dus enkel door middel van een ambtsbericht worden ingebracht in strafprocessen. In artikel 66 van het wetsvoorstel is een regeling uitgewerkt voor het uitbrengen van ambtsberichten aan het openbaar ministerie dat ertoe kan leiden dat tot opsporing en vervolging wordt overgegaan; bovendien kan de informatie in een ambtsbericht ook bijdragen aan het bewijs in een strafzaak.

Voorts vragen de leden van de GroenLinks-fractie de regering om te schetsen in welke situaties de bevoegdheid tot verificatie van een identiteit aan de hand van een aangelegde database een grote meerwaarde zal hebben, en of deze bevoegdheid niet een prikkel vormt voor de diensten om een database van aanzienlijke omvang aan te leggen. Er is gekozen om identificatie en verificatie van het door de diensten uit te (doen) voeren DNA-onderzoek afzonderlijk te benoemen. Daarmee wordt tegemoet gekomen aan hetgeen de CTIVD in haar toezichtsrapport (nr. 42) ter zake heeft gesteld. Daarbij wordt wel de kanttekening gemaakt dat – ondanks de aangebrachte scheiding – beide doeleinden in elkaars verlengde liggen en elkaar zelfs deels overlappen. In strafvordering wordt verificatie dan ook onder identificatie begrepen. Bij *identificatie* gaat het primair om het vaststellen van de nog onbekende identiteit van een target (daaronder begrepen de situatie dat die identiteit nog onvoldoende vast is gesteld). Een door de diensten opgesteld DNA-profiel wordt daartoe vergeleken met DNA-profielen die de diensten in eigen huis hebben of met DNA-profielen die bij derden beschikbaar zijn (zoals bijvoorbeeld in de DNA-databank voor strafzaken of aan de hand van DNA-profielen verkregen van of in beheer bij collegadiensten). Dit kan onder meer voor komen bij het vergelijken van DNA-profielen van terroristen die zich schuil hebben gehouden in safe houses in diverse landen. Bij de aanslagen in Parijs in november 2015 bleek dat diverse DNA-profielen een belangrijke rol speelden bij het identificeren van aanslagplegers en hun verblijfplaatsen. Bij *verificatie* (ook wel: toekomstige identificatie) is bij de dienst bekend welke identiteit bij een door de dienst opgesteld en bewaard DNA-profiel behoort en wordt het DNA-profiel gebruikt om op een later tijdstip te kunnen verifiëren – aan de hand van een beschikbaar gesteld DNA-profiel of aan de hand van een opgesteld DNA-profiel met betrekking tot beschikbaar gekomen celmateriaal - of een

bepaald target degene is van wie men de identiteit vermoedt, van wie door anderen wordt gesteld dat hij/zij een bepaalde identiteit heeft of waarvan de identiteit onbekend is, zoals bijvoorbeeld aan de hand van het afgenomen materiaal van een zelfmoordterrorist of het identificeren van een buitenlandse inlichtingenofficier hier ten lande. Indien een DNA-spoor wordt gevonden op materiaal gerelateerd aan het conflict in Syrië, een beraming tot het plegen van terroristische misdrijven, etc. (wapens, springstoffen, restmateriaal van IED's, basismateriaal voor het vervaardigen van IED's etc.) dan kan dit vergeleken worden met het DNA-profiel van bekende "terugkeerders" (verificatie). Ook kan een vergelijking worden gemaakt met DNA-profielen die in het kader van opsporing en vervolging zijn opgesteld. Bij het identificeren of het verifiëren van de identiteit van een buitenlandse inlichtingenofficier moet worden gedacht aan de situatie waarin inlichtingenofficieren van offensieve buitenlandse diensten met gebruikmaking van een pseudo-identiteit heimelijk activiteiten ontplooien in Nederland. Ook het DNA-onderzoek is met diverse waarborgen omgeven om zo de proportionaliteit, subsidiariteit, noodzaak en het doel van de het onderzoek goed af te wegen. Om te beginnen is er voor het verrichten van DNA-onderzoek ministeriële toestemming en bindend oordeel van de TIB nodig. Hiermee wordt gewaarborgd dat er altijd een goede reden is als er een DNA-onderzoek wordt gestart en een DNA-profiel in de DNA-database opgenomen wordt. Ieder afzonderlijk DNA-onderzoek heeft een 'dubbel slot'. De DNA-profielen die aldus beschikbaar komen, zijn voor een specifiek doel opgesteld (identificatie of verificatie) en mogen uitsluitend voor het onderzoek ten behoeve waarvan toestemming is verleend worden verwerkt. Verdere verwerking van DNA-profielen in het kader van andere onderzoeken van de dienst, bijvoorbeeld ter verstrekking aan een andere instantie, vergt altijd een afzonderlijke en op die verdere verwerking toegespitste toestemming van de voor de desbetreffende dienst verantwoordelijke minister (artikel 43, zesde lid). Verstrekking aan een buitenlandse collegadienst kan bijvoorbeeld aan de orde zijn in het kader van de internationale samenwerking in de strijd tegen het terrorisme, waarbij bijvoorbeeld via vergelijking van DNA-profielen die zijn verworven van omgekomen jihadstrijders, de identiteit kan worden vastgesteld of geverifieerd. Voor zover een DNA-profiel aan een buitenlandse collegadienst wordt verstrekt, dient daarbij op grond van artikel 65, tweede lid, van het wetsvoorstel, altijd de zogeheten derde partij-regel te worden gesteld: te weten dat de gegevens die worden verstrekt aan die dienst, door die dienst niet aan derden mogen worden verstrekt. Ook overigens kunnen aan een verstrekking, indien daartoe aanleiding bestaat, voorwaarden worden gesteld omtrent bijvoorbeeld het gebruik dat ervan gemaakt wordt (zoals niet opnemen in een eigen databank of na een bepaalde periode vernietigen).
Tot slot heeft de CTIVD als onafhankelijke toezichthouder toegang tot alle onderzoeksprocessen van de diensten, inclusief DNA-onderzoek. De CTIVD kan de rechtmatigheid van de te verrichten onderzoeken, gedurende het gehele proces van DNA-onderzoek beoordelen, zoals ook reeds uit het toezichtsrapport nr. 42 is gebleken. Niet alleen kan toezicht worden gehouden op het onderzoek zelf, maar ook op het gebruik van DNA-profielen. Zo kan de CTIVD onder meer toezicht houden op de opslagduur, het gebruik, toegang van derden, procedures voor het behoud van de integriteit en vertrouwelijkheid van de data en de procedures voor de vernietiging.

De leden van de SGP-fractie vragen naar het onderscheid tussen het doorzoeken van besloten plaatsen en het doorzoeken van gesloten voorwerpen. Deze leden vragen of kan worden gesteld dat er, zodra er sprake is van het verbreken of stukmaken er sprake is van het doorzoeken van gesloten voorwerpen? Valt, zo vragen deze leden zich af,

bijvoorbeeld het openen van een kast waar de sleutel in zit onder het doorzoeken van een besloten plaats (artikel 42, eerste lid, onder a) en het openen van een kast die opengebroken dient te worden onder het doorzoeken van gesloten voorwerpen (artikel 42, eerste lid, onder b)? In artikel 42 van het wetsvoorstel wordt de bevoegdheid tot het doorzoeken van besloten plaatsen (artikel 42, eerste lid, onder a) en het doorzoeken van gesloten voorwerpen (artikel 42, eerste lid, onder b) geregeld. Deze bijzondere bevoegdheden zijn in ongewijzigde vorm overgenomen uit de huidige wet op de inlichtingen- en veiligheidsdiensten. De bevoegdheid tot het doorzoeken van besloten plaatsen (eerste lid, onder a) ziet niet alleen op het doorzoeken van woningen, maar bijvoorbeeld ook op het doorzoeken van loodsen en bedrijfsgebouwen. Onder woningen worden onder meer verstaan woonwagens, woonschepen, tenten, caravans, keten en onder omstandigheden ook een hotelkamer.
Onder het begrip doorzoeken wordt in dit verband niet alleen het enkel bezichtigen van de desbetreffende besloten plaats verstaan, maar ook het openmaken van aldaar aanwezige kasten e.d. Bij het doorzoeken van gesloten voorwerpen moet worden gedacht aan het openen en vervolgens feitelijk doorzoeken van bijvoorbeeld koffers, containers, lockers, e.d. Om een kast te kunnen openen die in een huis staat is alleen toestemming nodig voor het doorzoeken van de besloten plaats. De hele plaats kan doorzocht worden; dus ook aldaar aanwezige kasten. Of er een sleutel zit in de kast maakt niet uit voor de inzet van deze bevoegdheid. Van belang is dat een besloten plaats wordt betreden om te doorzoeken. Indien men bij het doorzoeken een "geautomatiseerd werk" aantreft en men zich daartoe toegang wenst te verschaffen, dan is daarbij de in artikel 45 van het wetsvoorstel geregelde bijzondere bevoegdheid tot het binnendringen in een geautomatiseerd werk van toepassing.
Het doorzoeken van een gesloten voorwerp betreft een voorwerp 'an sich', zoals een koffer, container, locker e.d. Het gaat om het doorzoeken van een voorwerp dat zich niet in een besloten plaats bevindt.
Voor de uitoefening van de bevoegdheid is toestemming vereist van de minister of namens deze het hoofd van de desbetreffende dienst; ondermandaat is mogelijk (artikel 42, derde lid). Voor zover het een woning betreft, dient daarvoor door de voor de dienst verantwoordelijke minister schriftelijk toestemming te worden verleend aan het hoofd van de dienst. Het verzoek dient te worden gedaan door het hoofd van de dienst en dient in aanvulling op het bepaalde in artikel 29, tweede lid, het adres van de woning te bevatten die dient te worden doorzocht. De aldus verleende toestemming ziet uitsluitend op de uitoefening van deze bevoegdheid als zodanig. Voor het binnentreden in een woning zonder toestemming van de bewoner is daarnaast ingevolge artikel 2 van de Algemene wet op het binnentreden een machtiging vereist. Ingevolge artikel 58, derde lid, zijn voor het binnentreden in de woning de betrokken minister of namens deze het hoofd van de dienst bevoegd tot het geven van een dergelijke machtiging.

De leden van de SGP-fractie wijzen erop dat er een specifieke bepaling is opgenomen voor DNA-onderzoek en hebben gevraagd hoe de bewaartermijn van vijf jaar zich verhoudt tot de termijn van drie maanden waarbinnen het onderzoek plaats dient te vinden, en of dit betekent dat het bewaarde DNA-materiaal pas na een nieuwe toestemming opnieuw mag worden gebruikt. Onderscheid dient te worden gemaakt tussen het vergaarde celmateriaal enerzijds, en het op basis daarvan vervaardigde DNA-profiel anderzijds. Het DNA-onderzoek dient binnen drie maanden (met de mogelijkheid deze termijn maximaal eenmaal te verlengen) na het vergaren van het celmateriaal te worden uitgevoerd. Het bewuste celmateriaal dient binnen drie maanden na het DNA-onderzoek te worden vernietigd. Het vervaardigde DNA-profiel – dus niet het

celmateriaal – mag vervolgens voor een periode van maximaal vijf jaar (met de mogelijkheid deze termijn te verlengen) worden bewaard. De vervaardigde DNA-profielen zijn voor een specifiek doel opgesteld (identificatie of verificatie) en mogen uitsluitend voor het onderzoek ten behoeve waarvan toestemming is verleend worden verwerkt. Verdere verwerking van DNA-profielen in het kader van andere onderzoeken van de dienst, bijvoorbeeld ter verstrekking aan een andere instantie, vergt altijd een afzonderlijke en op die verdere verwerking toegespitste toestemming van de voor de desbetreffende dienst verantwoordelijke minister.

3.3.3.3.3 Openen van brieven en andere geadresseerde zendingen (§3.3.4.4.5 m.v.t.)

De leden van de D66-fractie hebben meerdere vragen gesteld over de praktische uitwerking van het voorgenomen artikel 44. Uit de wettelijke regeling vloeit zowel een medewerkingsplicht als een geheimhoudingsplicht voort. Gelet op de afscherming van de modus operandi van de diensten, kan ik niet nader ingaan op vragen omtrent de tijd die de diensten nodig hebben voor bijvoorbeeld het verkrijgen, openen, doorzoeken en retourneren van brieven en andere geadresseerde zendingen. Wel kan ik in zijn algemeenheid aangeven dat de diensten hun activiteiten heimelijk uitvoeren, en dus vanzelfsprekend maatregelen treffen opdat de ontvanger niet van een eventuele vertraging op de hoogte geraakt. Hiermee hebben de diensten reeds ervaring, want artikel 44 betreft geen nieuwe bevoegdheid.

De leden van de SGP-fractie vragen om een toelichting op het verschillende toestemmingsregime bij artikel 44 en artikel 45. De keuze voor de rechter ingeval van het openen van brieven vloeit voort uit het bepaalde in artikel 13 Grondwet. Voor het binnendringen van een geautomatiseerd werk geldt een dergelijke eis niet en is voorzien in toestemming van de minister, gevolgd door een rechtmatigheidstoets door de TIB. Daarop bestaat slechts een uitzondering voor zover de bevoegdheid tot het binnendringen in een geautomatiseerd werk wordt uitgeoefend jegens een advocaat of een journalist; in dat geval is eveneens voorzien in toestemming door de rechtbank Den Haag.

3.3.3.3.4 Verkennen van en binnendringen in geautomatiseerde werken (§3.3.4.4.6 m.v.t.)

De leden van de VVD-fractie vragen de regering of zij kan uitsluiten dat met de inzet van technische hulpmiddelen de integriteit van het menselijk lichaam wordt aangetast. Zijn, aldus de aan het woord zijnde leden, de bevoegdheden in het wetsvoorstel beperkt tot het inzetten van technische hulpmiddelen buiten het lichaam. Ik wil hier graag als volgt op reageren. Artikel 45 van het wetsvoorstel regelt de bijzondere bevoegdheid van de diensten tot onder meer het al dan niet met gebruikmaking van een technisch hulpmiddel binnendringen in geautomatiseerde werken. Deze bevoegdheid is uitsluitend gericht op het verzamelen van gegevens. Het begrip geautomatiseerd werk is weliswaar ruim en kan onder omstandigheden ook bepaalde in het lichaam aangebrachte medische apparatuur omvatten. Ik kan mij echter nu en in de nabije toekomst geen enkele situatie voorstellen dat de diensten in het kader van het verzamelen van gegevens deze bevoegdheid zouden willen inzetten op een manier waarbij de lichamelijke integriteit van personen wordt aangetast. Ik sluit dat dus uit.

De leden van de PvdA-fractie hebben meerdere vragen gesteld over de uitleg en reikwijdte van het begrip 'derde' in het voorgestelde artikel 45. Uitgangspunt is dat de diensten altijd ingevolge het vereiste van subsidiariteit kiezen voor het lichtste middel. In het geval van het binnendringen in het geautomatiseerd werk is dat het rechtstreeks binnendringen in het geautomatiseerde werk van het target. In het merendeel van de gevallen hebben de diensten echter geen directe fysieke toegang tot het bewuste geautomatiseerde werk van een target. Dergelijke geautomatiseerde werken kunnen dan enkel op afstand digitaal worden binnengedrongen. Hiervoor is dan uiteraard wel een verbinding van het bewuste werk van het target met de buitenwereld nodig. Voor wat betreft de vraag van de leden van de PvdA-fractie of er tussen het target en de derde nog veel schakels zitten, en zo ja, hoeveel, sluit ik mij aan bij de zienswijze van de CTIVD op het wetsvoorstel dat het precieze aantal technische (tussen)schakels waarbij nog kan worden gesproken van een directe technische relatie afhankelijk is van de omstandigheden van het geval, zulks ter toetsing door de betrokken minister en de toetsingscommissie (TIB). Ik acht het niet wenselijk op voorhand het aantal schakels tussen het geautomatiseerde werk van het target en de diensten limitatief vast te leggen, omdat de operationele praktijk leert dat deze per concrete inzet zal variëren. Ik acht het van groot belang te benadrukken dat het voorgestelde artikel 45, vijfde lid voor het binnendringen van een geautomatiseerd werk van een derde ministeriële toestemming vereist, waarbij in de aanvraag daartoe een afweging wordt gemaakt van noodzakelijkheid, proportionaliteit en subsidiariteit. Inzet van de bevoegdheid vindt bovendien slechts plaats nadat de toetsingscommissie (TIB) heeft geoordeeld dat de toestemming rechtmatig is verleend. Ten slotte houdt de CTIVD toezicht op de rechtmatigheid van de uitoefening van de bevoegdheid. Ik acht deze bevoegdheid hiermee van voldoende waarborgen voorzien.

Ik wil krachtig afstand nemen van de suggestie dat het begrip 'derde' zover mag worden opgerekt dat daarmee in feite bij alles en iedereen gehackt zou kunnen gaan worden. De wet biedt hiertoe geen ruimte.

De leden van de PvdA-fractie hebben een aantal vragen gesteld over het ongedaan maken van versleuteling. De huidige bevoegdheid tot het ongedaan maken van versleuteling door de diensten – niet alleen waar het gaat om het binnendringen in geautomatiseerde werken, maar ook ingeval van interceptie - is neergelegd in de artikelen 24, eerste lid, 25, eerste lid, 26, eerste lid, en 27, eerste lid, van de Wiv 2002. Daarnaast voorziet de huidige wet in de artikelen 24, derde lid, en 25, zevende lid, in een medewerkingsplicht bij de ontsleuteling van gegevens. De bestaande situatie – ook waar het gaat om de bevoegdheid tot het binnendringen van geautomatiseerde werken - wordt in het wetsvoorstel gecontinueerd. Wel wordt ten opzichte van de huidige wet in het wetsvoorstel voorzien in een uitbreiding van de medewerkingsplicht bij ontsleuteling waar het gaat om gegevens die zijn verkregen met toepassing van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie, terwijl een vergelijkbare plicht thans niet bestaat bij de bevoegdheid tot ongerichte interceptie van niet-kabelgebonden telecommunicatie op grond van artikel 27 Wiv 2002. In het wetsvoorstel wordt voorts in alle gevallen waarin een beroep wordt gedaan op de medewerkingsplicht, voorzien in toestemming door de minister, waarna nog een rechtmatigheidstoets door de TIB is voorgeschreven. Deze waarborg ontbreekt in de huidige wet. Voor de goede orde wordt opgemerkt dat uit de medewerkingsplicht geen bevoegdheid van de diensten kan worden afgeleid tot het (doen) inbouwen van achterdeuren in systemen om aldus toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor bijvoorbeeld

aanbieders van communicatiediensten om de encryptie die in hun systemen is toegepast te verzwakken.

De leden van de PvdA-fractie vragen hoeveel van het kabelgebonden verkeer op dit moment naar schatting is versleuteld? En ook vragen deze leden of de regering de verwachting deelt dat dit vanwege de gewenste bescherming van de privacy alleen maar zal toenemen? Zo ja, zijn de diensten daar behalve wat betreft wettelijke grondslagen ook wat betreft kennis en capaciteit op voorbereid? Zo nee, waarom deelt de regering die mening niet? Ik wil hier als volgt op reageren. Omdat de bevoegdheid tot kabelgebonden interceptie thans nog niet voorhanden is, is een schatting van het deel van de communicatie dat versleuteld is problematisch. Ten aanzien van HF (radio) verkeer geldt dat het overgrote deel daarvan is versleuteld. Dit is gezien het overwegend militaire karakter van dit verkeer verklaarbaar. Ten aanzien van SHF (satelliet) verkeer geldt dat van het militaire deel wederom het overgrote deel is versleuteld. Het niet-militaire deel valt grofweg uiteen in IP verkeer (80%) en niet-IP verkeer (20%). Van het IP-verkeer is naar schatting 70% in enige mate versleuteld en van het niet-IP verkeer is dit de helft. De regering deelt de verwachting dat het gebruik van versleuteling enkel zal toenemen. Zoals hierboven aangegeven is het ongedaan maken van versleuteling geen nieuwe bevoegdheid van de diensten en hebben zij hiermee ervaring.

Deze leden vragen voorts of versleutelde data zonder dat die ontsleuteld wordt toch nog van nut kan zijn voor de diensten, bijvoorbeeld om metadata te analyseren? Het antwoord is ja. Metadata zijn van wezenlijk belang voor de diensten, omdat deze onder omstandigheden veel aanwijzingen kunnen verschaffen over targets. Aan de hand van metadata kan in voorkomend geval worden vastgesteld of tussen telefoontoestellen contact is geweest, of e-mailadressen met elkaar verband houden, of IP-adressen met elkaar in contact staan en wanneer dat heeft plaatsgevonden, welke websites vanaf een PC zijn bezocht of waar een communicatiemiddel zich op een bepaald moment bevond. Door analyse van deze gegevens, indien die kunnen worden gecombineerd met gegevens uit andere identificerende bronnen, kan met betrekking tot een persoon een beeld worden verkregen omtrent bijvoorbeeld zijn relatienetwerk en zijn verplaatsingsgedrag.

De leden van de PvdA-fractie vragen of kan worden gegarandeerd dat de diensten zo gericht mogelijk zullen werken, en niet middels decryptie de digitale veiligheid van grote groepen gebruikers zullen ondermijnen. Ik verwijs naar mijn eerdere beantwoording op een soortgelijke vraag naar een zo gericht mogelijke inzet van de bevoegdheden, eveneens van de leden van de PvdA-fractie, onder 1.2.2. Het daar genoemde uitgangspunt geldt ook voor de bevoegdheid om in specifieke gevallen versleuteling ongedaan te maken c.q. te decrypteren. De diensten dienen zo gericht mogelijk te werken en niet door middel van decryptie de digitale veiligheid van grote groepen gebruikers te ondermijnen. In de aanvraag van een toestemming voor de uitoefening van een (bijzondere) bevoegdheid, moet het doel steeds voldoende specifiek zijn. Zowel de TIB als de CTIVD kunnen in het kader van de aan hen opgedragen taak (toets respectievelijk toezicht) daaromtrent een oordeel vormen.

De leden van de SP-fractie hebben meerdere vragen gesteld over de verhouding tussen het wetsvoorstel en technologische ontwikkelingen, zoals lichaamsgebonden technologie, en de gevolgen die dit heeft voor de schending van de privacy. Ik verwijs naar mijn eerdere beantwoording op een soortgelijke vraag van de fractie van D66 onder paragraaf

3.3.3.3 van deze nota. In aanvulling daarop, merk ik op, dat de kern van de taakuitvoering van de diensten bestaat uit het verwerken van gegevens. Daarbij zullen de grondrechtelijke en mensenrechtelijke eisen worden gerespecteerd. In antwoord op de vraag van deze leden of de regering andere ethische bezwaren ziet dan alleen de schending van de privacy kan ik aangeven dat bij de toepassing van de bevoegdheid vanzelfsprekend verschillende ethische vraagstukken op tafel kunnen komen.

Verder lezen de leden van de SP-fractie over het binnendringen van een geautomatiseerd werk van een derde. Daaromtrent stellen zij diverse vragen, die ik in samenhang bezien, graag als volgt beantwoord. Een 'derde' betreft een aan het geautomatiseerde werk van het target technisch gerelateerde partij. Daarbij moet onder andere gedacht worden aan een partij die een netwerk aansluit, een dienst levert, software levert of technische kennis levert. Het binnendringen van een geautomatiseerd werk van een derde vereist op grond van het voorgestelde artikel 45 ministeriële toestemming, waarbij in de aanvraag daartoe een afweging wordt gemaakt van noodzakelijkheid, proportionaliteit en subsidiariteit en waarbij technische risico's nadrukkelijk dienen te worden omschreven. Op grond van dit artikel is bovendien het uitgangspunt dat voor zover technische hulpmiddelen zoals malicieuze software zijn toegepast, deze door de diensten worden verwijderd. Inzet van de bevoegdheid vindt bovendien slechts plaats nadat de toetsingscommissie (TIB) heeft geoordeeld dat de toestemming rechtmatig is verleend. Ten slotte houdt de CTIVD toezicht op de rechtmatigheid van de uitoefening van de bevoegdheid. Ik acht deze bevoegdheid hiermee van voldoende waarborgen voorzien.
Voor de beantwoording van de vraag over de verplichting kwetsbaarheden ('zwakheden') te melden verwijs ik naar de brieven van 8 november 2016 en 16 december 2014 waarmee het parlement werd geïnformeerd over de omgang met kwetsbaarheden op internet door de AIVD en de MIVD.[6] Uitgangspunt hierbij is dat indien de AIVD of de MIVD in het kader van hun wettelijke taakuitvoering stuiten op een kwetsbaarheid die de belangen van gebruikers van het internet kan schaden, de diensten belangendragers, zoals het Nationaal Cyber Security Centrum, zullen informeren. Bovendien informeert de AIVD in het kader van de veiligheidsbevorderende taak belangendragers voortdurend over digitale dreigingen. Met deze informatie zijn die belangendragers dan beter in staat hun beveiliging in te richten. De dienst draagt zo bij aan het bevorderen van maatregelen die de (digitale) veiligheid en weerbaarheid structureel verbeteren. Toeleveranciers van Defensie krijgen van de MIVD advies over digitale dreigingen. Daarnaast worden aan defensieorderbedrijven eisen gesteld ten aanzien van informatiebeveiliging en worden cursussen voor beveiligingsfunctionarissen van deze bedrijven gegeven.

De leden van de D66-fractie stelden vragen over het hacken via een 'derde'. Ik verwijs deze leden naar mijn eerdere beantwoording op soortgelijke vragen van de fractie van de PvdA eerder in deze paragraaf. Uitgangspunt is dat de diensten altijd eerst zullen proberen rechtstreeks binnen te dringen in het geautomatiseerde werk van het target. Er kan dus geen sprake zijn van het binnendringen via het geautomatiseerde werk van een derde uit gemakzucht. Gemakzucht is geen overweging binnen het operationele werk van de diensten. Waar het gaat om het door het lid Verhoeven ingediende amendement (Kamerstukken II 2016/17, 345 88, nr.8), merk ik op dat dit miskent dat de diensten in het merendeel van de gevallen geen directe fysieke toegang tot het geautomatiseerde

[6] Kamerstukken I 2014/15, CVIII, N en Kamerstukken II 2016/17, 26 643, nr. 428.

werk van een target hebben. Dergelijke geautomatiseerde werken kunnen dan enkel op afstand digitaal worden binnengedrongen. Ik sluit mij aan bij de zienswijze van de CTIVD op het wetsvoorstel dat het precieze aantal technische (tussen)schakels waarbij nog kan worden gesproken van een directe technische relatie afhankelijk is van de omstandigheden van het geval, zulks ter toetsing door de betrokken minister en de toetsingscommissie (TIB). Ik acht het niet wenselijk op voorhand het aantal schakels tussen het geautomatiseerde werk van het target en de diensten limitatief vast te leggen, omdat de operationele praktijk leert dat deze per concrete inzet zal variëren.

De leden van de D66-fractie constateren dat het binnendringen in en verkennen van geautomatiseerde werken kan leiden tot het observeren en volgen binnen een woning. Deze leden vragen zich af of in dat geval de waarborgen die in artikel 40, derde en vierde lid, opgenomen zijn van toepassing zijn. Ik antwoord deze leden graag als volgt. In geval op grond van het gestelde in artikel 45, tweede lid, onder c, van het wetsvoorstel bij de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk tevens technische voorzieningen worden aangebracht teneinde de uitoefening van de bevoegdheid tot observatie (artikel 40, eerste lid) of gerichte interceptie (artikel 47, eerste lid) mogelijk te maken, dient voor inzet van de relevante bevoegdheden toestemming te worden verleend. In het geval dat daarbij de microfoon wordt ingeschakeld, is er mede sprake van toepassing van artikel 47 van het wetsvoorstel (gerichte interceptie). De uitoefening van die bevoegdheid is onderworpen aan de notificatieregeling. Indien sprake is van observatie zijn de waarborgen van artikel 40, derde en vierde lid, ook van toepassing. In de geschetste situatie is echter geen sprake van het zonder toestemming van de bewoner binnentreden in een woning. Zoals geschetst omvat de bevoegdheid tot het binnendringen in een geautomatiseerd werk tevens de bevoegdheid tot het aanbrengen van technische voorzieningen voor (onder meer) observatie. Hieronder valt ook de toepassing van observatie- en registratiemiddelen binnen woningen. Voor de bijzondere bevoegdheid van observatie geldt geen notificatieplicht.

De leden van de D66-fractie hebben gevraagd om een toelichting over de uitspraak dat het van belang is “hetzelfde gereedschap te hebben als de digitale aanvaller”. De AIVD en MIVD onderkennen een groot aantal digitale spionage-aanvallen op Nederlandse overheidsinstellingen, bondgenootschappelijke netwerken en producenten van relevante producten. Ik verwijs u hierbij kortheidshalve naar de openbare jaarverslagen over 2015 van beide diensten. In het kader van het onderkennen en attribueren van dergelijke digitale aanvallen is het inderdaad van belang dat de AIVD en MIVD over eenzelfde, en waar mogelijk betere, toolbox als de tegenstander beschikken. De onderwerpen computer network exploitation (CNE, zogenoemd ‘hacken’) en computer network defence (CND, de digitale verdediging) zijn immers nauw aan elkaar gerelateerd. Het door middel van de wettelijke bevoegdheid tot de inzet van 'hacking' (CNE) door de diensten verkrijgen van toegang tot bijvoorbeeld een command and control-server die wordt misbruikt door een buitenlandse statelijke actor om Nederlandse werken aan te vallen of data te exfiltreren is van essentieel belang om vervolgens de Nederlandse verdediging tegen digitale aanvallen in het kader van CND voldoende op orde te kunnen brengen. Aldus stelt het bedoelde 'gereedschap' de diensten in staat specifieke aanvalskenmerken vroegtijdig te kunnen onderkennen, en draagt zodoende in grote mate bij aan een andere kernactiviteit van de AIVD en MIVD, namelijk de verdediging tegen digitale aanvallen (CND).

De leden van de D66-fractie hebben gevraagd hoe de coördinatie verloopt tussen de inlichtingen- en veiligheidsdiensten en de politie met betrekking tot de verschillende hackbevoegdheden. In het voorgestelde artikel 93, tweede lid, is een met het huidige artikel 61, tweede lid, Wiv 2002 vergelijkbare regeling getroffen dat steeds wanneer de vervulling van de taak van het openbaar ministerie en van een dienst daartoe aanleiding geeft, overleg wordt gepleegd. In geval van mogelijke sprake van interferentie van opsporingsonderzoeken naar bijvoorbeeld cybercriminaliteit met (contra-) inlichtingenonderzoeken naar digitale spionage, vindt binnen een reeds daartoe in het leven geroepen platform deconflictie plaats. Ik ben van mening dat hiermee voldoende waarborgen aanwezig zijn om ongewenste interferentie te voorkomen. Overigens regardeert dit wetsvoorstel niet het eventuele gebruik van malware door de politie.

De vragen van de D66-fractie omtrent het door de politie aankopen van onbekende kwetsbaarheden, zijn in het kader van de parlementaire behandeling van het wetsvoorstel Computercriminaliteit III ook aan de orde gekomen. Het kabinet bevordert een vrij, open en veilig internet. Het beperken van kwetsbaarheden in hardware en software is daarvoor van belang. De overheid bevordert het melden van kwetsbaarheden, onder meer met het beleid voor responsible disclosure. Het kabinet heeft tegelijk tot taak om binnen de wettelijke kaders de nationale veiligheid te waarborgen en strafbare feiten op te sporen, in de digitale en in de fysieke wereld. Daarvoor is toegang tot digitale informatie noodzakelijk, waarbij in bepaalde gevallen kan worden gekozen voor het binnendringen in een geautomatiseerd werk. Het gebruik van kwetsbaarheden is daarbij één van de technische mogelijkheden om de bevoegdheid tot binnendringen uit te voeren. Deze bevoegdheid is alleen onder strenge, bij wet bepaalde voorwaarden toegestaan en is met specifieke waarborgen omkleed. De noodzaak, proportionaliteit en de subsidiariteit zijn leidend bij de afweging tot inzet. De waarborgen verzekeren een zorgvuldige afweging van de betrokken belangen.

Voor de beantwoording van de vraag van de D66-fractie over de verplichting kwetsbaarheden (‘zwakheden’) te melden verwijs ik allereerst naar hetgeen ik eerder in antwoord op vragen van leden van de SP-fractie ter zake heb gesteld. Waar het gaat om de vraag van deze leden of de regering bereid is hiervoor een richtlijn op te stellen en de CTIVD hierop toezicht te laten houden, merk ik het volgende op. De richtlijn over de wijze van omgang met kwetsbaarheden is neergelegd in de hierboven reeds genoemde kamerstukken. De CTIVD kan op de rechtmatige uitvoering daarvan door de inlichtingen- en veiligheidsdiensten toezicht houden.

De leden van de GroenLinks-fractie geven aan dat zij de keuze van de regering begrijpen om de wet technologieneutraal te formuleren in het kader van de duurzaamheid van de wet in de toekomst. Wel vragen deze leden of de regering bereid is om in artikel 45 de mogelijkheid te creëren tot nadere regelgeving waarin een heldere definitie kan worden gegeven van wat verstaan dient te worden onder geautomatiseerde werken. Zowel in de Wiv 2002 als in het voorliggende wetsvoorstel wordt met het begrip geautomatiseerd werk aangesloten bij hetgeen daaronder in artikel 80 sexies van het Wetboek van Strafrecht wordt verstaan. Ik zie, mede gelet op de recente parlementaire behandeling van het wetsvoorstel Computercriminaliteit III, geen aanleiding om af te wijken van de bestaande methodiek waarbij in de Wiv wordt aangesloten bij de definitie zoals deze in het Wetboek van Strafrecht wordt gehanteerd.

De leden van de GroenLinks-fractie vragen naar de bevoegdheid om te hacken via een 'derde'. Ik verwijs naar mijn eerdere beantwoording van soortgelijke vragen van de fracties van de SP en D66 eerder in deze paragraaf. De GroenLinks-fractie stelt dat het expliciteren van deze bevoegdheid ertoe leidt dat de uitzondering de regel wordt, en dat daarmee in potentie de privacy van veel Nederlandse burgers waar geenszins een verdenking op rust op ernstige wijze zal worden geschonden. Dit is niet juist. Ik acht het van belang te benadrukken dat die derden in de meeste gevallen geen individuele Nederlandse burgers zullen betreffen. Dit betekent echter niet dat een individuele burger van dit begrip uitgesloten moet worden. In bijzondere gevallen moet het namelijk mogelijk zijn om het geautomatiseerde werk van een target binnen te dringen via een geautomatiseerd werk toebehorende aan een individuele burger. Hiervan kan alleen sprake zijn wanneer alternatieve, minder inbreukmakende manieren van binnendringen niet mogelijk zijn of niet succesvol zijn gebleken. Indien dergelijke gevallen zich in de praktijk voordoen zal hier in het verzoek om toestemming aandacht aan worden besteed, waarbij tevens een afweging wordt gemaakt van noodzakelijkheid, proportionaliteit en subsidiariteit. Inzet van de bevoegdheid vindt slechts plaats na ministeriële toestemming en nadat de toetsingscommissie (TIB) heeft geoordeeld dat de toestemming rechtmatig is verleend. Ten slotte houdt de CTIVD toezicht op de rechtmatigheid van de uitoefening van de bevoegdheid. Ik acht deze bevoegdheid hiermee van voldoende waarborgen voorzien.

De leden van de GroenLinks-fractie geven aan kritisch te zijn op de medewerkingsplicht van personen aan ontsleuteling van gegevens en vragen of hier niet een principiële grens wordt overschreden. De medewerkingsplicht is niet met dit wetsvoorstel in het leven geroepen, maar is reeds neergelegd in de huidige wetgeving, zoals hierboven reeds is aangegeven. Het betreft een verzoek om medewerking te verlenen aan de legitieme uitoefening van een overheidsbevoegdheid.

De leden van de GroenLinks-fractie stelden een aantal vragen over zogenoemde 'zero day'-beveiligingslekken. Ik verwijs deze leden naar de eerdere beantwoording in deze paragraaf van soortgelijke vragen van de leden van de D66-fractie. In aanvulling daarop wijs ik erop dat de hoofdregel is, dat significante kwetsbaarheden die de belangen van gebruikers op internet schaden worden gemeld. Indien er geen wettelijke argumenten inzake de bescherming van actueel kennisniveau, werkwijze of bronnen bestaan om hiervan af te zien, zullen soortgelijke kwetsbaarheden dus worden gemeld. De CTIVD kan vanuit haar wettelijke taak toezicht houden op deze afwegingen.

3.3.3.3.5 Onderzoek van communicatie (§3.3.4.4.7 m.v.t.)

3.3.3.3.5.1 Onderzoeksopdrachtgerichte interceptie van communicatie (§3.3.4.4.7.4 m.v.t.)

De leden van de VVD-fractie stelden een aantal vragen over de bewaartermijnen, onder meer waarom de huidige termijnen door de diensten als knelpunt worden ervaren en waarom langere bewaartermijnen van belang zouden zijn voor Defensie. Ik reageer hier graag als volgt op. Historische data zijn noodzakelijk om tijdig en gericht invulling te geven aan de inlichtingenbehoefte van beide diensten. Het beperken van de mogelijkheden van de beide diensten om historische data te kunnen gebruiken zal de effectiviteit van het inlichtingenproces sterk degraderen. Voor militaire inzet zijn reeds voorafgaand aan de daadwerkelijke inzet inlichtingen nodig. Het opbouwen van een

informatiepositie in het buitenland is een proces van een lange adem. Om zicht te krijgen op de veiligheidssituatie, machthebbers, onderlinge relaties en verbanden en geografische omstandigheden zijn historische gegevens onmisbaar.
Dreigingen worden in kaart gebracht door het reconstrueren van reeds ontvangen data over een relevant netwerk. Als deze gegevens er niet meer zijn, moeten deze data opnieuw worden gegenereerd en dat is dan in veel gevallen onmogelijk of vergt kostbare tijd. Onder verwijzing naar de voorbeelden die in paragraaf 3.3.4.4.7.3 van de toelichting bij het wetsvoorstel zijn opgenomen, en die gelden voor AIVD en MIVD onderzoek, en zijn omkleed met stevige waarborgen, ben ik van mening dat met een bewaartermijn van drie jaar doeltreffend, met een acceptabel restrisico, de uitvoering van de wettelijke taken kan worden gewaarborgd.
De bepaling van de bewaartermijn is overigens geen mathematisch proces welke onvermijdelijk tot een bepaalde (objectieve) bewaartermijn leidt. Het is een afweging tussen enerzijds het belang om waar mogelijk inbreuken op de persoonlijke levenssfeer zoveel als mogelijk te beperken en anderzijds het belang van een goede taakuitvoering van de diensten. Ten aanzien van dat laatste is in de memorie van toelichting (blz. 100) ingegaan op een aantal voorbeelden waaruit het belang van het bewaren van gegevens naar voren komt. Na afweging van beide belangen is uiteindelijk in het wetsvoorstel gekozen voor de in artikel 48 opgenomen bewaartermijn.

Voor wat betreft de vragen van de leden van de VVD-fractie wat er gebeurt met de data die niet relevant zijn en niet voldoen aan het filter, hoe deze verwijderd worden op een wijze dat dit gecontroleerd kan worden, wordt het volgende opgemerkt: op verschillende momenten in het interceptieproces kan worden vastgesteld dat data buiten de onderzoeksopdrachten of andere lopende onderzoeken van de diensten valt. Dit kan reeds in fase 1, bij de ontvangst van telecommunicatie (artikel 48 van het wetsvoorstel), blijken. Ook bij het onderzoek van de diensten in fase 2 en 3 van het interceptiestelsel (artikel 49 en 50 van het wetsvoorstel) kan worden vastgesteld dat geïntercepteerde gegevens niet gerelateerd zijn aan onderzoeksopdrachten. Al deze gegevens worden op dat moment vernietigd.

Het zo snel mogelijk en zo veel mogelijk reduceren van de data in de eerste fasen van de interceptie is een belangrijk onderdeel van het interceptieproces en een vereiste in het wetsvoorstel. Ook uit oogpunt van effectiviteit van de diensten is het pure noodzaak, omdat anders het inlichtingenproces volledig verstopt raakt. De crux is die data te verwerven die van belang zijn voor het onderzoek en de verwerking zo te organiseren dat die data snel worden geanalyseerd en tijdig in een betrouwbaar inlichtingenproduct bij de afnemer komen. Dit betekent dat de diensten filteren. Enerzijds negatief, hetgeen wil zeggen dat gegevens worden verwijderd die op voorhand niet relevant zijn. Evidente voorbeelden zijn Netflix en Youtube. Maar ook de inhoud van veel webbrowser activiteiten, Facebook-verkeer etc. heeft in dit kader geen inlichtingenwaarde. Anderzijds wordt positief gefilterd. Hierin zit het vakmanschap van een inlichtingen- en veiligheidsdienst. Op basis van locatiegegevens, bijvoorbeeld gerelateerd aan dorpen in het Somalisch kustgebied waar vandaan kapingen zijn gelanceerd of het type communicatie, bijvoorbeeld een applicatie gebouwd door jihadisten. Met behulp van samengestelde filters kan op intelligente wijze worden gefilterd, waardoor niet relevante communicatie niet behoeft te worden opgeslagen. Zo kan SMS-verkeer van belang zijn omdat er losgeld-onderhandelingen mee plaatsvinden, maar dan alleen in relatie tot bepaalde regio’s. Dan wordt de communicatie enkel opgeslagen indien afkomstig uit een bepaalde regio en in contact staand met een bekende relevante set aan

telefoonnummers. Metadata zijn van groot belang om netwerken en ongekende dreigingen te achterhalen. De metadata die niet op basis van de negatieve filtering is uitgesloten wordt bewaard. Tenslotte kan bij het onderzoek van de diensten in fase 2 en 3 van het interceptiestelsel (artikel 49 en 50 van het wetsvoorstel) worden vastgesteld dat bepaalde geïntercepteerde gegevens op generlei wijze gerelateerd zijn aan onderzoeksopdrachten of andere lopende onderzoeken. Deze gegevens worden dan vernietigd. Dit is een voortdurend proces en vormt de laatste reductieslag in het interceptieproces.

De bewaartermijn bij onderzoeksopdrachtgerichte interceptie, maximaal 3 jaar, ziet op die gegevens die na de bovengenoemde reductieslagen overblijven. Aangezien middels het hierboven beschreven filterproces een zeer groot percentage van de in fase 1 toegankelijke data niet wordt opgeslagen, is dat een hoeveelheid data die reeds significant is gereduceerd. De data die met inachtneming van het bovenstaande ten behoeve van een onderzoeksopdracht zijn bewaard, worden bij het verstrijken van de maximale bewaartermijn van 3 jaar alsnog vernietigd, tenzij deze is geselecteerd op grond van artikel 50.

De diensten dragen op basis van artikel 18, tweede lid, van het wetsvoorstel zorg voor een behoorlijke en zorgvuldige wijze van verwerking van gegevens. De CTIVD houdt toezicht op de wijze waarop de AIVD en de MIVD het proces van datareductie en de deugdelijke vernietiging van gegevens uitvoeren. Zij heeft hiertoe toegang tot alle systemen, software en data van de diensten.

De leden van de VVD-fractie hebben gevraagd uit te leggen waarom het in het werk van de inlichtingen- en veiligheidsdiensten niet werkt om het uitgangspunt ‘select before you collect’ te hanteren. Zoals ook door dhr. Bart Jacobs gesteld, veronderstelt een dergelijke aanpak ten onrechte dat de diensten van te voren altijd precies weten waar ze naar op zoek zijn. Aangezien een van de kerntaken van de diensten het onderkennen van nog ongekende dreigingen is, is het onverantwoord louter op vooraf bekende kenmerken te filteren. Dat zou immers enkel nadere inlichtingen over gekende dreigingen opleveren. Bij de opslag van de uiteindelijke gegevens (na alle reductieslagen) zal het mechanisme van een rolling buffer gehanteerd worden, waarbij deze gekoppeld is aan de bewaartermijn.

De leden van de PvdA-fractie lezen dat de voorziene bewaartermijn in het geval van onderzoeksopdrachtgerichte interceptie op drie jaar zou moeten worden gezet. Zij geven aan de behoefte van de diensten aan een dergelijke lange bewaartermijn te begrijpen, maar ze wijzen er ook op dat een dergelijk lange bewaartermijn van drie jaar ook een risico voor de privacy oplevert. De leden van de PvdA-fractie naar de mening van de regering over de mogelijkheid om de regel te laten zijn dat de bewaartermijn een jaar is, maar dan met de mogelijkheid om bij uitzondering, na toetsing van de rechter, een langere bewaartermijn mogelijk te maken. Ik verwijs naar mijn eerdere beantwoording van vragen van de VVD-fractie in deze paragraaf, waarin ik heb aangegeven waarom de bewaartermijn van drie jaar voor gegevens verkregen uit onderzoeksopdrachtgerichte interceptie aangewezen is. Ik zie dan ook geen aanleiding om het voorstel van de leden van de PvdA-fractie tot een verkorting van de bewaartermijn of een aparte uitzonderingsregel over te nemen. Overigens zou los daarvan een voorafgaande onafhankelijke toets door een rechter niet passen in het gekozen systeem, waarbij niet

alleen is voorzien in een (eventuele) toets van de toepassing van bijzondere bevoegdheden, maar deze bovendien is belegd bij de TIB.

De leden van de PvdA-fractie hebben gevraagd de regering wil ingaan op de vraag of echt sprake is van 'select while you collect' of dat al bewust ruime data worden verzameld met het oog op latere toepassing. Onderzoeksopdrachtgerichte interceptie wordt zo gericht mogelijk ingezet. De wet staat niet toe dat bewust ruimer data wordt verzameld met het oog op latere toepassing. 'Select while you collect' sluit evenwel niet uit dat sprake is van de verwerving van gegevens die ook voor latere doeleinden geschikt kunnen zijn. Er moet dan wel sprake zijn van lopende onderzoeken.

De leden van de SP-fractie vragen of de regering nader kan ingaan op opmerkingen van zowel de CTIVD als de Raad van State dat de scheiding tussen verwerving, verwerking en nabewerking van gegevens niet altijd even duidelijk zal zijn. Ik ben van mening dat in het wetsvoorstel de verschillende fases helder worden onderscheiden. Met het hierboven in de beantwoording van de vragen van de VVD-fractie geschetste proces van datareductie wordt recht gedaan aan het principe van 'select while you collect'.

De leden van de SP-fractie vragen hoe het principe van 'select while you collect' zich verhoudt tot de bewaartermijn van drie jaar, en vragen waarom niet gekozen is voor een onderscheid tussen metadata en inhoudelijke gegevens. 'Select while you collect' en de bewaartermijn van drie jaar sluiten elkaar geenszins uit. Immers 'select while you collect' vindt een uitdrukking in het proces van datareductie. De termijn van drie jaar geldt voor de data die overblijven na deze reductie. De regering heeft reeds in de reactie op het rapport van de Commissie Dessens aangegeven dat een onderscheid tussen metadata en inhoudelijke gegevens niet langer de bepalende factor is om de zwaarte van de inbreuk op de privacy vast te stellen (Zie Kamerstukken II 2013/14, 33 8220, nr. 2, blz. 2 e.v.). De huidige technologische ontwikkelingen hebben ertoe geleid dat ook enkel aan de hand van metadata een indringend beeld kan worden verkregen over het privéleven van personen.

De leden van de SP-fractie stelden een aantal vragen over de medewerkingsplicht bij het onsleutelen van encryptie. Zoals ik heb aangegeven bij de beantwoording van eerdere vragen van leden van de PvdA-fractie onder 3.3.3.3.4, bestaat de medewerkingsplicht reeds en is deze niet nieuw in het wetsvoorstel. In mijn eerdere antwoord heb ik eveneens aangegeven dat het een verzoek tot medewerking aan de uitoefening van een legitieme overheidsbevoegdheid betreft. Deze bevoegdheid kan pas worden uitgeoefend door de diensten na ministeriële toestemming en een bindend oordeel van de TIB. Aldus is de uitoefening van deze bevoegdheid aan een 'dubbel slot' onderworpen. Bovendien houdt de CTIVD toezicht op deze praktijk. Er vindt zorgvuldig overleg plaats met de betrokken bedrijven. De diensten hebben een verplichting tot geheimhouding, die ook geldt voor eventuele bedrijfsgevoelige informatie die in dit kader zou moeten worden gewisseld. Van belang is dat de verplichting alleen kan worden ingeroepen jegens een persoon of bedrijf waarvan vermoed wordt dat deze de benodigde kennis om de gegevens te ontsleutelen bezit; in de aanvraag om toestemming zal de dienst dit dan ook dienen te onderbouwen. Voorts strekt de verplichting voor betrokkenen niet verder dan waartoe de kennis reikt. Als een bedrijf de kennis niet heeft, zullen de diensten zich niet (langer) tot die partij richten.

De leden van de SP-fractie vragen of er ook een medewerkingsplicht is wanneer gegevens zich in Nederland bevinden, maar het bedrijf niet in Nederland gevestigd is. Is dat ook het geval wanneer een dienst in Nederland wordt aangeboden, maar het bedrijf niet in Nederland is gevestigd? Zij vragen of nader uiteengezet kan worden wanneer bedrijven moeten meewerken aan de informatieplicht. In algemene zin geldt dat er een aanknopingspunt voor Nederlandse rechtsmacht moet zijn. Ingeval gegevens zich in Nederland bevinden, zijn deze onderworpen aan Nederlandse rechtsmacht. Indien een in Nederland woonachtige burger gebruik maakt van de mogelijkheid tot opslag van zijn gegevens in de cloud wil dat echter nog niet zeggen dat die gegevens op servers die zich in Nederland bevinden, zijn opgeslagen. Als diezelfde burger gebruik maakt van een in Nederland gevestigde aanbieder van communicatiediensten, zal die aanbieder echter in beginsel wel aan een opdracht tot gegevensverstrekking moeten voldoen, zeker indien die aanbieder in het kader van de dienstverlening aan in Nederland gevestigde gebruikers van zijn dienst toegang tot die gegevens heeft. Indien het gaat om de situatie dat een dienst in Nederland wordt aangeboden en er is geen vestiging van het bedrijf in Nederland, dan kan weliswaar een verzoek aan het bedrijf worden uitgebracht om bepaalde gegevens aan de dienst te verstrekken, maar een medewerkingsplicht zal niet in rechte afdwingbaar zijn; men bevindt zich dan immers buiten de Nederlandse rechtsmacht.

De leden van de CDA-fractie vragen de regering nader uiteen te zetten wat precies moet worden verstaan onder ‘onderzoeksopdrachtgericht’. De Geïntegreerde Aanwijzing voor de Inlichtingen- en Veiligheidsdiensten die door het kabinet wordt opgesteld valt uiteen in een aantal themagebieden. Deze thematische behoeften, die uiteraard altijd binnen de wettelijke taakstelling van de AIVD en de MIVD moeten passen, worden door de diensten vertaald in onderzoeksopdrachten. In een onderzoeksopdracht wordt een concrete onderzoeksvraag geformuleerd die richting geeft aan het onderzoek. Voorbeelden van onderzoeksopdrachten kunnen zijn het bieden van inzicht in aanslagplanning in Europa vanuit het ISIS-leiderschap in Syrië, het onderkennen van digitale aanvallen vanuit Rusland en het bieden van inzicht in de activiteiten van militante groeperingen in Mali.

De leden van de CDA-fractie vragen naar het standpunt van de regering omtrent verantwoorde databeperking. Ik steun de opmerking van de CTIVD dat gegevens altijd zo gericht mogelijk moeten worden verworven en gereduceerd tot die gegevens die de AIVD en MIVD daadwerkelijk nodig hebben om hun taken goed uit te voeren. Verantwoorde databeperking is een principe dat reeds in het wetsvoorstel is verankerd in de meer algemene vereisten inzake een verwerking van gegevens. Iedereen is gebaat bij een verantwoorde databeperking. De oproep van de CTIVD om hier geen misverstand over te laten bestaan, onderschrijf ik volledig. Ik ben het voorts met de CTIVD eens dat het uitgangspunt moet zijn dat de diensten in het interceptieproces waar mogelijk doorlopend gegevens die niet relevant zijn vernietigen. Daarom is in artikel 48, vijfde lid, de verplichting opgenomen om gegevens waarvan in het kader van search (artikel 49) of selectie (artikel 50) is vastgesteld dat deze niet relevant zijn, te vernietigen. Daarmee wordt aan de zorg van de CTIVD tegemoet gekomen. Ik zie dan ook geen meerwaarde in een aanpassing van artikel 48, vijfde lid, van het wetsvoorstel (behoudens de eerder in deze nota aangekondigde aanpassing dat de vernietiging terstond moet plaatsvinden). In het huidige voorstel kan effectief toezicht worden gehouden op het interceptieproces: de CTIVD kan immers vanuit haar rechtmatigheidstaak overal bij. Ik zie geen aanleiding om de wet op dit punt te voorzien van een aanvulling. Die zou de vraag oproepen of de CTIVD toezicht kan uitoefenen op delen van de wet waarbij dit niet expliciet is gemaakt.

Daarover moet juist duidelijkheid zijn: geen enkel deel van de wet is uitgezonderd van rechtmatigheidstoezicht door de CTIVD.

De leden van de CDA-fractie vragen de regering, onder verwijzing naar het pleidooi van de WRR, in te gaan op de mogelijkheden voor het opnemen van een zorgplicht in het voorliggende wetsvoorstel. Ik heb eerder in antwoord op vragen van de leden van de PvdA-fractie naar het opnemen van een zorgplicht in paragraaf 1.2.2 van deze nota aangegeven dat bij nota van wijziging zal worden voorzien in een aanvulling van de bestaande zorgplicht in artikel 24, tweede lid, onder a, van het wetsvoorstel. Ik verwijs deze leden naar hetgeen ik daar heb gesteld.

De leden van de CDA-fractie vragen of de regering voornemens is extra middelen te investeren voor crypto- en signaalonderzoek en ontcijfertechnieken. Crypto- en signaalonderzoek en ontcijfertechnieken maken, zoals is geantwoord op vragen van verschillende leden, op dit moment al onderdeel uit van de taakuitvoering van de diensten. Dit wordt reeds bekostigd uit het taakbudget van de diensten. Dit zal met de nieuwe wet niet wijzigen.

De leden van de D66-fractie hebben een aantal vragen gesteld over onderzoeksopdrachtgerichte interceptie. Voor de vragen over het nut van onderzoeksopdrachtgerichte interceptie terwijl sprake is van steeds meer versleutelde data verwijs ik naar mijn eerdere antwoord op soortgelijke vragen van de D66-fractie onder 1.3.1 en van de leden van de PvdA-fractie onder 3.3.3.3.4. Daarnaast gaat de onderhavige vraagstelling uit van de notie dat de identificerende gegevens van de verzender of ontvanger altijd bij de diensten bekend zullen zijn. Dit is onjuist. Voor de vragen over het gesuggereerde sleepnet verwijs ik naar mijn antwoord op soortgelijke vragen van de VVD-fractie onder paragraaf 12.1.1.
In mijn reactie richting het parlement op het genoemde rapport van de CTIVD heb ik aangegeven dat de opbrengst van de inzet van de selectiebevoegdheid is onder te verdelen in twee categorieën; de opbrengst in de vorm van inhoudelijke communicatie (bijvoorbeeld een telefoongesprek, sms-bericht of e-mail) en de opbrengst in de vorm van metadata. Met betrekking tot de hoeveelheid inhoudelijke opbrengst, stelt de Commissie vast dat die in 2014 (zeer) gering was. Dit roept volgens de Commissie vragen op over de effectiviteit en daarmee de proportionaliteit van deze inzet. De toegevoegde waarde van de inzet van sigint is echter met name gelegen in de metadata die hiermee worden verkregen. Het verzamelen van metadata is van groot belang voor het onderzoek van de dienst, bijvoorbeeld bij het in kaart brengen van een netwerk van een target. De opbrengst van de inzet van de selectiebevoegdheid van sigint is naar mijn mening dan ook effectief.[7]
De drie fases van onderzoeksopdrachtgerichte interceptie zijn in de wet duidelijk omschreven juist om ze juridisch goed van elkaar te kunnen scheiden. In de praktijk zal sprake zijn van een nauwere verwevenheid. Zo zal in de praktijk veelal sprake zijn van een combinatie van een verzoek om toestemming tot interceptie op grond van artikel 48 en een verzoek voor onderzoek als bedoeld in artikel 49, eerste lid, aanhef en onder a, in verband met het feit dat de ene bevoegdheid ondersteunend is aan de uitvoering van de ander. Omdat niet geïntercepteerd wordt om te intercepteren, zal een last voor interceptie (artikel 48) gevolgd worden door verzoeken om toestemming voor inzet van de bevoegdheden in de andere fasen (artikelen 49 en 50). Interceptie vindt immers juist

[7] Kamerstukken II 2015/16, 29 924, nr. 138.

plaats met het oog op de uitoefening van de bevoegdheden tot search en selectie. Dat laat onverlet dat de voor de uitoefening van deze bevoegdheden vereiste toestemming op de voorgeschreven wijze dient te worden verkregen; elk verzoek om toestemming dient aan de daaraan gestelde eisen te voldoen. Een combilast maakt aldus inzichtelijk hoe de bevoegdheden zich tot elkaar verhouden en draagt bij aan een transparante motivatie.
Voor wat betreft het vernietigen van gegevens wordt opgemerkt dat in de wet is gewaarborgd dat niet-relevante gegevens terstond worden vernietigd. Eerder is onderkend dat in een beperkt aantal gevallen ten onrechte niet is opgenomen dat de vernietiging terstond moet plaatsvinden; in de nota van wijziging wordt deze onvolkomenheid gecorrigeerd. Vernietiging van gegevens wil zeggen dat zij in tegenstelling tot verwijderde gegevens nimmer meer kunnen worden gebruikt voor enig onderzoek van de dienst. De gegevens worden definitief en onomkeerbaar uit de systemen en de gegevensdragers waarop ze zijn vastgelegd gewist.

De leden van de D66-fractie stellen vragen naar aanleiding van enkele commentaren over opdrachtgerichte interceptie. Ik acht de opvatting dat de diensten niet geïnteresseerd zijn in de gehele kabel, maar slechts door middel van het intercepteren op specifieke fibers van een specifieke kabel met vervolgens negatieve filtering informatie uit de kabel willen verwerven het meest juist. Het is niet aan de regering om aan te geven hoe de indruk heeft kunnen ontstaan dat de diensten een kopie van de gehele glasvezelkabel krijgen. Een dergelijke toepassing van de bevoegdheid zou nooit proportioneel zijn.

De leden van de D66-fractie vragen naar de omvang van de datareductie in het proces van ‘select while you collect’. Van een tap op de gehele kabel is zoals ik hiervoor al aangaf geen sprake. Interceptie is gericht op een specifieke datastroom die over enkele fibers van een kabel loopt. Van deze datastroom wordt op basis van uiterlijke kenmerken een groot deel van de data afgebogen, zodat deze niet bij de diensten terechtkomt. Na deze reductie wordt data opgeslagen: de resterende inhoud enkel indien deze voldoet aan bepaalde filters (selectie) en de resterende metadata. Selectie kan pas worden ingezet nadat de minister en de TIB toestemming hebben gegeven. Ter illustratie kan het volgende voorbeeld uit de memorie van toelichting dienen: een kabel bevat 24 fibers met in totaal 480 kanalen. Van die 480 kanalen zijn er 3 kanalen relevant voor één of meerdere onderzoeksopdrachten en deze zijn verdeeld over 2 fibers. Enkel van deze 3 relevante kanalen (van de 480 op die specifieke kabel) wordt de data geïntercepteerd. Van de daadwerkelijk geïntercepteerde data wordt naar verwachting bij een eerste filtering 95% tot 98% direct weer verwijderd en vernietigd. Hierna volgt verdere volumereductie in fase 2 en 3. Het deel van de data die over de kabel gaat dat uiteindelijk wordt binnengehaald, is vele malen minder dan een promille.

De leden van de D66-fractie hebben verder gevraagd hoe de gedachte van dataminimalisatie zich verhoudt tot het in het kader van artikel 48 real-time monitoren van het internetverkeer op ongebruikelijke activiteiten om een cyberaanval of malware op te merken, en of alleen de anomalieën waarnaar men op zoek is daadwerkelijk bij de dienst binnengehaald worden. Op grond van het voorgestelde artikel 49, eerste lid, aanhef en onder a, zijn de diensten bevoegd de aard en kenmerken van de op grond van artikel 48 verworven gegevens vast te stellen. Deze bevoegdheid is van essentieel belang voor het uitvoeren van de taken van de diensten op het gebied van computer network defence (CND), bijvoorbeeld door de op grond van artikel 48 verworven

gegevens te onderzoeken op malicieuze spionagesoftware of specifieke anomalieën. Datareductie is hierbij uitgangspunt: inhoud zal pas worden geïntercepteerd en opgeslagen eerder onderzoek hiertoe aanleiding geeft en nadat hiervoor toestemming is verkregen. Er kan niet worden gegarandeerd dat enkel de gegevens waarnaar de diensten op zoek zijn worden binnengehaald. In dat geval zou immers sprake zijn van gerichte interceptie.

De leden van de D66-fractie vragen naar de samenwerking met buitenlandse collegadiensten, naar aanleiding van de paragraaf over het belang van onderzoeksopdrachtgerichte interceptie. Het waarborgen van de veiligheid in binnen- en buitenland kan enkel plaatsvinden door intensieve internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Het verder teruglopen van de informatiepositie van de Nederlandse diensten zal gevolgen hebben voor de samenwerking met buitenlandse diensten. De voorgestelde modernisering van de bevoegdheden zorgt voor behoud van de hoogwaardige inlichtingenpositie van de Nederlandse diensten. Deze maakt het enerzijds mogelijk om eigenstandig gegevens te blijven verwerven, verwerken en analyseren opdat eigen oordeelsvorming plaatsvindt en is anderzijds essentieel voor de internationale samenwerking.

De leden van de D66-fractie vragen verder of er vanuit het buitenland druk is uitgeoefend op de regering en/of de diensten om de bijzondere bevoegdheden van de diensten uit te breiden naar communicatie over de kabel. Ik kan u bevestigen dat er geen sprake is (geweest) van druk uit het buitenland om bijzondere bevoegdheden van de diensten op enigerlei wijze vorm te geven.

De leden van de D66-fractie stellen dat niet sluitend wordt gemotiveerd waarom een verlengde bewaartermijn van drie jaar nodig is, en vragen waarom de regering niet heeft gekozen voor een meer gedifferentieerd model van bewaartermijnen. Kenmerkend voor het inlichtingen- en veiligheidsdomein is dat vaak lange tijd onduidelijk is welke exacte betekenis gegevens hebben. Zo werd na de aanslagen in Parijs en Brussel duidelijk dat ISIS al jaren bezig was geweest aanslagplegers naar Europa te sturen. Direct na de aanslagen hebben Europese inlichtingen- en veiligheidsdiensten de gegevens die zij in deze jaren hebben vergaard (nogmaals) uitgekamd op zoek naar verbanden tussen de aanslagplegers en nog onbekende derden. Gegevens die tot dan toe zonder betekenis waren, kregen die in het licht van de aanslagen en hetgeen daaromtrent bekend werd plotseling wel. Enkel omdat deze gegevens konden worden bewaard, konden nieuwe cellen van ISIS in Europa worden ontdekt en aanslagplots worden verijdeld. Naast de bestrijding van terrorisme nopen ook andere (inter)nationale veiligheidsbelangen tot een bewaartermijn van 3 jaar. Een goede inlichtingenondersteuning van de uitvoering van militaire operaties, opdat deze zo effectief en veilig mogelijk plaatsvinden, vergt het langdurig kunnen analyseren van hieraan gerelateerde telecommunicatie. Dit geldt evenzeer voor inlichtingenonderzoek naar de brandhaarden in de wereld waar de krijgsmacht actief is of zou kunnen worden, de actoren achter destabilisering aan de grenzen van Europa en dreigingen als nucleaire proliferatie en de cyberactiviteiten van statelijke actoren. Gelet op het belang van de bewaartermijn voor zowel de civiele en militaire taakvelden acht ik een gedifferentieerd model niet aangewezen.

Daarnaast zijn de leden van de D66-fractie benieuwd of artikel 48, vijfde en zesde lid, zo gelezen mag worden dat de bewaartermijn voor versleutelde gegevens zes jaar bedraagt, indien deze gegevens net voordat ze vernietigd zouden moeten worden,

worden ontsleuteld. Wat gebeurt er verder als de analyse op één van de laatste dagen van de bewaartermijn van de verkregen gegevens plaatsvindt? Betekent dit dat het product van die analyse niet meer onderbouwd kan worden, of mogen die gegevens bewaard blijven binnen dat analyseproduct?

De leden van de D66-fractie vragen naar de bewaartermijn van versleutelde gegevens. Wanneer gegevens worden ontsleuteld geldt voor de ontsleutelde gegevens de in artikel 48, vijfde lid, vastgelegde termijn van ten hoogste drie jaar te rekenen vanaf het moment van ontsleuteling. Indien de analyse uitwijst dat deze gegevens als relevant moeten worden aangemerkt, worden deze voor het desbetreffende onderzoek gebruikt. Niet relevante gegevens moeten terstond worden vernietigd.

De leden van de D66-fractie stelden vragen over de balans tussen snel wisselende omstandigheden en communicatiewijzen en de termijn waarvoor een interceptielast wordt afgegeven. Waarom is gekozen voor een jaar, en wat is het grote verschil tussen metadata-analyse en selectie van gegevens? De toestemming voor verwerving in het kader van onderzoeksopdrachtgerichte interceptie kent een maximale toestemmingstermijn van 1 jaar. Het betreft het ontvangen van communicatie (artikel 48) en de verkenning van telecommunicatie gericht op de interceptie (artikel 49, eerste lid). Deze vorm van search is primair gericht op de optimalisatie van de interceptie. Wordt datgene geïntercepteerd wat wordt beoogd? Vanwege deze koppeling zijn de (maximum)termijnen hier gelijkgetrokken. De vervolgstappen van het interceptieproces, te weten search gericht op selectie (artikel 49, tweede lid) en selectie (artikel 50) kennen een maximale toestemmingstermijn van drie maanden. Van fase tot fase wordt in indringender mate inzicht verkregen in de persoonlijke levenssfeer. De waarborgen die in het wetsvoorstel zijn opgenomen, worden zwaarder naarmate de persoonlijke levenssfeer van individuen indringender in beeld komt. Bij selectie wordt immers kennisgenomen van de inhoud van de geselecteerde communicatie. In de verwervingsfase van onderzoeksopdrachtgerichte interceptie worden personen of organisaties niet onderzocht. Hierdoor is de inbreuk op de persoonlijke levenssfeer beperkter. Metadata-analyse in artikel 50, eerste lid, onder b, beoogt subjecten te identificeren en zicht te krijgen op personen en organisaties zonder de inhoud te analyseren. Hiervoor is een maximale toestemmingstermijn van 1 jaar passend. Bij de selectie van geïntercepteerde gegevens ten behoeve van de analyse van de inhoud van telecommunicatie (artikel 50, eerste lid, onder a) vindt een verdergaande inbreuk op de persoonlijke levenssfeer plaats, waarvoor een kortere termijn is aangewezen. Ook voor gerichte interceptie (artikel 47) waar kennis wordt genomen van de inhoud van de communicatie geldt een toestemmingstermijn van maximaal drie maanden.

De leden van de D66-fractie lazen in het artikel ‘Select while you collect’ van de heer Jacobs dat in recente Amerikaanse wetgeving bulkverzameling is beperkt tot bepaalde thematische doelen. Volgens de heer Jacobs ontbreken dergelijke themagerichte bepalingen in de Nederlandse wet. Deze leden zouden daar graag een reactie op krijgen, mede in relatie tot de onderzoeksthema’s en onderzoeksdoelstellingen in de Geïntegreerde Aanwijzing. Ik zou hier als volgt op willen reageren. De Geïntegreerde Aanwijzing valt uiteen in een aantal themagebieden. Deze thematische behoeften, die uiteraard altijd binnen de wettelijke taakstelling van de AIVD en de MIVD moeten passen, worden door de diensten vertaald in onderzoeksopdrachten. Voor de uitvoering van een onderzoeksopdracht kan de inzet van onderzoeksopdrachtgerichte interceptie worden overwogen. Hiermee wordt geborgd dat onderzoeksopdrachtgerichte interceptie

slechts over een beperkt aantal thema's kan worden ingezet. Daarbij geldt tevens dat de inzet van onderzoeksopdrachtgerichte interceptie altijd moet voldoen aan de vereisten van proportionaliteit en subsidiariteit. Het belang van de onderzoeksopdracht moet de inzet van een dusdanig zware bevoegdheid als interceptie kunnen dragen. Ook dit beperkt het aantal thema's waarop de bevoegdheid kan worden ingezet. De Geïntegreerde Aanwijzing wordt uiteraard besproken met de Commissie IVD. In de openbare versies van de jaarplannen alsmede in de jaarverslagen wordt ernaar gestreefd een zo goed mogelijk beeld te geven van de thema's die ingevolge de Geïntegreerde Aanwijzing worden onderzocht, zonder dat daarmee het actueel kennisniveau, de werkwijze en de bronnen van de diensten geschaad kunnen worden. Verdergaande berichtgeving in het openbaar zou deze wettelijk te beschermen belangen schaden.

De leden van de D66-fractie vragen zich af welke verhouding tussen geautomatiseerde (meta)data-analyse en human intelligence de regering voorstaat. Voor een goed begrip van mijn antwoord is het van belang om de begrippen 'human intelligence' en 'menselijke tussenkomst' te scheiden. Human intelligence is het vergaren van gegevens door menselijke bronnen. Menselijke bronnen vormen een onderdeel van het totale palet aan inlichtingenmiddelen. Het levert soms hoogwaardige, unieke inlichtingen op maar tevens informatie-van-horen-zeggen, vage geruchten alsmede roddel en achterklap. In dat opzicht zijn technische inlichtingen verkregen uit onderzoeksopdrachtgerichte interceptie veelal exacter en eenduidiger. De meerwaarde van een goede inlichtingen- en veiligheidsdienst steekt juist in de combinatie van inlichtingenmiddelen, waardoor verkregen informatie uit de ene bron kan worden gecontroleerd met informatie uit een andere.
Zoals de leden van de D66-fractie aangeven, wordt het belang van menselijke tussenkomst bij geautomatiseerde processen onderkend in de wet. Er kan geen sprake van zijn dat enkel op basis van een geautomatiseerd proces conclusies worden getrokken ten aanzien van een persoon of inlichtingen worden verstrekt aan derden. De menselijke tussenkomst blijft een onlosmakelijk element van het inlichtingen- en veiligheidswerk, juist bij het verwerken van grote hoeveelheden gegevens. Ik kan de aangehaalde woorden van Bill Binney niet in verband brengen met de door de wet beoogde Nederlandse praktijk.
Tot slot wil ik benadrukken dat de diensten continu moeten afwegen welke informatie verder te onderzoeken en welke te laten. Dat is en blijft mensenwerk. Er valt nooit uit te sluiten dat achteraf blijkt dat er wel degelijk informatie was over een persoon die een aanslag voorbereidde. Achteraf en op basis van gerichte gegevens terugredeneren is nu eenmaal iets fundamenteel anders dan trachten te voorspellen waar de dreiging zich zal manifesteren en daarop mensen en middelen inzetten.

De leden van de D66-fractie stelden vragen over de gevolgen van de bevoegdheid van de minister op grond van artikel 48, vierde lid, om ambtenaren aan te wijzen die bij uitsluiting kennis kunnen nemen van de op grond van dat artikel verworven data voor de gerichtheid van de onderzoeksopdrachtgerichte interceptie. Met behulp van functiescheiding wordt in de eerste plaats bewerkstelligd dat van de in de eerste fase geïntercepteerde data slechts in kleine kring kennis wordt genomen, namelijk door de technisch specialisten. Deze kennisneming staat primair in het teken van de optimalisatie van het interceptieproces, zoals nader verwoord in artikel 48, eerste lid. Het opstellen van selectiecriteria wordt uitgevoerd door een andere groep, die kennis draagt over waar de diensten naar zoeken in de verworven data. Ik zie dus niet het

geschetste verband tussen functiescheiding en het risico dat meer communicatie wordt verworven dan strikt noodzakelijk.

De leden van de D66-fractie vragen verder wat er onder 'access-locaties' wordt verstaan. Onder een 'access-locatie' wordt verstaan het fysieke ontvangstpunt voor onderzoeksopdrachtgerichte interceptie bij een aanbieder van een communicatiedienst. Alhier vindt het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats.

De leden van de D66-fractie vragen of de medewerkingsverplichting ook geldt voor buitenlandse aanbieders van communicatie. Ik verwijs naar mijn antwoord op de vraag over de rechtsmacht van de leden van de SP-fractie in deze paragraaf.

De leden van de D66-fractie vragen of gebruik van bepaalde vormen van versleuteling een reden kan vormen om geselecteerd te worden, zoals bijvoorbeeld PGP. Een technisch kenmerk zoals de aanwezigheid van een specifieke vorm van versleuteling kan een selectiecriterium vormen om toe te passen op een voor een geautoriseerde onderzoeksopdracht verkregen gegevens. Te denken valt aan een dergelijke communicatietoepassing ontwikkeld en gebruikt door terroristen. Een universeel voorbeeld als het gebruik van PGP is geen grond voor selectie als bedoeld in artikel 50 van het wetsvoorstel.

De leden van de D66-fractie vragen hoe en door wie de controle plaatsvindt of de gebruikte analyse- en verwerkingssoftware wel veilig genoeg is en of de gebruikte algoritmes naar behoren functioneren. Zoals ik eerder heb aangegeven wordt de in artikel 24, tweede lid, onder a, van het wetsvoorstel neergelegde zorgplicht zodanig aangepast, dat de hoofden van de diensten (tevens) zorg dienen te dragen voor de nodige voorzieningen ter bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen. De CTIVD heeft toegang tot alle systemen, software en data van de diensten en houdt binnen haar wettelijke taak toezicht op het rechtmatig functioneren ervan.

De leden van de ChristenUnie-fractie constateren dat meer ongerichte interceptie (onderzoeksopdrachtgerichte interceptie) van telecommunicatie mogelijk wordt met dit wetsvoorstel. Zij vragen of de regering nader kan onderbouwen waarom de huidige bevoegdheid tot gerichte interceptie onvoldoende is. De constatering van de leden van de ChristenUnie-fractie is juist. Voor een nadere toelichting van het belang van onderzoeksopdrachtgerichte interceptie, verwijs ik naar de eerdere antwoorden op de vragen van de leden van de VVD-fractie.

De leden van de ChristenUnie-fractie vragen of de regering de noodzaak van de lengte van de bewaartermijnen bij onderzoeksopdrachtgerichte interceptie nader kan onderbouwen. Voor het antwoord op de vraag met betrekking tot de bewaartermijn verwijs ik de hier aan het woord zijnde leden naar mijn eerdere antwoord in deze paragraaf op een soortgelijke vraag van de leden van de VVD-fractie. Zoals daar ook is aangegeven, heeft de bewaartermijn betrekking op de data die reeds onderworpen is geweest aan reductie. Het kan dan overigens nog steeds gaan om een grote hoeveelheid gegevens.

De leden van de ChristenUnie-fractie verwijzen naar de conclusie van de Raad van State en de CTIVD dat de drie fases van onderzoeksopdrachtgerichte interceptie nauw zijn verweven, en vragen of de regering nader kan aangeven wat in dit kader de betekenis is van de opmerking dat de gegevens die worden bewaard reeds significant gereduceerd zouden zijn. De drie fases van onderzoeksopdrachtgerichte interceptie zijn in het wetsvoorstel duidelijk omschreven om ze juist juridisch goed van elkaar te kunnen onderscheiden. In de praktijk zal echter sprake zijn van een nauwere verwevenheid. Zo zal in de praktijk veelal sprake zijn van een combinatie van een verzoek om toestemming tot interceptie op grond van artikel 48 en een verzoek voor onderzoek als bedoeld in artikel 49, eerste lid, aanhef en onder a, in verband met het feit dat de ene bevoegdheid ondersteunend is aan de uitvoering van de ander. Omdat niet geïntercepteerd wordt om te intercepteren, zal een last voor interceptie (artikel 48) gevolgd worden door verzoeken om toestemming voor inzet van de bevoegdheden in de andere fasen (artikelen 49 en 50). Interceptie vindt immers juist plaats met het oog op de uitoefening van de bevoegdheden tot search en selectie. Dat laat onverlet dat de voor de uitoefening van deze bevoegdheden vereiste toestemming op de voorgeschreven wijze dient te worden verkregen; elk verzoek om toestemming dient aan de daaraan gestelde eisen te voldoen.
Voor het deel van deze vraag inzake datareductie verwijs ik u naar het eerdere antwoord op de vraag van de leden van de VVD-fractie over het filteren en verwijderen van gegevens bij onderzoeksopdracht gerichte interceptie onder 3.3.3.3.5.1.

De leden van de ChristenUnie-fractie vragen of de gegevens die zijn verzameld in de eerste of tweede fase van onderzoeksopdrachtgerichte interceptie op enigerlei wijze mogen worden gedeeld met het buitenland. Door de diensten verzamelde gegevens kunnen, mits aan de wettelijke vereisten ter zake wordt voldaan, worden gedeeld met een buitenlandse dienst. Voor de duidelijkheid wordt opgemerkt dat enkel data kunnen worden gedeeld die daadwerkelijk beschikbaar zijn. Zoals voorgaand beschreven wordt een zeer groot percentage van de in fase 1 toegankelijke data dus niet opgeslagen en dus niet gedeeld met buitenlandse diensten.

De leden van de GroenLinks-fractie vragen naar het gebruik van de term onderzoeksopdrachtgerichte interceptie. Zij vragen ook waarom geen gehoor is gegeven aan het advies van de Raad van State om de bewaartermijn voor aldus verworven gegevens te beperken tot één jaar, en verzoeken om een definitie van hetgeen een ‘onderzoeksopdracht’ kan behelzen, aan welke vereisten deze opdrachten dienen te voldoen en of de CTIVD in voldoende mate in staat zal zijn om in dit kader toezicht uit te oefenen. Ik verwijs allereerst naar mijn beantwoording van de vragen van de VVD-fractie over het gebruik van de term ‘sleepnet’ onder paragraaf 12.1.1. Voor wat betreft het antwoord op de vraag over de bewaartermijn verwijs ik deze leden naar mijn eerdere antwoord op de vraag van de leden van de VVD-fractie over de bewaartermijnen bij onderzoeksopdrachtgerichte interceptie. Waar het gaat om de definitie van ‘onderzoeksopdracht’, merk ik het volgende op. Zoals ook in de Wiv 2002 reeds het geval is, zijn in het wetsvoorstel de taken van de AIVD en de MIVD gedefinieerd. Buiten deze taken kan niet worden getreden. De taken worden inhoudelijk ingevuld door de Geïntegreerde Aanwijzing, waarin de regering in de richting van de diensten aangeeft wat noodzakelijk wordt geacht voor een veilig Nederland, voor een goed geïnformeerde regering en voor de internationale veiligheid. Zie ook hetgeen ik eerder heb opgemerkt over de Geïntegreerde Aanwijzing. De onderzoeken van de diensten zijn dus helder ingekaderd. Voor die onderzoeken waardoor dat noodzakelijk is en voldaan wordt aan de

eisen van proportionaliteit en subsidiariteit, kan onderzoeksopdrachtgerichte interceptie worden ingezet. Het ontvangen van telecommunicatie is altijd zo gericht mogelijk.

De leden van de GroenLinks-fractie vragen de regering hoeveel opslagruimte zal worden gereserveerd voor de via de sleepnetbevoegdheid ontvangen gegevens en welke kosten daaraan zijn verbonden. Zoals in de beantwoording onder 12.1.1 wordt aangegeven, is er geen sprake van een sleepnetbevoegdheid. Er is geen gekwantificeerde hoeveelheid opslagruimte voor onderzoeksopdrachtgerichte interceptie gereserveerd. Bij de implementatie van de interceptie van telecommunicatie op kabelgebonden netwerken is sprake van schaalbaarheid in omvang en tijd. De kosten voor opslagruimte zijn onderdeel van de in hoofdstuk 11 opgenomen financiële gevolgen, die kaderstellend zijn voor implementatie en toepassing van de uitoefening van de bevoegdheid. De betrokken departementen zullen de mate waarin van deze bevoegdheid gebruik wordt gemaakt, de opbrengsten ervan voor de taakuitoefening van de diensten en de hiermee samenhangende kosten, jaarlijks evalueren.

De leden van de GroenLinks-fractie vragen de regering in het bijzonder naar de proportionaliteit van de duur van een onderzoeksopdracht die ten grondslag ligt aan de sleepnetbevoegdheid. Deze leden vragen waarom gekozen is voor de zeer ruime periode van een jaar. Ik verwijs deze leden graag naar het antwoord dat ik eerder in deze paragraaf heb gegeven op vragen van de leden van de D66-fractie inzake de gehanteerde toestemmingstermijnen bij de onderzoeksopdrachtgerichte interceptie.

De leden van de GroenLinks-fractie of er niet een principiële grens wordt overschreden door de medewerkingsplicht bij de hier bedoelde interceptiebevoegdheid. Naar mijn mening is dat geenszins het geval en is die in lijn met andere reeds bestaande medewerkingverplichtingen in het kader van interceptie van telecommunicatie.

De leden van de SGP-fractie onderkennen het belang van onderzoeksopdrachtgerichte interceptie, en vragen of de regering van mening is dat met de in het wetsvoorstel opgenomen waarborgen voldoende waarborgen zijn opgenomen voor de bescherming van de privacy en de eerbiediging van de persoonlijke levenssfeer? Ik realiseer mij dat de bevoegdheden van de diensten verregaand zijn. De in het wetsvoorstel opgenomen bevoegdheden van de inlichtingen- en veiligheidsdiensten vragen om goede waarborgen. Ruim tien jaar toezicht door de CTIVD geeft een beeld van twee inlichtingen- en veiligheidsdiensten die hun taken zorgvuldig uitvoeren, binnen de kaders van de wet. Het wetsvoorstel geeft extra waarborgen ter bescherming van de privacy en de eerbiediging van de persoonlijke levenssfeer. De bijzondere bevoegdheden van de diensten zijn in overeenstemming met de eisen die daaraan ingevolge de Grondwet en het EVRM (zoals ook neergelegd in de jurisprudentie van het EHRM) worden gesteld in het wetsvoorstel ingekaderd. Met een toets voorafgaand aan de daadwerkelijke uitoefening van een bijzondere bevoegdheid door een nieuwe onafhankelijke toetsingscommissie, toezicht tijdens en achteraf van de onafhankelijke CTIVD, en de mogelijkheid een klacht in te dienen bij de CTIVD die in dat geval bindend oordeel geeft, is voorts het stelsel van rechtsbescherming aanmerkelijk verbeterd. Ik ben van mening dat het stelsel van waarborgen in het wetsvoorstel robuust is.

De leden van de SGP-fractie vragen hoe is gewaarborgd dat iemand die mee dient te werken aan het doorbreken van versleuteling zo min mogelijk te maken krijgt met negatieve consequenties hiervan. Op grond van de artikelen 45 en 57 van het

wetsvoorstel kunnen de AIVD en MIVD zich wenden tot degenen die kennis dragen van de wijze van versleuteling van gesprekken, telecommunicatie of gegevensoverdracht, met de opdracht alle noodzakelijke medewerking te verlenen voor ontsleuteling om zo tot het ontsleutelen van de gegevens te komen door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken. Met de formulering in het wetsvoorstel is aansluiting gezocht bij artikel 126m, elfde lid, van het Wetboek van Strafvordering. Degene aan wie de opdracht tot medewerking wordt gericht is verplicht daaraan te voldoen. Het niet meewerken aan een verzoek is in artikel 143 van het wetsvoorstel strafbaar gesteld. De diensten kunnen iemand die de kennis niet heeft om de wijze van versleuteling ongedaan te maken, vanzelfsprekend niet dwingen. De hoofden van de diensten hebben ingevolge artikel 23, aanhef en onder c, van het wetsvoorstel een zorgplicht voor de veiligheid van de personen met wier medewerking gegevens worden verzameld. Deze zorgplicht strekt naar mijn mening ook uit tot degene die medewerking verleent aan de ontsleuteling van gegevens.

3.3.3.3.5.2 Informatie en medewerkingsplicht aanbieders van communicatiediensten bij de verwerving van telecommunicatie op grond van artikel 47 en 48 (§3.3.4.4.7.5 m.v.t.)

De leden van de D66-fractie vragen op welke wijze de regering voornemens is overleg te plegen met een aanbieder van een communicatiedienst alvorens op grond van artikel 53 opdracht gegeven wordt om medewerking te verlenen. Allereerst zal contact worden gezocht met de aanbieder van een communicatiedienst om gegevens te verzamelen, welke noodzakelijk zijn om uitvoering te kunnen geven aan de bevoegdheid tot zowel gerichte- als onderzoeksopdrachtgerichte interceptie. Het gaat hierbij bijvoorbeeld om technische gegevens die zicht bieden op de door de aanbieder verzorgde communicatiediensten alsmede hoe en waar communicatie verloopt. Ook kunnen de gegevens betrekking hebben op de fysieke en logische inrichting van netwerken, routering en signaaleigenschappen. Deze gesprekken zullen met meerdere aanbieders van communicatie worden gevoerd en op deze manier kunnen de diensten bepalen over welke kabel de voor hen relevante communicatie zich verplaatst. Op deze manier wordt de netwerktopologie inzichtelijk. Artikel 52 van het wetsvoorstel biedt voor het opvragen van dergelijke gegevens de wettelijke grondslag.
Zodra de diensten weten welke aanbieder van communicatie zij op grond van artikel 53 willen benaderen, wordt hiertoe een verzoek om toestemming gedaan aan de betreffende minister. Indien de betreffende minister toestemt, zullen de diensten in overleg treden met de betreffende communicatieaanbieder om nadere invulling te geven aan het verzoek en de verlangde medewerking. Zo bevat het voornoemde verzoek naar verwachting nog niet alle details van de verlangde medewerking zoals de precieze specificaties van de technische voorzieningen en dergelijke. Het wettelijk voorgeschreven nader overleg met de aanbieder is onder meer bedoeld om hieraan nader uitwerking te geven. Ook kan dan over andersoortige aangelegenheden als de implementatietermijn en eventuele personele en organisatorische aspecten verbonden aan de uitvoering van de verleende toestemming worden gesproken. Denk daarbij aan de te nemen beveiligingsmaatregelen en het aanwijzen van vertrouwensfuncties. Overigens zal er in de praktijk regelmatig contact en overleg zijn tussen de diensten en de betreffende aanbieders over de diverse aspecten van de tenuitvoerlegging van de verleende toestemming.

De leden van de D66-fractie vragen naar het overleg tussen de regering en aanbieders, en vraagt of de regering ook inziet dat voor het efficiënt en effectief inzetten van de interceptiebevoegdheid goed en constructief overleg nodig zal zijn. Verschillende bedrijven hebben gereageerd in het kader van de internetconsultatie van het ontwerp-voorstel voor de nieuwe wet. De regering is met de sector in overleg getreden over de zorgen die bij de sector leefden. Het in de afgelopen periode gevoerde overleg met de communicatieaanbieders wordt door de regering als waardevol beschouwd. Een goede verstandhouding met de sector is inderdaad van belang voor het kunnen uitvoeren van de interceptiebevoegdheid. Niet voor niets is het overleg met de aanbieder van een communicatiedienst ingeval van een opdracht tot interceptie verankerd in de wet.

De D66-fractie vraagt in welke mate bij de diensten en de betrokken ministeries ambtenaren aanwezig zijn die (uitgebreide) kennis hebben van de communicatiedienstensector. Bij de diensten en ministeries zijn in voldoende mate specialisten op het gebied van communicatiediensten in dienst.

De leden van de D66-fractie hebben vragen gesteld over de formulering van de kostenvergoeding voor communicatiedienstaanbieders. Ik kan deze leden mededelen dat de vergoeding naar redelijkheid in de praktijk zal neerkomen op een vergoeding van de kosten die rechtstreeks voortvloeien uit de inzet van de bevoegdheid, mits kan worden aangetoond dat de kosten die men heeft gemaakt niet als overmatig kunnen worden aangemerkt. De aanbieder zal deze kosten moeten onderbouwen.
Omdat het hier publieke middelen betreft moet worden voorkomen dat aanspraak gemaakt zou kunnen worden op onredelijke vergoedingen door bijvoorbeeld het hanteren van excessieve, en in vergelijking met andere partijen, niet gangbare uurtarieven.
Voor wat betreft het externaliseren van kosten wordt opgemerkt dat het budget met 20 miljoen is uitgebreid. Binnen dit financiële kader moet de inzet van de bevoegdheid inclusief de vergoeding aan telecomaanbieders plaatsvinden. Het beeld dat een dempende prikkel is weggenomen of het risico dat sluipenderwijs meer data binnengehaald wordt, is niet in overeenstemming met dit financiële kader.

De leden van de D66-fractie vragen naar de belasting van aanbieders van telecommunicatiediensten door de medewerkingsplicht. Hoe kan een aanbieder laten weten dat hij onevenredig getroffen wordt, wordt de aanbieder gehoord door de TIB en kan het zo zijn dat het ontbreken van overleg een reden is om de ministeriële toestemming niet te accorderen? Ik wil hier graag als volgt op reageren. Weliswaar berust er een medewerkingsplicht bij de aanbieder van de communicatiedienst, maar de regering ziet het grote gezamenlijke belang ten aanzien van zowel de taakuitvoering van de aanbieders, als het kunnen verrichten van de interceptie. Ook de regering is bij de medewerkingsplicht gebonden aan de vereisten van redelijkheid en billijkheid zoals in het Nederlandse rechtsverkeer betamelijk is. Zoals eerder uiteengezet zullen de regering en de aanbieder voorafgaand aan het feitelijk plaatsvinden van de interceptie met elkaar in gesprek gaan om alle facetten waaronder de effecten van de interceptie op de bedrijfsvoering van de aanbieder te bespreken. Deze overlegplicht is eveneens verankerd in het wetsvoorstel (artikel 53, vierde lid). Een aanbieder zal niet door de TIB worden gehoord voorafgaand aan de beslissing van de TIB. De TIB verricht immers uitsluitend een rechtmatigheidstoets op de door de minister verleende toestemming. In het verzoek om toestemming aan de minister zal echter naast hetgeen in artikel 29, tweede lid, is bepaald, ook ingegaan moeten worden op hetgeen in artikel 53, derde lid,

van het wetsvoorstel is bepaald. Dat betekent dat ook de soort medewerking die aan de aanbieder wordt opgedragen dient te worden beschreven. Indien er duidelijke contra-indicaties aanwezig zijn, zoals verwoord in het voorbeeld van de leden van D66, zullen deze vanzelfsprekend in het verzoek om toestemming aan de minister dienen te worden gemeld. Deze informatie komt uiteindelijk ook bij de TIB terecht, die dat in haar beoordeling kan betrekken.

De leden van de D66-fractie vragen of de regering uitsluit dat bedrijven geremd worden in het bieden van veiligheid aan hun consumenten of in hun technologische ontwikkeling ten gevolge van het in stand moeten houden van technische voorzieningen ten behoeve van de diensten. Indien dat het geval is, dan vragen deze leden hoe dat is geborgd. Indien dat niet het geval is, dan vragen deze leden hoe de beide belangen tegen elkaar worden gewogen. Ik sluit hierbij uit dat van overheidswege ten behoeve van de inlichtingen- en veiligheidsdiensten aan bedrijven verplichtingen worden opgelegd die remmend werken op het bieden van veiligheid aan consumenten of technologische ontwikkeling. Datzelfde geldt voor het niet kunnen updaten van beveiligingssystemen of encryptie.

3.3.3.3.5.3 Informatieverzoeken en medewerkingsplicht met betrekking tot telecommunicatiegegevens (§3.3.4.4.7.6 m.v.t.)

De leden van de D66-fractie kunnen in artikel 55 niet met zekerheid teruglezen hoe gericht het opvragen van mastgegevens zal plaatsvinden. Zij vragen of het gaat om een straal van 10 meter, 100 meter, 1 kilometer of 10 kilometer, en of het gaat om elke ontmoeting waar de dienst in geïnteresseerd is, of enkel om ontmoetingen waarbij niet iemand kan observeren wie er aanwezig zijn. De gevraagde kwantificering is altijd afhankelijk van de weging van noodzakelijkheid, proportionaliteit en subsidiariteit en kan dus niet worden gegeven. De uitoefening van de bevoegdheid tot het opvragen van mastgegevens zal gericht geschieden, in die zin dat het altijd gegevens betreft die aan een gespecificeerde locatie zijn gerelateerd (zie artikel 55, derde lid, onder b). Voor de uitoefening van deze bevoegdheid is toestemming vereist van de betreffende minister of namens deze het hoofd van de dienst. Bijzondere bevoegdheden worden nooit zonder reden ingezet: in het verzoek om toestemming worden het doel en de noodzakelijkheid (waarin de evenredigheid en subsidiariteit beoordeeld dienen te worden) van de inzet van de bevoegdheid aangegeven. Hiermee wordt in tegenstelling tot de huidige regeling, waarbij geen toestemmingsvereiste is gesteld, voorzien in een extra waarborg. In zijn algemeenheid geldt dat het zendbereik van een antenne voor gsm of UMTS door tal van omgevingsfactoren wordt beïnvloed, zoals hoge bebouwing, dichte bebossing en diverse atmosferische omstandigheden.

De leden van de fractie van D66 merken op dat bij algemene maatregel van bestuur de gegevens worden aangewezen waarop de opdracht tot verstrekking van gegevens ex artikel 55, eerste lid, van het wetsvoorstel betrekking kan hebben. Zij wensen reeds enig inzicht te krijgen om wat voor soort type gegevens het gaat. Het gaat hierbij om grotendeels dezelfde gegevens die nu reeds zijn opgenomen in het Besluit ex artikel 28 Wiv 2002, maar die vanwege het bredere bereik van de regeling – zowel wat de aanbieders betreft als de communicatiediensten waarop het betrekking heeft – daaraan is aangepast. Het gaat om de volgende gegevens:

a. de naam, het adres en de woonplaats van de gebruiker;

b. de nummers of technische kenmerken van de gebruiker;
c. de naam, het adres, de woonplaats en het nummer of het technisch kenmerk van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft, heeft gehad of heeft getracht tot stand te brengen, of van de natuurlijke persoon of rechtspersoon die heeft getracht met de gebruiker verbinding tot stand te brengen;
d. de datum en het tijdstip waarop de verbinding met de gebruiker tot stand is gebracht en beëindigd en de duur van de verbinding, dan wel, indien er geen verbinding tot stand is gekomen, de datum en het tijdstip waarop is getracht verbinding met de gebruiker tot stand te brengen, alsmede de afwijking van dit tijdstip van de wettelijke tijd, bedoeld in artikel 1, eerste lid, van de wet van 16 juli 1958 tot nadere regeling van de wettelijke tijd (Stb. 352);
e. de locatiegegevens van het netwerkaansluitpunt dan wel gegevens betreffende geografische posities van de randapparatuur van een gebruiker gedurende de tijd dat er een verbinding is met het netwerk, of ingeval van een poging tot verbinding;
f. de nummers van de randapparatuur waarvan de gebruiker gebruik maakt of heeft gemaakt;
g. de soort diensten waarvan de gebruiker gebruik maakt of heeft gemaakt evenals de daarbij behorende gegevens;
h. de naam, het adres, de woonplaats van degene die de rekening betaalt voor de communicatiediensten die de gebruiker ter beschikking heeft of heeft gehad en het daartoe gebruikte bankrekeningnummer;
i. nummers of technische kenmerken van de randapparatuur van gebruikers die gedurende een bepaalde periode, op een nader aangeduide locatie, verbinding maken of hebben gemaakt met het communicatienetwerk van de aanbieder.

In dit verband is het van belang het volgende op te merken. Er is voor gekozen om – evenals in het vervallen Besluit ex artikel 28 Wiv 2002 (dat zowel betrekking had op alle openbare telecommunicatienetwerken en –diensten) – niet te differentiëren naar soort communicatiedienst maar te voorzien in een limitatieve lijst van categorieën van verkeers- en locatiegegevens en die voorts in algemene bewoordingen te omschrijven. Met de gekozen benadering kan ook worden volstaan nu de verplichting tot verstrekking voor de aanbieder van een communicatiedienst zich immers slechts uitstrekt tot die verkeers- en locatiegegevens die de aanbieder in het kader van de eigen bedrijfsvoering ter beschikking krijgt; men heeft geen vergaar- of bewaarplicht. Het begrip verbinding, zoals dat hier wordt gebruikt, heeft voorts een andere betekenis dan in het Besluit ex artikel 28 Wiv 2002. De uitleg die hieraan in de toelichting op het Besluit ex artikel 28 Wiv 2002 is gegeven dient in het licht van de ontwikkelingen in de elektronische communicatiesector die zich sinds de totstandkoming van dat besluit hebben voorgedaan alsmede de uitbreiding van de reikwijdte van de informatieverplichting tot alle communicatiediensten, te worden herijkt. In de toelichting op het Besluit ex artikel 28 Wiv 2002 is voor de uitleg (uitsluitend) aangesloten bij de toenmalige gebruikelijke communicatievormen (zoals conventionele spraaktelefonie en datatransmissie via internet). Dat betrof in het bijzonder de situaties waarbij tussen gebruikers uitwisseling van communicatie over een openbaar telecommunicatienetwerk plaatsvond en waarbij (telkens) een actieve handeling tot het leggen van die verbinding vereist was. Deze uitleg doet geen recht aan de ontwikkelingen die zich sindsdien hebben voorgedaan, zoals de enorme proliferatie van het gebruik van smartphones en tablets alsmede de ontwikkeling van OTT-diensten. Communicatie vindt in toenemende plaats via het

gebruik van apps met chatfunctionaliteit. Het grootste verschil met toen is wellicht het feit dat bij het gebruik van deze nieuwe communicatiemiddelen, zoals smartphones en tablets, er thans sprake is van een continu verbinding met internet. Gebruikers ontvangen automatisch mails, berichten en nieuwsupdates (pushberichten), mede op basis van locatiegegevens van de door de gebruiker gehanteerde mobiele randapparatuur. Hiervoor dienen geen actieve handelingen, zoals inloggen bij een internettoegangsdienst of op een mailaccount, meer te worden verricht. Er vindt dus de hele dag datatransmissie plaats. Bij de meeste apps worden automatisch allerlei gegevens van gebruikers gedeeld met de beheerder van de betreffende app, zoals bijvoorbeeld locatiegegevens. Dat gebeurt niet eenmaal, maar gedurende de gehele periode dat er sprake is van verbinding met internet. Het begrip 'verbinding' dient in deze context, naast de traditionele uitleg die ook zijn relevantie blijft behouden, dan ook te worden herijkt. Onder verbinding moet dan ook worden verstaan de gevallen waarbij onder gebruikmaking van deze nieuwe diensten een chatbericht wordt verzonden of ontvangen, een Voice Over IP-gesprek (VOIP) wordt opgezet.

3.3.3.3.5.4 Medewerkingsplicht bij ontsleuteling van communicatie (§3.3.4.4.7.7 m.v.t.)

De leden van de D66-fractie vragen waarom niet expliciet is opgenomen in het wetsvoorstel dat medewerkingsplicht bij ontsleuteling geen bevoegdheid betreft om te verzoeken tot het afzwakken van encryptie van systemen en/of het inbouwen van toegang tot de systemen om ontsleutelde gegevens te verkrijgen. Zoals eerder is aangegeven in mijn antwoord op vragen van de PvdA-fractie onder 3.3.3.3.4 kan uit de medewerkingsplicht geen bevoegdheid van de diensten worden afgeleid tot het (doen) inbouwen van achterdeuren in systemen om aldus toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor bijvoorbeeld aanbieders van communicatiediensten om de encryptie die in hun systemen is toegepast te verzwakken. De tekst van het wetsartikel laat daarover geen enkele twijfel ontstaan. Het betreffende amendement van het lid Verhoeven (Kamerstukken II 2016/17, 34588 nr. 13) komt mij dus als overbodig voor.

De leden van de D66-fractie hebben via de media begrepen van de AIVD druk bezig is de encryptie van Whatsapp te verbreken en vragen hoe een eventueel verzoek aan de makers van Whatsapp om mee te helpen communicatie te ontsleutelen vorm zal krijgen. Ook vragen zij wanneer wordt volstaan met het meewerken aan het ongedaan maken van versleuteling en wanneer wordt vereist dat een persoon actief zelf de versleuteling ongedaan maakt. Zoals aangegeven in eerdere antwoorden over dit onderwerp hebben de diensten zowel in de huidige wet als in het onderhavige wetsvoorstel de bevoegdheid om versleuteling in specifieke gevallen ongedaan te maken en kunnen daartoe aan derden medewerking verzoeken. Indien deze derde niet beschikt over de sleutel, dan kunnen de diensten enkel trachten zelf de versleuteling ongedaan te maken.

De leden van de D66-fractie hebben een aantal vragen gesteld over media-uitlatingen van de DG AIVD en de NCTV over de wens encryptie te mogen doorbreken, en over de relatie tussen media-uitlatingen en het kabinetsstandpunt dat doorbreking van encryptie niet aan de orde is. Ik kan hier helder over zijn. Het afzwakken van encryptie is niet aan de orde, het ongedaan maken van versleuteling in specifieke, bij de wet voorziene gevallen wel. De uitlatingen van de genoemde ambtenaren passen dan ook binnen het

kabinetsstandpunt over encryptie. [8] Het belang van het rechtmatig kunnen doorbreken van encryptie wordt daarin benadrukt (zie blz. 3).

De leden van de D66-fractie stellen verder een aantal vragen over uitspraken van de DG AIVD in de Volkskrant van 17 september 2016 en van de NCTV in de Telegraaf van 16 december 2016 over het inzien van communicatie van terroristen en over privacy-waarborgen in relatie tot bulkinterceptiebevoegdheden. De DG AIVD heeft gewezen op de duistere kant van encryptie, zoals deze ook in het kabinetsstandpunt wordt benoemd. Kwaadwillenden maken immers ook gebruik van encryptie. Het kabinetsstandpunt is helder: afzwakken van encryptie is niet aan de orde, het doorbreken ervan in specifieke, bij de wet voorziene gevallen, is dat wel. In het wetsvoorstel wordt de bevoegdheid tot dit laatste, net als in de huidige wet, neergelegd.
In de uitspraak over privacy wijst de directeur-generaal van de AIVD op het feit dat altijd naar een balans tussen veiligheid en privacy dient te worden gezocht en dat dus ook het belang van privacy niet absoluut is. Het kabinet heeft in het voorliggende wetsvoorstel gestalte gegeven aan deze balans. Ook de NCTV wijst hierop. Dat de CTIVD over het wetsvoorstel een zienswijze heeft uitgebracht waarin zij stelt dat essentiële privacywaarborgen ontbreken, doet daar niet aan af.

De leden van de D66-fractie hebben een aantal vragen gesteld over het informeren van belangendragers over significante kwetsbaarheden, en over het inkopen van kwetsbaarheden. Het kabinet heeft het beleid neergelegd in de eerder - in het antwoord op vragen van de SP-fractie onder 3.3.3.3.4 - gememoreerde reactie op de motie De Vries. De hoofdregel is dat significante kwetsbaarheden die de belangen van gebruikers op internet schaden worden gemeld. Wettelijke argumenten die een melding in de weg kunnen staan, zijn het belang van de bescherming van het actueel kennisniveau, de werkwijze of de bronnen van de diensten. De soort kwetsbaarheden waar de diensten zich op richten, kunnen niet door een ieder gevonden worden. Indien bijvoorbeeld een bron in de buurt van terroristische cel kennis heeft van de technische kwetsbaarheden in de zeer besloten communicatieomgeving van die cel, dan zal het melden van die kwetsbaarheden de bron compromitteren. Het actueel kennisniveau kan een melding in de weg staan indien deze specifiek is voor de beveiligde communicatiestructuur van de organisatie die de diensten onderzoeken. De melding zou deze organisatie dan erop alerteren dat zij onderwerp is van onderzoek door de diensten. De bovengenoemde gronden zijn niet van die aard, dat zij altijd kunnen worden ingeroepen. Integendeel, hoe significanter de kwetsbaarheid en hoe groter de groep voor wie de kwetsbaarheid relevant is, hoe minder voorstelbaar het is dat de bovengenoemde gronden kunnen worden ingeroepen. Overigens kan de CTIVD op de bovengenoemde praktijk toezicht houden en hierover rapporteren aan het parlement.
Voor het al dan niet melden van een kwetsbaarheid is een aantal zaken relevant, zoals de vraag of de kwetsbaarheid het gevolg is van onachtzaamheid bij het target of dat het een systeemkwetsbaarheid betreft, of dat de systeemkwetsbaarheid reeds publiek bekend is, welk zwaarwegend belang ermee kan zijn gemoeid en in hoeverre er schade op kan treden. De afweging tot het al dan niet melden van een kwetsbaarheid is uiteindelijk maatwerk. Er is geen vast impactniveau en de impact gaat niet alleen om de hoeveelheid geraakte mensen c.q. bedrijven, maar ook om de ernst van de schade die kan ontstaan op individueel niveau.

[8] Kamerstukken II 2015/16, 26 643, nr. 383.

Voor wat betreft de vragen aangaande de aankoop van kwetsbaarheden wordt verwezen naar de beantwoording van eerdere vragen van de leden van de D66-fractie in paragraaf 3.3.3.3.4.

De regering deelt de mening van de leden van de GroenLinks-fractie dat druk jegens aanbieders van communicatiediensten om zwakheden in software in te bouwen of encryptie te verzwakken onwenselijk is. De CTIVD kan vanuit haar wettelijke taak erop toezien dat de AIVD en de MIVD niet een dergelijke druk zullen uitoefenen.

Waar het gaat om de vragen van de leden van de GroenLinks-fractie om uit te sluiten dat zogenoemde 'zero day'-beveiligingslekken worden aangekocht door de diensten in het kader van de bevoegdheid tot het (doen) ontsleutelen van encryptie, alsmede te bevestigen dat door de diensten bij het ontsleutelen van encryptie gebruikte kwetsbaarheden terstond aan fabrikanten zullen worden gemeld indien het gebruik ervan niet langer strikt noodzakelijk is voor de modus operandi van de diensten, en dat de CTIVD hier strikt op zal toetsen, verwijs ik deze leden naar het antwoord dat ik eerder op vergelijkbare vragen in paragraaf 3.3.3.3.4 van deze nota heb geantwoord.

3.4 Het uitbrengen van verslag omtrent de uitoefening van enkele bijzondere bevoegdheden

De leden van de D66-fractie geven aan dat het hen niet geheel duidelijk is op grond van welke criteria de lijst van bijzondere bevoegdheden waarvoor een actieve notificatieplicht geldt tot stand is gekomen. Zij vragen of het klopt het dat de lijst (grotendeels) is gekopieerd uit de huidige wet. Er is niet overwogen om de lijst met andere bijzondere bevoegdheden uit te breiden. Daartoe bestaat naar mijn mening ook geen noodzaak, ook niet vanuit het perspectief van het EVRM. De Nederlandse regering heeft zich immers altijd op het standpunt gesteld, dat uit het EVRM geen actieve notificatieplicht voortvloeit. Het EHRM beschouwt de aanwezigheid van een notificatieplicht weliswaar als een belangrijke waarborg tegen misbruik van bevoegdheden, maar het gewicht van zo'n plicht moet worden afgezet tegen het geheel van overigens aanwezige rechtswaarborgen. Daar komt bij dat de tenuitvoerlegging van de notificatieplicht een aanzienlijk beslag legt op de capaciteit van de diensten en die zal naar verwachting in de toekomst alleen maar toenemen. De praktijk wijst uit dat notificatie niet leidt tot een toename van klachten of inzageverzoeken. Ook vanuit die optiek bezien zie ik geen reden de notificatieplicht uit te breiden tot andere bijzondere bevoegdheden.

3.5 Geautomatiseerde (big) data-analyse door de diensten

De leden van de D66-fractie vragen zich af hoe geborgd wordt dat de context van de geanalyseerde metadata altijd duidelijk blijft. Er is weliswaar ten opzichte van eerdere versies van het wetsvoorstel een waarborg opgenomen die het verbiedt maatregelen te treffen jegens een persoon uitsluitend op basis van resultaten van een gegevensverwerking, maar de beoordelaar van dat resultaat zal om een daadwerkelijk verschil te kunnen maken, wel voldoende inzicht in en begrip van de gepresenteerde resultaten moeten hebben. Is de regering bereid te onderzoeken welke manier van presentatie van die analyseresultaten de grootste zorgvuldigheid bij de menselijke interpretatie tot stand brengt? Worden daar ook gedragswetenschappers bij betrokken? Indien één van beide vragen met nee beantwoord wordt, waarom niet?

Ik wil hier als volgt op reageren. Ik onderschrijf het belang van terdege kennis over welke manier van presentatie van analyseresultaten de grootste zorgvuldigheid bij de menselijke interpretatie tot stand brengt. Het onderzoeken van grote hoeveelheden data, inclusief metadata, is voor de diensten geen nieuw fenomeen. De medewerkers van de diensten zijn opgeleid om met dergelijke vraagstukken om te gaan. Het hoort bij de professionaliteit van hun dagelijks werk. De diensten maken gebruik van gedragswetenschappers. Deze vraagstukken vergen continue aandacht, omdat ze steeds in beweging zijn. Een onderzoek hiernaar zou naar mijn oordeel slechts van beperkte en tijdelijke waarde zijn.

3.6 De verstrekking van gegevens

De leden van de CDA-fractie vragen of in artikel 64 van het wetsvoorstel sprake is van een nieuwe bevoegdheid, of van een bevoegdheid die nu al bestaat met betrekking tot de gegevens die op grond van artikel 27, eerste lid, Wiv 2002 zijn verworven. Tevens vragen zij onder welke voorwaarden ongeëvalueerde gegevens kunnen worden verstrekt aan buitenlandse collegadiensten en op welke wijze wordt gegarandeerd dat de waarborgen die van toepassing zijn op het verzamelen en verwerken van gegevens door de diensten ook van toepassing zijn als gegevens worden verstrekt aan buitenlandse collegadiensten. De verstrekking van ongeëvalueerde gegevens (verkregen op grond van artikel 27 lid 1 Wiv 2002) aan een buitenlandse dienst vindt thans plaats op grond van artikel 36 Wiv 2002 (in het kader van een goede taakuitvoering) respectievelijk artikel 59 Wiv 2002 (in het belang van de buitenlandse dienst). Het betreft geen nieuwe bevoegdheid.

Een intensieve samenwerking met buitenlandse diensten is onmisbaar voor het beschermen van de nationale veiligheid. Of het nu gaat om het uitwisselen van identifiers van terroristen die Europa inreizen, het uitwisselen van signatures van cyberaanvallen gericht op het hoogwaardig Europees bedrijfsleven of het met bondgenoten uitvoeren van militaire operaties in brandhaarden over de wereld: de razendsnelle uitwisseling van gegevens blijft doorslaggevend voor het nemen van adequate tegenmaatregelen. Het delen van gegevens, waaronder ook ongeëvalueerde gegevens maakt hier onderdeel van uit. In beginsel kan elke soort informatie worden gedeeld met een buitenlandse dienst, zolang deze door de AIVD of MIVD rechtmatig is vergaard. Niet elke buitenlandse dienst komt echter voor het delen van gegevens in aanmerking. Voorafgaand aan het aangaan van een samenwerkingsrelatie met de buitenlandse dienst waarmee informatie wordt gedeeld, wordt deze relatie gewogen aan de hand van een aantal criteria waaronder de democratische inbedding en de eerbiediging van de mensenrechten door het desbetreffende land en de professionaliteit en betrouwbaarheid van de dienst. De samenwerkingsrelatie kan pas worden aangegaan nadat de minister hiervoor toestemming heeft verleend. Voorafgaand aan het delen van informatie wordt beoordeeld of het delen bijdraagt aan de goede taakuitvoering door de diensten of dat deze zich er niet tegen verzet. Voor het delen van ongeëvalueerde gegevens geldt voorts dat dit slechts met een beperkt aantal betrouwbare partners en met toestemming van de minister plaatsvindt.

Voor de buitenlandse diensten kunnen op grond van eigen wet en regelgeving andere waarborgen gelden dan voor de AIVD en MIVD. Bij de overweging om gegevens te verstrekken aan een buitenlandse dienst wordt tevens overwogen of de door de buitenlandse dienst te behartigen belangen niet onverenigbaar zijn met de belangen die

de Nederlandse diensten hebben te behartigen. Dit is ook zo in de wet vastgelegd. De risico's die het delen van ongeëvalueerde gegevens met zich meebrengen dienen voorafgaand aan de toestemming van de betreffende minister zoveel mogelijk in kaart worden gebracht. Indien een bepaald risico zich in de praktijk heeft voorgedaan dan kan dat reden zijn voor de heroverweging van een samenwerking.

Er kunnen garanties worden gevraagd van buitenlandse diensten. Evenwel kan ik de tenuitvoerlegging van die garanties niet controleren.

3.6.1 De externe verstrekking van gegevens (§3.6.3 m.v.t.)

De leden van de GroenLinks-fractie vragen de regering aan te geven waar de grens ligt welke organisaties kunnen vallen onder het begrip "daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen". De bepaling is afdoende scherp geformuleerd, maar is door zijn formulering ook voldoende flexibel. Andere landen kennen immers een andere opzet van de diensten, bijvoorbeeld aparte inlichtingendiensten en aparte veiligheidsdiensten, veiligheidsdiensten die ook opsporingstaken hebben of aparte diensten die zich enkel bezighouden met bijvoorbeeld satellietinterceptie. Door in de memorie van toelichting een aantal organisaties te noemen is een beeld geschetst van de soort organisaties waaraan moet worden gedacht.

De leden van de GroenLinks-fractie geven aan ernstige bedenkingen te hebben bij de bevoegdheid tot het verstrekken van niet-geëvalueerde gegevens aan buitenlandse diensten. De leden van de GroenLinks-fractie vragen de regering in te gaan op het risico dat bijvoorbeeld informatie over een in een bepaald land vervolgde persoon zo op een presenteerblaadje wordt aangeleverd, via gegevensverstrekking aan de veiligheidsdienst van het betreffende land. Deze leden vragen de regering nader te motiveren waarom het in bepaalde situaties van vitaal belang kan zijn om niet-geëvalueerde gegevens te delen met buitenlandse diensten en vragen waarom het niet mogelijk is dat de betreffende gegevens met spoed worden geëvalueerd. In reactie op deze vragen antwoord ik als volgt. Het delen van ongeëvalueerde gegevens vindt reeds onder de huidige wet plaats. Het vindt in principe alleen plaats met betrouwbare partners en onder de voorwaarden dat de gegevens niet aan derden mogen worden verstrekt zonder uitdrukkelijke toestemming van de verstrekkende dienst (de zogenaamde derde partijregel). Het met spoed evalueren is niet mogelijk gezien de soms grote hoeveelheid van de gegevens en vanwege mogelijke tijdkritische factoren zoals bijvoorbeeld een op handen zijnde aanslag of bij tactische informatie voor coalitiepartners bij het uitvoeren van een militaire missie. Het met spoed evalueren van ongeëvalueerde gegevens kan niet altijd op zinvolle wijze plaatsvinden. Zo kan een gegeven bijvoorbeeld voor de Nederlandse diensten nietszeggend zijn, maar voor de dienst van een ander land het missende stukje informatie betreffen waardoor een netwerk zichtbaar wordt.

In rapport nr. 49 is door de CTIVD vastgesteld dat pas nadat is beoordeeld of de gegevens relevant zijn voor de taakuitvoering van de AIVD/MIVD, sprake kan zijn van geëvalueerde gegevens. In de praktijk betekent dit dat bijvoorbeeld de gegevens aangetroffen op een Iphone bij een potentiële ISIS operative moeten worden aangemerkt als ongeëvalueerd. Indien niet wordt gewacht op de evaluatie van de gegevens, maar deze direct worden gedeeld in het Europese platform van de Counter

Terrorism Group is sprake van het delen van ongeëvalueerde gegevens. Dit voorbeeld illustreert naar mijn oordeel treffend de noodzaak ongeëvalueerde gegevens te kunnen delen.

De leden van de GroenLinks-fractie vragen verder waarom de regering er niet voor heeft gekozen de bevoegdheid tot het verstrekken van niet-geëvalueerde gegevens te beperken tot veiligheidsdiensten waarmee een samenwerkingsverband is aangegaan als bedoeld in artikel 88. Het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten waarmee geen samenwerkingsrelatie bestaat zal zich slechts in uitzonderlijke situatie voordoen. Hierbij kan worden gedacht aan gegevens van personen die nog niet nader door de diensten zijn beoordeeld, maar waarvan wel bekend is dat deze personen in relatie staan tot een ophanden zijnde aanslag. De diensten zullen hierbij een afweging maken tussen het algemeen belang van het voorkomen van de aanslag en een eventueel individueel nadeel dat kan ontstaan wanneer de gegevens worden gedeeld.

3.6.1.1 Algemene bepalingen (§3.6.3.1 m.v.t.)

De leden van de D66-fractie stellen een aantal vragen over de verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten, conform het bepaalde in artikel 64. De leden vragen of het individuele nadeel dat kan ontstaan (bijvoorbeeld een serie doodstraffen doordat per ongeluk gegevens omtrent een groep homoseksueel georiënteerde personen gedeeld wordt) wel op weegt tegen het verkregen voordeel voor het algemeen belang? Voor het antwoord op deze vragen verwijs ik naar hetgeen ik in antwoord op een vraag van de leden van de PvdA-fractie over de wettelijke waarborgen bij het delen van gegevens met buitenlandse diensten heb gesteld. In het hier aangehaalde voorbeeld van een land dat de doodstraf toepast wegens homoseksualiteit, is het overigens zeer onwaarschijnlijk dat het land aan de wegingscriteria voldoet om tot een samenwerkingsrelatie te komen met de betreffende dienst.

De leden van de D66-fractie vragen voorts of de regering kan toelichten wat voor ongeëvalueerde gegevens nu met diensten van andere landen gedeeld worden. Deze leden vragen of de telefoongesprekken die (waarschijnlijk) via GCHQ bij een gesprekanalyse bedrijf in Australië terecht kwamen afkomstig zijn van de Nederlandse diensten, en of de regering het mogelijk, en wenselijk, acht dat Nederlandse diensten ongeëvalueerde gegevens, inclusief persoonlijke gegevens van onschuldige mensen, uit ongerichte kabeltaps delen met andere landen. Deze leden vragen tot slot in hoeverre de mogelijkheid is uitgesloten dat ongeëvalueerde kabelgebonden informatie direct doorgestuurd wordt naar andere landen en in hoeverre het doorsturen van ongeëvalueerde gegevens naar andere landen, waar ruimere bevoegdheden tot analyse van gegevens bestaan, mogelijkheden biedt om de Nederlandse wet te omzeilen.
Ik verwijs allereerst naar mijn eerdere antwoord op vragen van de GroenLinks-fractie over het delen van ongeëvalueerde gegevens onder 3.6.1. Ongeëvalueerde gegevens worden gekenmerkt door het feit dat de precieze inhoud van de gegevens nog niet is beoordeeld. Het delen van deze informatie, die door de diensten rechtmatig moet zijn verkregen in het kader van de wettelijke taakuitvoering, is benodigd voor het verkrijgen van voor Nederland belangrijke informatie. Er kan informatie worden uitgewisseld die anders voor een van de diensten niet of nauwelijks beschikbaar is. Voorts kan door het uitwisselen van ongeëvalueerde gegevens, gefragmenteerde informatie worden aangevuld. Dit kan leiden tot het verkrijgen van benodigde inzichten in een mogelijke dreiging. Het uitsluiten van bepaalde gegevens binnen een set van ongeëvalueerde

gegevens zoals persoonsgegevens is niet altijd mogelijk. Om deze reden is naast het onderzoeksopdrachtgericht verwerven van gegevens ook het delen van ongeëvalueerde gegevens met extra waarborgen omkleed. Voor het antwoord op de vraag met betrekking tot de telefoongesprekken die (waarschijnlijk) via de GCHQ bij een gespreksanalysebedrijf in Australië terecht zijn gekomen verwijs ik naar de brief die op 5 december 2016[9] aan de Tweede Kamer is verzonden.

De leden van de SGP-fractie vragen naar de onderlinge verhouding tussen artikel 64 en artikel 69. Artikel 69 ziet specifiek op het delen van persoonsgegevens waarvan de juistheid redelijkerwijs niet kan worden vastgesteld of die ouder zijn dan 10 jaar en biedt enkele extra waarborgen, bovenop de waarborgen die reeds zijn opgenomen in artikel 62. Deze bepaling is in de in artikel 69 beschreven gevallen van toepassing en veronderstelt dat wel de inhoud van het gegeven dat wordt verstrekt bekend is. Dat laatste is bij ongeëvalueerde gegevens juist niet het geval.

4. Overige bijzondere bevoegdheden van de diensten

4.1 Het bevorderen of treffen van maatregelen (§4.3 m.v.t.)

De leden van de D66-fractie hebben gevraagd wat voor maatregelen in het kader van het voorgestelde artikel 73 kunnen worden getroffen, hoe de proportionaliteit en subsidiariteit worden gewogen en hoe het vereiste "voor de betrokkene het minste nadeel" concreet toetsbaar zal worden gemaakt. Allereerst merk ik op dat de huidige wet reeds voorziet in het door de diensten inzetten van natuurlijke personen ('agenten') die onder instructie en verantwoordelijkheid van de dienst zijn belast met het bevorderen of treffen van maatregelen ter bescherming van door de diensten te behartigen belangen. Op basis van deze bevoegdheid kunnen de diensten situaties of ontwikkelingen reeds gericht beïnvloeden, bijvoorbeeld door activiteiten van targets, zoals het plegen van een aanslag of het gebruik van fysiek geweld, te ontmoedigen, frustreren of in de kiem te smoren (zie CTIVD-rapport nr. 37 inzake de inzet van enkele langlopende agentenoperaties door de AIVD). Met betrekking tot bijvoorbeeld verstoringsacties in de sfeer van internet kunnen ook reguliere medewerkers van de dienst, niet zijnde agenten, worden ingezet. Vandaar dat wordt voorgesteld om in artikel 73 de mogelijkheid tot het bevorderen of treffen van maatregelen te formuleren als een bevoegdheid die de diensten als zodanig toekomt. De bevoegdheid zal niet louter voor verstoring worden ingezet, maar ook anderszins. Het gaat er bij de toepassing van deze mogelijkheid met name om, indien niet anders kan worden gehandeld en in uitzonderlijke situaties, bepaalde anti-democratische, staatsgevaarlijke activiteiten of andere activiteiten die gericht zijn tegen één van de andere in de wet genoemde belangen te ontmoedigen of in de kiem te smoren met als doel te voorkomen (preventief) dat de met de genoemde activiteiten gepaard gaande risico's worden gerealiseerd. Het nadeel voor de betrokkene zal in de aanvraag tot toestemming dienen te worden beschreven, waarbij vanzelfsprekend ook wordt getoetst aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Zie daartoe het bepaalde in artikel 73, derde lid, van het wetsvoorstel. De toepassing van de hier bedoelde bevoegdheid en de gemaakte afwegingen ter zake kunnen door de CTIVD in het kader van haar toezichthoudende taak worden onderzocht.

[9] Tweede Kamer, vergaderjaar 2016–2017, 26 643, nr. 430

5. Kennisneming van door of ten behoeve van de diensten verwerkte gegevens

De leden van de SGP-fractie vragen zich af of de geheimhouding van bronnen niet kan spelen bij de inzage van gegevens op grond van artikel 76. De geheimhouding van bronnen speelt ook bij de inzage van gegevens op grond van artikel 76. De vergelijkbare uitzondering is opgenomen in artikel 23, aanhef en onder b. Op grond van dit artikel dragen de hoofden van de diensten zorg voor de geheimhouding van daarvoor in aanmerking komende bronnen waaruit gegevens afkomstig zijn.

6. Samenwerking tussen inlichtingen- en veiligheidsdiensten en met andere instanties

6.1 Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen (§6.3 m.v.t.)

De leden van de VVD-fractie vragen de regering of zij helder kan aangeven wat voor informatie er door de diensten met het voorliggende wetsvoorstel straks gedeeld kan worden met andere buitenlandse veiligheidsdiensten. Deze leden vragen de regering aan te geven welke voorwaarden en waarborgen er zijn, en welke stappen doorlopen dienen te worden alvorens data kunnen worden gedeeld met buitenlandse veiligheidsdiensten. Ik verwijs deze leden naar mijn eerdere antwoord op een soortgelijke vraag van de CDA-fractie in paragraaf 3.6.

De leden van de PvdA-fractie vragen zich af of de voorziene wettelijke bepaling om in situaties van acute nood bij uitzondering ook aan niet-bevriende diensten informatie te geven, niet te ruim is opgesteld in verband met het ontbreken van een toets aan de samenwerkingscriteria. Ook de CTIVD heeft in haar zienswijze vergelijkbare zorgen geuit en een voorstel gedaan tot verscherping van de regeling van het verstrekken van (ongeëvalueerde) gegevens. Naar aanleiding van de vragen van deze fractie en het voorstel in de zienswijze van de CTIVD heb ik besloten geen misverstand over deze regel te laten bestaan en deze verder te aan te scherpen. In de gelijktijdig met deze nota naar aanleiding van het verslag uitgebrachte nota van wijziging wordt daarin voorzien. In relatie tot de vragen van de PvdA-fractie betekent een en ander dat bij alle verstrekkingen in het kader van een goede taakuitvoering van de diensten op grond van artikel 62 er getoetst dient te zijn aan de samenwerkingscriteria; voor andere gevallen zal, zowel waar het gaat om de verstrekking van zowel geëvalueerde als ongeëvalueerde gegevens aan een buitenlandse dienst, waarmee geen samenwerkingsrelatie bestaat, de norm van artikel 64 gaan gelden: er dienst sprake te zijn van een dringende en gewichtige reden en voorts moet er toestemming zijn van de voor de dienst verantwoordelijke minister. De CTIVD kan op de toepassing van die bevoegdheid toezien. Aldus is een regeling getroffen voor uitzonderingssituaties die is voorzien van adequate waarborgen. Het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten waarmee geen samenwerkingsrelatie bestaat zal zich overigens slechts in uitzonderlijke situaties voordoen. Hierbij kan worden gedacht aan gegevens van personen die nog niet nader door de diensten zijn beoordeeld, maar waarvan wel bekend is dat deze personen in relatie staan tot een ophanden zijnde aanslag. De dienst zal hierbij een afweging maken tussen het algemeen belang van het voorkomen van de aanslag en het mogelijke individuele nadeel dat kan ontstaan wanneer de gegevens worden gedeeld. Bij een verstrekking van (persoons)gegevens aan een buitenlandse dienst zal ook toepassing dienen te worden gegeven aan het bepaalde in artikel 65 van

het wetsvoorstel; dat betekent in ieder geval de toepassing van de derde-partijregel en indien aan de orde kunnen aan de verstrekking aanvullende voorwaarden worden verbonden. Waar het gaat om het aspect individuele rechtsbescherming: de in de Wiv opgenomen mogelijkheden tot rechtsbescherming voor betrokkene (kennisneming van hem betreffende gegevens, indienen klacht e.d.) zijn gewoon van toepassing. Met betrekking tot de door de PvdA-fractie gestelde vraag wat de verantwoordelijkheid is van de minister in geval van gegevensverstrekking aan diensten waarmee geen samenwerkingsrelatie bestaat, kan het volgende worden opgemerkt. De beslissing om in deze uitzonderingssituatie al dan niet over te gaan tot gegevensverstrekking ligt bij de betrokken minister op een daartoe te verstrekken verzoek van het hoofd van de dienst. De betreffende minister is daarmee betrokken bij het al dan niet verstrekken van de betreffende gegevens.

De leden van de SP-fractie vragen waarom de regering niet de gevaren ziet van het massaal delen van veel privacygevoelige informatie van Nederlanders met andere landen. Zij vragen waarom de regering de veiligheid van de eigen burgers voldoende gewaarborgd vindt, en hoe de regering gaat voorkomen dat door onderlinge uitwisseling van informatie door diensten gegevens van burgers worden 'witgewassen'. Ik verwijs deze leden graag naar mijn eerdere antwoord op vragen van de leden van de CDA-fractie onder 3.6 alsmede naar het antwoord hiervoor naar aanleiding van de vragen van de PvdA-fractie. Indien met de term 'witwassen' gedoeld wordt op de mogelijkheid dat de Nederlandse diensten andere diensten vragen om middelen in te zetten waarover zij zelf niet wettelijk kunnen beschikken, kan ik melden dat de wet daarvoor geen ruimte laat.

De leden van de GroenLinks-fractie vragen de regering waarom zij het noodzakelijk acht dat door de Nederlandse diensten vergaarde 'big data' gedeeld kunnen worden met buitenlandse diensten. Zij vragen of hiermee niet het risico ontstaat dat onbewust wordt meegewerkt aan doeleinden van buitenlandse diensten die tegen de belangen van Nederland of Nederlandse burgers indruisen. Bij de overweging om gegevens te verstrekken aan een buitenlandse dienst wordt tevens overwogen of de door de buitenlandse dienst te behartigen belangen niet onverenigbaar zijn met de belangen die de Nederlandse diensten hebben te behartigen. Dit is ook zo in de wet vastgelegd. De risico's die het delen van ongeëvalueerde gegevens met zich meebrengen dienen voorafgaand aan de toestemming van de minister zoveel mogelijk in kaart worden gebracht. Indien een bepaald risico zich in de praktijk heeft gerealiseerd dan zal dat reden zijn voor de heroverweging van een samenwerking.

De leden van de GroenLinks-fractie vragen of het klopt dat op grond van artikel 89 in combinatie met artikel 48 de mogelijkheid ontstaat om buitenlandse diensten een sleepnetonderzoek (daarvan is geen sprake; de juiste term is onderzoeksopdrachtgerichte interceptie) in Nederland te laten uitvoeren. Deze leden vragen of er een garantie is dat de situatie niet kan ontstaan dat buitenlandse diensten zonder tussenkomst c.q. controle van de diensten communicatie op Nederlands grondgebied aftappen en, zo ja, of de regering dit wenselijk acht. Het is wettelijk niet toegestaan dat zonder tussenkomst van de AIVD/MIVD onderzoeksopdrachtgerichte interceptie van communicatie door buitenlandse diensten op Nederlands grondgebied plaatsvindt. Dat zou immers een inbreuk op de Nederlandse soevereiniteit betekenen. Binnen een bestaand samenwerkingsverband, dat aan de in artikel 88 genoemde factoren is gewogen en door de minister of namens deze door het hoofd van de dienst is

geaccordeerd, kan op grond van artikel 89 door de buitenlandse dienst een verzoek tot technische steunverlening worden gedaan aan de AIVD/MIVD. Een dergelijk verzoek zal niet worden gehonoreerd indien dit verzoek onverenigbaar is met de belangen die de AIVD/MIVD hebben te behartigen (artikel 89, eerste lid, onder a) dan wel in strijd is met een goede taakuitvoering (artikel 89, eerste lid, onder b). Voor zover het betreft de inzet van onderzoeksopdrachtgerichte interceptie door de AIVD/MIVD ten behoeve van een buitenlandse dienst dient daarvoor ministeriële toestemming te worden verkregen met bindend advies van de TIB. Er zitten aldus twee sloten op een dergelijke toestemmingsaanvraag. Tot slot merk ik het volgende op. Het wordt in strijd met een goede taakuitvoering geacht, indien een buitenlandse dienst zou worden toegestaan in Nederland zelfstandig onderzoeksopdrachtgerichte interceptie zou uit te voeren.

6.1.1 Het aangaan en onderhouden van samenwerkingsrelaties met inlichtingen- en veiligheidsdiensten van andere landen (§6.3.2 m.v.t.)

De leden van de D66-fractie vragen waarom wegingsnotities niet al gereed zijn, of gereed kunnen zijn per 1 januari 2018 (een voor deze leden niet geheel onwaarschijnlijke datum van inwerkingtreding). Zij geven voorts aan dat in afwachting van een bevredigend antwoord het lid Verhoeven het amendement over de wegingscriteria (Kamerstukken II 2016/17, 34 588, nr. 16) zal handhaven. De totstandkoming van de wegingsnotities is, zoals door de CTIVD in haar rapport over de invulling van samenwerkingscriteria door de AIVD en MIVD (CTIVD-rapport nr. 48) ook is geconstateerd, een veelomvattend en zeer arbeidsintensief proces. De CTIVD heeft in de afgelopen jaren geleidelijk een kader ontwikkeld, dat met het in 2016 uitgebrachte rapport nr. 48 tot een afronding lijkt te zijn gekomen. Daarmee kunnen de wegingsnoities nu worden vastgesteld. Het gaat hierbij echter om een nauwgezette weging van alle samenwerkingsrelaties aan de geformuleerde criteria. Daarvoor is de genoemde twee jaar benodigd.

Over de inhoud van de wegingsnotitie vragen de leden van de D66-fractie waarom daarin niet mede expliciet een beschrijving van de wettelijke bevoegdheden en technische mogelijkheden van een buitenlandse dienst zijn opgenomen, en het door die dienst geboden niveau van gegevensbescherming. Deze criteria zullen expliciet worden meegenomen in de wegingsnotities. In de gelijktijdig met deze nota naar aanleiding van het verslag uitgebrachte nota van wijziging wordt voorzien in aanvulling van de criteria van artikel 88, derde lid, van het wetsvoorstel.

6.1.2 De verstrekking van gegevens alsmede het verlenen van technische en andere vormen van ondersteuning in samenwerkingsrelaties (§6.3.3 m.v.t.)

De leden van de D66-fractie vernemen graag of het verstrekken van gegevens aan diensten van andere landen waarmee wij samenwerken elke keer opnieuw aan toestemming onderhevig is, of dat de betreffende minister een toestemming kan geven voor meerdere verstrekkingen, en in dat laatste geval, voor hoeveel verstrekkingen uitgedrukt in aantal of tijdsduur. De minister kan toestemming geven voor meerdere verstrekkingen. Zoals in de aanbiedingsbrief bij de CTIVD-rapporten nr. 48 en nr. 49 is opgenomen geldt deze toestemming voor een periode van maximaal één jaar wanneer het de verstrekking van ongeëvalueerde gegevens betreft.

De leden van de D66-fractie stelden een aantal vragen over het verlenen van technische of andere vormen van ondersteuning. Deze leden vragen of getoetst wordt of de desbetreffende dienst zelf bevoegd zou zijn tot het op die wijze – of qua inbreuk op de persoonlijke levenssfeer en andere grondrechten vergelijkbare wijze - verkrijgen van die informatie. Als dat het geval is vragen zij hoe die toets plaatsvindt en als dat niet het geval is vragen zij waarom Nederland meewerkt aan het omzeilen van in andere landen opgenomen waarborgen in de uitoefening van de bevoegdheden door die dienst. Zoals gesteld worden ook de wettelijke bevoegdheden en technische mogelijkheden van een dienst expliciet meegenomen in de wegingsnotitie. Indien wordt vastgesteld dat een buitenlandse dienst bij een verzoek om ondersteuning buiten zijn bevoegdheden treedt, zal daar niet aan worden meegewerkt. Voorts zal dat gevolgen hebben voor de beoordeling van de professionaliteit en betrouwbaarheid van de desbetreffende dienst en dit kan van invloed zijn op de mate en intensiteit van de samenwerking met deze dienst.

De leden van de fractie van de ChristenUnie-fractie hebben gevraagd toe te lichten waarom de regering niet heeft gekozen om het delen van informatie met het buitenland vooraf te laten toetsen. De Toetsingscommissie inzet bevoegdheden (TIB) is ingevolge het wetsvoorstel belast met de toetsing van de rechtmatigheid van de door een betrokken Minister verleende toestemming met betrekking tot een aantal ingrijpende bijzondere bevoegdheden. Bij de verstrekking van gegevens gaat het niet om dergelijke bevoegdheden. Daar komt bij dat het hier gaat om rechtmatig door de diensten verworven gegevens, waarbij in de daarvoor in aanmerking komende gevallen een toets door de TIB heeft plaatsgevonden. Onder omstandigheden kan overigens het aspect van delen van informatie met het buitenland als onderdeel van een toestemmingsverzoek zijn meegewogen, bijvoorbeeld als de interceptie plaatsvindt in het kader van een militaire operatie en er sprake is van een division of effort overeengekomen met de andere coalitiepartijen. Het delen van informatie (met het buitenland) behoort tot de kernactiviteiten van de diensten. Er moet ook voorkomen worden dat een groot deel van het primaire werkproces van de diensten aan een voorafgaande externe toets onderworpen gaat worden. Dat levert een voor de diensten onwerkbare situatie op. Wanneer het gaat om het delen van ongeëvalueerde gegevens die zijn verworven op basis van 48 van onderhavig wetsvoorstel met een buitenlandse dienst zullen extra voorwaarden worden gesteld en zal de CTIVD direct na de verstrekking actief worden geïnformeerd. De voorwaarden kunnen onder meer betrekking hebben op het niet verder delen van de informatie en de te hanteren bewaartermijn.
Daarbij is van belang op te merken dat op de rechtmatigheid van gegevensverstrekking onafhankelijk toezicht wordt uitgeoefend door de CTIVD.

7. Toezicht, klachtbehandeling en behandeling van meldingen van vermoedens van misstanden

De leden van de VVD-fractie vragen hoe de regering tegen de suggestie aankijkt om de zorgplicht ook van toepassing te maken tijdens de analyse van de data. Ik verwijs deze leden graag naar hetgeen ik eerder in antwoord op vragen van de leden van de PvdA-fractie ter zake heb gesteld in paragraaf 1.2.2 van deze nota, waarbij ik voorts heb aangegeven dat bij nota van wijziging de zorgplicht van artikel 24, tweede lid, onder a wordt aangevuld. De voorgestelde aanvulling van de zorgplicht zal naar mijn mening met name ook van betekenis zijn voor de kwaliteit van de gegevensverwerking na de verwervingsfase en biedt de CTIVD aldus ter zake een adequaat toezichtskader. Voorts

verwijs ik deze leden naar mijn antwoord op vragen van de leden van de D66-fractie in paragraaf 3.2.4.

De leden van de PvdA-fractie geven aan dat het wetsvoorstel voorziet in een gecompliceerd systeem van voorafgaande toestemming door de minister, toetsing door de TIB of de rechter en toezicht en klachtbehandeling door de CTIVD. Nu deze partijen zich – ten minste voor een deel – bezig zullen gaan houden met dezelfde rechtsvragen, vragen deze leden hoe de regering denkt om in het belang van een uniforme en consistente rechtstoepassing de TIB en de CTIVD gezamenlijk een taak te geven om de rechtseenheid te bevorderen en hoe dit vormgegeven zou kunnen worden. Een vergelijkbare vraag is eerder gesteld door de leden van de fractie van het CDA. Kortheidshalve verwijs ik naar hetgeen ik antwoord daarop in paragraaf 3.3.2 van deze nota heb gesteld.

De leden van de fractie van de SP-fractie vragen waarom de Nationale ombudsman niet is geconsulteerd over het feit dat de klachtbehandeling wordt ondergebracht bij de CTIVD en niet langer bij de Ombudsman. Daaromtrent kan ik het volgende mededelen. Binnen het kabinet was – gelet op het bijzondere karakter ervan – de afspraak gemaakt dat pas met het concept-wetsvoorstel naar buiten zou kunnen worden getreden na akkoord van de ministerraad. Na het verkregen akkoord is het concept-wetsvoorstel dan ook door mij bij brief van 29 juni 2015 voor een reactie aan de Nationale ombudsman aangeboden. Een eerdere consultatie van de Nationale ombudsman was dan ook niet mogelijk. De Nationale ombudsman is door mij van het voorgaande bij brief van 11 augustus 2015 op de hoogte gesteld. De leden van de fractie van de SP vragen voorts of de regering nader in kan gaan over de onwenselijkheid van de schijn van belangenverstrengeling en partijdigheid. Ik verwijs deze leden graag naar hetgeen ik daaromtrent hieronder in paragraaf 7.1.2 heb gesteld. Waar het gaat om de vraag van deze leden waarom de Ombudsman niet voldoet als klachteninstituut, merk ik het volgende op. Voor zover deze vraag in die zin uitgelegd moet worden waarom de klachtbehandeling zoals in onderhavig wetsvoorstel is uitgewerkt niet is belegd bij de Nationale ombudsman, verwijs ik eveneens naar genoemde paragraaf. Voor het overige moet dat niet gezien worden als een diskwalificatie van de Ombudsman als klachteninstituut. De Ombudsman staat als klachteninstituut immers in hoog aanzien.

7.1 Versterking van het klachtstelsel (§7.3 m.v.t.)

De leden van de fractie van het CDA vragen de regering de keuze voor de CTIVD als klachtinstantie met de bevoegdheid van een bindend oordeel nader te onderbouwen in het licht van de aanbevelingen van de Commissie Dessens. Met name vragen deze leden, waarom de bevoegdheid van de Nationale ombudsman om te oordelen over klachten die betrekking hebben op de AIVD en de MIVD komen te vervallen. Ik wil hierop graag als volgt reageren. De Commissie Dessens heeft in haar advies aanbevolen de behandeling van klachten over de AIVD en MIVD zo veel mogelijk te laten verlopen via de procedure van hoofdstuk 9 van de Algemene wet bestuursrecht (Awb). Dit betekent dat klachten eerst bij de verantwoordelijke minister worden ingediend. Vervolgens – als de klager het niet eens is met de zienswijze van de minister – kan een klacht bij de CTIVD worden ingediend, die – aldus de Commissie Dessens - door de Wiv moet worden aangewezen als een onafhankelijke klachtinstantie in de zin van artikel 9:23, sub m, van de Awb. Als de klager daarna nog de behoefte heeft om een klacht bij de Nationale ombudsman in te dienen, dan is de ombudsman volgens de Awb bevoegd, maar niet

verplicht de behandeling van deze klacht in behandeling te nemen.[10] Overeenkomstig het naar aanleiding hiervan uitgebrachte kabinetsstandpunt, waarin is aangegeven de aanbeveling van de Commissie Dessens om de CTIVD als (zelfstandige) onafhankelijke klachtbehandelaar te positioneren, is de klachtbehandeling aan de CTIVD opgedragen en ondergebracht in een afzonderlijke afdeling; daarbij zijn diverse voorzieningen getroffen teneinde een onpartijdige en onbevooroordeelde klachtbehandeling mogelijk te maken. Wat echter niet is overgenomen is de aanwijzing als onafhankelijke klachtinstantie in de zin van artikel 9:23, sub m, Awb. De reden daarvoor is dat is besloten om de CTIVD de bevoegdheid te geven om jegens de minister bindende oordelen te geven over klachten over het optreden of het vermeende optreden van de diensten.[11] Dit had als consequentie dat aanwijzing als klachtinstantie in de zin van artikel 9:23, sub m, Awb niet meer in de rede lag, met als nevenconsequentie dat daarmee ook de mogelijkheid om een klacht eventueel nog aan de Nationale ombudsman voor te leggen kwam te vervallen. Het alsnog voorzien in een (rest)taak voor de Nationale ombudsman in het klachtstelsel zoals thans in het wetsvoorstel is neergelegd, was echter geen aanleiding meer, nu de bevoegdheden van de afdeling klachtbehandeling van de CTIVD, zowel met betrekking tot de te volgen procedure als met betrekking tot de bindendheid van het oordeel, aanzienlijk verder strekken dan die welke de Nationale ombudsman toekomen. Hieraan voeg ik toe dat de in het wetsvoorstel opgenomen klachtregeling de (potentiële) klager een effectief rechtsmiddel biedt in de zin van artikel 13 EVRM.
De leden van de CDA-fractie vragen voorts hoeveel klachten over de AIVD en de MIVD de Nationale ombudsman jaarlijks behandelt. Het betreft gemiddeld twee klachten per jaar. Ook vragen zij of er problemen zijn geconstateerd ten aanzien van de klachtbehandeling door de Nationale ombudsman, en zo ja, van welke aard waren die? Daarvan is geen sprake.

De leden van de CDA-fractie merken op dat bij de vormgeving van procedures voor klachtbehandeling de bevordering van het vertrouwen van burgers in de overheid leidend moet zijn. Deze leden vragen of de regering de mening deelt dat daarom elke vorm van schijn van partijdigheid bij het afhandelen van deze klachten dient te worden vermeden, en of de regering de mening deelt dat bij klachtbehandeling onafhankelijkheid en onpartijdigheid essentieel zijn, dat zelfs elke schijn van afhankelijkheid en partijdigheid dient te worden vermeden, en dat het onderbrengen van klachtbehandeling bij dezelfde instantie die toezicht houdt, de schijn van partijdigheid heeft? Ik verwijs voor een antwoord hierop naar mijn antwoord op soortgelijke vragen van de PvdA-fractie onder 7.1.2.

De leden van de CDA-fractie vragen verder of het voor de voorgestelde klachtbehandelingskamer van de CTIVD mogelijk is om een onderzoek uit eigen beweging in te stellen, en zo nee waarom niet. Dat is niet het geval. Zoals in paragraaf 7.3.5 van de memorie van toelichting is aangegeven, is daarvan afgezien nu de klachtbehandeling kan leiden tot een bindend oordeel jegens de desbetreffende minister en dit spanning zou opleveren met de bevoegdheid van de afdeling toezicht van de CTIVD om uit eigen beweging een rechtmatigheidsonderzoek te starten, waarbij geen bindende oordelen kunnen worden uitgesproken.

[10] Zie het rapport van de Commissie Dessens: *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, blz. 176.
[11] In paragraaf 9.5 van de memorie van toelichting wordt nader ingegaan op de daaraan ten grondslag liggende overwegingen in het licht van artikel 13 EVRM.

7.1.1 De inrichting en organisatie van de CTIVD (§7.3.2 m.v.t.)

De leden van de D66-fractie vrezen dat de vermelde extra middelen – 1 miljoen euro voor de CTIVD en TIB tezamen – niet toereikend zullen zijn. Deze leden vragen of de regering kan garanderen dat de CTIVD en de TIB toereikende middelen tot hun beschikking hebben voor toezicht (en autorisatie in het geval van de TIB), en op welke wijze de regering inzichtelijk wil maken dat dit bedrag ook daadwerkelijk het benodigde bedrag voor goed toezicht is. Voorts vragen deze leden hoe er zorg voor wordt gedragen dat als door middel van budgetstijging bij de diensten de hoeveelheid te autoriseren en controleren bevoegdheden toeneemt, ook de middelen van de TIB en de CTIVD meegroeien. Op dit moment is een zo goed mogelijke inschatting gemaakt van de benodigde extra capaciteit voor de CTIVD en TIB en het tempo waarin die capaciteit zal moeten toenemen. Op basis hiervan worden aan de CTIVD en de TIB middelen beschikbaar gesteld, zodat beide de aan hen toebedeelde taken kunnen uitvoeren.
Voor de TIB is voorzien in een adequaat secretariaat, waaronder mogelijk ook juristen. Voor de TIB is niet voorzien in een team van onderzoekers. Ik zal monitoren hoe over de jaren de extra toezichts- en autorisatietaken zich ontwikkelen voor CTIVD respectievelijk TIB. Ik wijs er daarbij op dat het totaalbudget van de CTIVD in 2016 reeds met een bedrag van € 0,5 miljoen is opgehoogd naar € 1,62 miljoen. Met de komst van de nieuwe bevoegdheden is in aanvulling hierop €1 mln. op de begroting gereserveerd voor CTIVD en TIB. Om functiescheiding te waarborgen is de verantwoordelijkheid voor het adequaat toerusten van de CTIVD en TIB niet belegd bij de ministers, onder wie de inlichtingen- en veiligheidsdiensten vallen, maar bij de Minister-president. Bij het toezicht door de CTIVD is tot op heden is geen aanleiding gebleken te twijfelen aan het vertrouwen in de diensten dat zij de rechtmatigheid in acht nemen. Ik wijs daarbij op de vele toezichtrapporten, de reacties daarop en uitgevoerde verbeteringen waar dat nodig is. De CTIVD is naar mijn opvatting adequaat uitgerust, zowel qua bevoegdheden als qua middelen. Zoals al aangegeven zal ik scherp monitoren hoe de taakuitvoering verandert als gevolg van de nieuwe wet en daar passend op reageren.

7.1.2 Gevolgen voor de Nationale ombudsman (§7.3.6 m.v.t.)

De leden van de D66-fractie vragen of de regering kan toelichten hoe, gegeven de functiescheiding binnen de CTIVD tussen klacht en toezicht, een even grote onafhankelijkheid van klachtbehandeling gegarandeerd is als wanneer deze taak bij de Nationale ombudsman zou liggen. Naar mijn oordeel zijn in het wetsvoorstel adequate functionele, personele en organisatorische voorzieningen aangebracht die een onafhankelijke klachtbehandeling door de afdeling klachtbehandeling garandeert, juist ook ten opzichte van de afdeling toezicht van de CTIVD (zie paragraaf 7.3.2 van de memorie van toelichting). Deze onafhankelijkheid is naar mijn mening ook vergelijkbaar met behandeling door de Nationale ombudsman, zij het dat ik erken dat de onderbrenging van toezicht en klachtbehandeling in één instantie waar het gaat om de eis van onafhankelijkheid *de schijn* tegen heeft. Het gaat hier echter om een beeld en niet om de feiten; het is dan ook zaak dat beeld effectief bij te stellen. Hier ligt een rol voor de regering, de CTIVD maar naar mijn mening ook voor de Nationale ombudsman. Daarmee kom ik ook op de vraag van deze leden dat de Nationale ombudsman er op zou wijzen dat de burgers mogelijkerwijs niet weten dat zij voor klachten over de AIVD en de MIVD bij de CTIVD moeten zijn. Ik weet niet waar de Nationale ombudsman deze stelling baseert. Ik heb zelf de idee dat de burger de weg naar de CTIVD wel weet te vinden, ook

waar het gaat om klachtbehandeling. In de praktijk komt het nu al voor dat burgers klachten bij de CTIVD indienen, die deze dan ter behandeling doorstuurt naar de voor de desbetreffende dienst verantwoordelijke minister. Ik ben het met de leden van de D66-fractie eens, dat dit overigens een oplosbaar probleem is. Uiteraard ben ik bereid om indien dat nodig wordt geacht hierover het gesprek met de CTIVD en de Nationale ombudsman aan te gaan. Ik ga er overigens van uit dat de Nationale ombudsman ten onrechte bij hem ingediende klachten doorverwijst naar de afdeling klachtbehandeling van de CTIVD en daaromtrent de klager ook informeert. Naar aanleiding van de vraag van deze leden of ook kan worden ingegaan op de vraag hoe volgens de regering in de praktijk een soortgelijke functiescheiding, namelijk die tussen advisering en bestuursrechtspraak, bij de Raad van State uitpakt, merk ik op dat naar mijn mening de functiescheiding bij de Raad van State niet op een lijn is te stellen met functiescheiding bij de CTIVD. Het gaat bij beide organisaties om verschillende sets van taken, enerzijds wetgevingsadvisering en bestuursrechtspraak bij de Raad van State en anderzijds toezicht en klachtbehandeling bij de CTIVD, die ook in een verschillende context moeten worden uitgevoerd.

De leden van de PvdA-fractie lezen dat de klachtbehandeling zoals die nu is belegd bij de Nationale ombudsman, overgaat naar de CTIVD, waarvoor een aparte afdeling zal worden ingericht. De CTIVD krijgt, nu deze ook toezicht op de diensten houdt, daarmee twee taken. Weliswaar is sprake van een strikte scheiding tussen de afdeling toezicht en afdeling klachtbehandeling, maar deze leden kunnen zich toch voorstellen dat tenminste in de ogen van (potentiële) klagers er de schijn van partijdigheid kan bestaan. Ik verwijs deze leden graag naar hetgeen ik hiervoor in reactie op een soortgelijke vraag van de leden van de D66-fractie heb gesteld. De leden van de PvdA-fractie begrijpen – in het licht van de schijn van partijdigheid - vervolgens ook niet waarom het niet toch beter zou zijn als de klachtbehandeling bij de Nationale ombudsman zou blijven. Hierover merk ik het volgende op. In het wetsvoorstel wordt voorzien in een vorm van klachtbehandeling die wezenlijk afwijkt van de reguliere klachtbehandeling, zoals die in hoofdstuk 9 van de Algemene wet bestuursrecht is vormgegeven. Weliswaar blijft de procedure voor de interne behandeling van klachten omtrent het (vermeende) optreden van de diensten onverkort van kracht, maar het vervolg, de externe klachtbehandeling, krijgt een geheel ander karakter dan normaliter voor klachtprocedures geldt; dat in het wetsvoorstel een groot deel van de processuele regels voor de behandeling van klachten door externe klachtinstanties is overgenomen, doet daar niet aan af. Klachtprocedures resulteren in een niet bindend oordeel; dat geldt ook voor de oordelen van de Nationale ombudsman. De oordelen van de afdeling klachtbehandeling bij de CTIVD krijgen echter een volstrekt ander – in wezen een semi-rechterlijk - karakter, namelijk zij zijn wel bindend. Het gaat derhalve om een vergaande afwijking van het reguliere stelsel. Het onderbrengen van deze vorm van (bindende) klachtbehandeling bij de Nationale ombudsman is dan ook niet onproblematisch en kan bij (potentiële) klagers bij de Nationale ombudsman de vraag oproepen waarom de ene categorie klachten wel en de andere categorie klachten niet tot een bindend oordeel leiden. De positionering bij de CTIVD is dan ook alleszins te prefereren.

8. Geheimhouding

De fracties hebben hierover geen vragen en opmerkingen.

9. Grondrechtelijke en mensenrechtelijke aspecten

De leden van de CDA-fractie vragen hoe de bewaartermijn van drie jaar van door middels van onderzoeksopdrachtgerichte interceptie verkregen gegevens zich verhoudt tot de eis van proportionaliteit en op basis van welke objectieve criteria de bewaartermijn voor de inhoud van de communicatie niet bekort kan worden en waarom deze strikt noodzakelijk is. Ik wil deze leden verwijzen naar hetgeen ik eerder in antwoord op vragen van de leden van de fractie van de VVD over de bewaartermijn van drie jaar heb gesteld; zie daartoe paragraaf 3.3.3.3.5.1 van deze nota.

De leden van de CDA-fractie vragen de regering om te reflecteren op het feit dat landen als het Verenigd Koninkrijk en Duitsland geen wettelijke bewaartermijnen kennen, maar dat de in die landen op grond van jurisprudentie toegepaste bewaartermijn aanzienlijk korter is dan de in het voorliggende wetsvoorstel opgenomen termijn. Ik kan hier niet anders op reageren door te stellen dat ieder land hier zijn eigen afwegingen in dient te maken, waarbij men ook rekening zal dienen te houden met de voor hen relevante jurisprudentie. De Nederlandse regering heeft op basis van een eigen afweging gekozen voor een termijn van drie jaar waar het gaat om gegevens die verkregen zijn door onderzoeksopdrachtgerichte interceptie en acht die bewaartermijn verdedigbaar.

De leden van de CDA-fractie vragen tevens of de regering kan reageren op de suggestie van de CTIVD om onderscheid te maken tussen de bewaartermijn voor metadata en voor de inhoud van gegevens. Door middel van metadata wordt inzicht gegeven in netwerken en onderlinge verbanden. De inhoud van de communicatie draagt vervolgens bij aan een actueel en concreet beeld en verschaft daarmee handelingsperspectief. Beide componenten dragen bij aan het verkrijgen van een hoogwaardige inlichtingenpositie en zijn onlosmakelijk met elkaar verbonden. Het hanteren van eenzelfde bewaartermijn past in deze systematiek. Ik zie derhalve geen aanleiding om een onderscheid te maken, zoals door de CTIVD wordt gesuggereerd.

10. Overzicht wetgeving in enkele andere landen

De leden van de SP-fractie vragen of de regering kan aangeven hoeveel terroristische aanslagen voorkomen zijn door de verzameling van bulkdata in de omringende landen. Deze leden vraag of de regering ook kan ingaan op de situatie in de Verenigde Staten, waar de FBI stelt dat de verzameling van grote hoeveelheden data niet heeft geleid tot opheldering van grote zaken. Zij vragen waarom massale inbreuk op de privacy en grondrechten van Nederlanders dan nog gerechtvaardigd is.
Ik heb geen informatie over de hoeveelheid terroristische aanslagen die zijn voorkomen in andere landen, noch op grond van welke informatie deze aanslagen zijn voorkomen. Ik ben niet bekend met de hier aan de FBI toegeschreven uitspraak. Ik weet wel dat een soortgelijke uitspraak is gedaan met betrekking tot de Patriot Act. Deze wet is naar mijn oordeel onvergelijkbaar met het voorliggende wetsvoorstel. Zoals ook in hoofdstuk 1 van de memorie van toelichting is aangegeven, gaf het Verenigd Koninkrijk in 2015 aan dat de analyse van gegevens verkregen door onderzoeksopdrachtgerichte interceptie een significante rol speelde in elk belangrijk onderzoek met betrekking tot contraterrorisme in de voorgaande tien jaar. Daaronder ook de zeven terroristische aanslagen die sinds november 2014 werden voorkomen. 95% van de cyberaanvallen die in een periode van zes maanden waren gedetecteerd door de inlichtingen- en veiligheidsdiensten konden alleen worden ontdekt door inzet van onderzoeksopdrachtgerichte interceptie. Daaronder zaten talloze aanvallen op alle belangrijke bedrijfssectoren en op overheidsnetwerken. In

een toenemend aantal gevallen verkrijgen de Nederlandse inlichtingen- en veiligheidsdiensten informatie van hun partnerdiensten over directe dreiging voor Nederland, die zij vanwege de beperkte bevoegdheden zelf niet konden onderkennen. Onze diensten lopen dan soms achter de feiten aan: het kwaad, zoals het stelen van intellectueel eigendom, is reeds geschied. Overigens is geen enkele bijzondere bevoegdheid op zichzelf een garantie tegen aanslagen, dit geldt eveneens voor onderzoeksopdrachtgerichte interceptie. De inlichtingen- en veiligheidsdiensten zetten in verreweg de meeste onderzoeken een mix van inlichtingenmiddelen in, die juist in combinatie met elkaar een bijdrage leveren aan de te behalen doelstellingen. Zoals ik meermalen heb aangegeven, betekent dit wetsvoorstel geen massale inbreuk op de privacy en grondrechten van Nederlanders.

De leden van de fractie van D66 constateren terecht dat veel Europese landen hun diensten ruimere bevoegdheden of minder toezicht toekennen bij de inzet van bevoegdheden in het buitenland en vragen de regering of deze kan toelichten welke bevoegdheden de diensten die zijn opgenomen in de memorie van toelichting kunnen uitoefenen in Nederland. Ook vragen zij de regering of de bevoegdheden van deze diensten naar aanleiding van de Snowden-onthullingen over het algemeen zijn ingeperkt of juist uitgebreid. In de memorie van toelichting wordt in hoofdstuk 10 in algemene zin uitgewerkt welke bevoegdheden de Duitse, de Franse, de Belgische en de Britse inlichtingen- en veiligheidsdiensten in het buitenland kunnen inzetten. In de onderzochte wetgeving werd voor wat betreft de inzet van verschillende bijzondere bevoegdheden geen onderscheid gemaakt tussen bevoegdheden die wel of niet in het buitenland kunnen worden ingezet. Het is mij niet bekend of een dergelijk onderscheid elders mogelijk nog op andere wijze is vastgelegd. In de periode na de Snowden-onthullingen hebben de wetgevers in Duitsland, het Verenigd Koninkrijk, Frankrijk en België de nationale wetgeving die de inzet van bijzondere bevoegdheden in het licht van fundamentele rechten en vrijheden normeert, herzien. Deze herzieningen, die voor het leeuwendeel een nadere versteviging van het toezicht en niet zozeer een inperking van de bevoegdheden behelsden, werden mede veroorzaakt door grotendeels publieke en politieke discussies over de bevoegdheden van de inlichtingen- en veiligheidsdiensten als gevolg van de genoemde onthullingen. Voor de details hierbij wordt wederom verwezen naar hoofdstuk 10 van de toelichting.

De leden van de D66-fractie vragen of de regering kennis heeft genomen van het boek ‘Global Intelligence Oversight. Governing Security in the Twenty-First Century (Goldman en Roscoff (uitg.), 2016). In dit boek komt, aldus deze leden, naar voren dat *best practices* elkaar kunnen versterken, maar ook dat *worst practices* elkaar kunnen versterken. Deze leden vragen zich af hoe het Nederlandse wetsvoorstel er aan kan bijdragen dat de Nederlandse diensten hun buitenlandse collega’s ten positieve kunnen beïnvloeden ten aanzien van fundamentele rechten en vrijheden bij de uitoefening van hun taken en bevoegdheden. De regering heeft ten behoeve van de beschrijving van de rechtsstelsels kennis genomen van enkele vergelijkende onderzoeken en van de wetgeving met betrekking tot de inlichtingen- en veiligheidsdiensten in Duitsland, Frankrijk, België en het Verenigd Koninkrijk. Daarbij is het door de leden van de D66-fractie genoemde boek, dat overigens na het schrijven van de toelichting is uitgekomen, niet betrokken. Omdat het voorliggende wetsvoorstel voorziet in versteviging van effectieve waarborgen waaronder een versterkt toezichtmechanisme in elke fase waarin de bijzondere bevoegdheden kunnen worden ingezet, ga ik er vanuit dat de nieuwe wetgeving naar andere landen in verschillende opzichten een voorbeeldfunctie kan

vervullen. Zo is in het ontwerp van het toezicht uitdrukkelijk rekening gehouden met de eisen die het EVRM op dit punt stelt. De inrichting van de inlichtingen- en veiligheidsdiensten en de regeling van de bijzondere bevoegdheden van de inlichtingendiensten in Europa en in de wereld vertoont weliswaar een gedifferentieerd beeld, maar de maatstaven van het EVRM zijn voor alle partijen bij het verdrag, waaronder Nederland, kaderstellend. Daarnaast kan bijzondere aandacht worden gevestigd op het feit dat de waarborgen die de Nederlandse wetgeving vastlegt altijd gelden - in vergelijking met Duitsland, Frankrijk en het Verenigd Koninkrijk en België - ongeacht of de bijzondere bevoegdheid wordt ingezet ten aanzien van het nationale of het internationale communicatieverkeer.

10.1 Duitsland (§10.2 m.v.t.)

De leden van de D66-fractie vragen de regering om toe te lichten op welke vlakken de recente aanscherping van de wetgeving omtrent de diensten is veranderd. Ik neem aan dat deze leden daarbij met name doelen op de wijziging van de Bundesnachrichtendienstgesetz (BNDG). Daaromtrent kan ik, voor zover ik het kan overzien, het volgende melden. De uitoefening van de taken van de Duitse Buitenlandse Veiligheidsdienst (BND) wordt voortaan achteraf gecontroleerd door een onafhankelijk rechterlijk comité. Bovendien zal het onderzoeken van EU-burgers of EU-instellingen alleen nog mogelijk zijn om de 'handelingsbekwaamheid van de Bondsrepubliek te waarborgen'. Voor Duitsers geldt hier het criterium van 'concreet gevaar', zoals bijvoorbeeld terrorisme. Dat staat in een wetsvoorstel waarmee de Bondsregering heeft ingestemd en dat nu naar de Bondsdag gaat. Het wetsvoorstel moet tegemoet komen aan de binnenlandse kritiek dat er onvoldoende toezicht op de BND is. Het rechterlijke gremium zal bestaan uit twee rechters en een advocaat-generaal van het Bundesgerichtshof (en drie plaatsvervangers). Het comité moet elk zoekwoord kunnen toetsen, waarop de BND in telecommunicatie naar informatie zoekt. Ook is een aantal zaken waaraan de BND zich moet houden nu ook uitdrukkelijk in de wet vastgelegd: zo is het inwinnen van data van Duitsers, Duitse bedrijven of van in Duitsland verblijvende personen, niet toegestaan (BND is immers de buitenlandse veiligheidsdienst). De wet regelt ook de samenwerking met buitenlandse geheime diensten. Zo moet de samenwerking in het licht van 'zwaarwegende buitenlandse- en veiligheidsbelangen' noodzakelijk zijn. Ook mag alleen met die staten worden samengewerkt, waar de 'principes van de rechtsstaat gewaarborgd zijn'. Onder deze voorwaarden is het voortaan mogelijk ook gemeenschappelijke databanken met andere diensten op te zetten.

Ook vragen deze leden waarom de regering niet voor dezelfde motiveringscriteria heeft gekozen als die Duitse diensten dienen te gebruiken bij een verzoek tot bulkinterceptie. Ik wil daar in algemene zin eerst het volgende over stellen, ook om de waarde van rechtsvergelijking in deze enigszins te relativeren. Als ik de verschillende stelsels van een aantal landen overzie, zoals ook beschreven in de memorie van toelichting, constateer ik dat er geen één hetzelfde is. Dat is ook niet zo vreemd, omdat elk land – binnen de grenzen die het EVRM laat – op zijn eigen wijze invulling geeft aan de inrichting van de werkzaamheden van diens inlichtingen- en veiligheidsdiensten. Dat blijkt uit de verschillen in de taakstelling en de bevoegdheden van de diensten, de daarbij in acht te nemen waarborgen, de inrichting van het toezichtstelsel enz. Bij die nationale keuzes, dat geldt ook voor Nederland, spelen culturele en politieke aspecten een rol, maar bijvoorbeeld ook kunnen uitspraken van (inter)nationale rechters sturing geven aan de wijze waarop daaraan invulling moet worden gegeven. De Nederlandse

wetgever maakt hierin ook zijn eigen keuze. Als ik vervolgens naar de genoemde criteria kijk dan constateer ik dat als het gaat om wat, waar en hoe lang – zij het op een ander abstractieniveau – dit ook zaken zijn die in een verzoek om toestemming tot onderzoeksopdrachtgerichte interceptie zullen terugkomen. Waar het gaat om het criterium 'hoeveel' stel ik vast dat we dat in Nederland niet hanteren. In Duitsland heeft de wetgever het blijkbaar wenselijk geacht om ook in dit opzicht de bevoegdheid van de BND te normeren.

10.2 Vergelijkende observaties (§10.6 m.v.t.)

De leden van de VVD-fractie vragen of omringende landen gebruik mogen maken van kabelinterceptie, en zo ja hoe het toezicht daarop is geregeld en hoe zich dit verhoudt tot het voorliggende wetsvoorstel. In hoofdstuk 10 van de MvT is een wetsvergelijking opgenomen teneinde de keuzes die in het kader van de herziening van de Wiv zijn gemaakt in een bredere Europese context te plaatsen. De focus in deze wetsvergelijking ligt op Duitsland, het Verenigd Koninklijk, België en Frankrijk. De onderzochte landen beschikken alle over de wettelijke bevoegdheid gegevens in bulk via de kabel te intercepteren. De wijze waarop de bevoegdheden en de waarborgen in de verschillende landen zijn vastgelegd laat een divers beeld zien. Dat geldt ook voor het toezicht daarop. Voor een specificering hiervan verwijs ik naar hoofdstuk 10 van de MvT en bijlage 5, waarin dit per onderzocht land is uitgewerkt. Ik verwijs verder naar hetgeen ik hiervoor in paragraaf 10.1 in reactie op vragen van de leden van de D66-fractie heb gesteld, waar het gaat om de (waarde van de) vergelijking van de diverse beschreven stelsels.

11. Financiële gevolgen voor het Rijk en het bedrijfsleven

De leden van de SP-fractie vragen of de regering kan garanderen dat de vrijgemaakte €21 miljoen voldoende is om zowel het uitgebreide toezicht als de noodzakelijke toename in fte's te financieren, en of dit niet ten koste zal gaan van de inzet van het huidige personeel en de capaciteiten van de diensten. Het wetsvoorstel laat voor een groot deel de bestaande praktijk bij de diensten ongewijzigd. Ten aanzien van het uitgebreide toezicht en de toepassing van de kabelbevoegdheid is €20 miljoen structureel toegekend; niet €21 miljoen, zoals deze leden in hun vraagstelling hebben opgenomen . Ik beschouw dit bedrag als kaderstellend voor implementatie en toepassing van de uitoefening van de bevoegdheid (inclusief de vergoeding van de kosten die door het bedrijfsleven worden gemaakt). De betrokken departementen zullen de mate waarin van deze bevoegdheid gebruik wordt gemaakt, de opbrengsten ervan voor de taakuitoefening van de diensten en de hiermee samenhangende kosten, jaarlijks evalueren en betrekken bij het bepalen van het ambitieniveau.

De leden van de CDA-fractie geven aan het met de regering eens te zijn, dat voor de groep aanbieders van communicatiediensten – anders dan de traditionele aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten - niet redelijk is te verwachten dat deze vooraf reeds organisatorische en technische maatregelen worden getroffen om interceptie te kunnen faciliteren. Zij vragen in dit verband of hun conclusie juist is, dat alleen een concreet verzoek om interceptie voor de bedoelde aanbieders kosten met zich meebrengt. De conclusie van deze leden is juist. Anders dan de aanbieders waarop de regeling van hoofdstuk 13 Telecommunicatiewet van toepassing is, hoeven deze aanbieders niet op voorhand aftapbaar te zijn en daarvoor de te maken kosten zelf te dragen.

De leden van de D66-fractie constateren dat veel bedrijven zorgen hebben over het digitale vestigingsklimaat van Nederland en dat de regering verzuimd heeft de economische gevolgen van dit wetsvoorstel te onderzoeken. Deze leden vragen of de regering bereid is het Centraal Planbureau (CPB) onderzoek te laten doen naar het effect van voorliggend wetsvoorstel op het vestigingsklimaat en het concurrentievermogen van Nederland, waarbij specifiek gekeken wordt naar mogelijk verlies van banen, gevolgen voor innovatie in ICT-infrastructuur, misgelopen investeringen (in bijvoorbeeld datacenters), te maken kosten door Nederlandse bedrijven en de economische gevolgen van de handel in en het in stand houden en gebruiken van software kwetsbaarheden, al dan niet door middel van ingekochte hacksoftware. Zij vragen ook of de regering van mening is dat dergelijk onderzoek bijdraagt aan een zorgvuldige afweging van alle verschillende belangen (privacy, economisch, veiligheid) die geraakt worden door dit wetsvoorstel.
Teneinde de impact op het bedrijfsleven te kunnen inschatten en de belangen tussen privacy, economie en veiligheid te kunnen wegen heeft de regering een Bedrijfseffectentoets (BET) uitgevoerd. Hieruit komt naar voren dat de impact op het bedrijfsleven zeer beperkt zal zijn. Aangezien de BET het instrument is om bij nieuwe en wijzigende regelgeving in kaart te brengen wat de gevolgen voor het bedrijfsleven kunnen zijn acht ik een aanvullend onderzoek door het CPB overbodig.

De leden van de ChristenUnie-fractie vragen naar de middelen die beschikbar komen voor toezicht. Zij vragen of de regering de budgettaire effecten voor het toezicht nader kan onderbouwen en kan aangeven waarom zij meent dat daarmee effectief toezicht mogelijk is. Deze leden vragen of de regering bereid is de Algemene Rekenkamer te vragen een toets te doen op het noodzakelijk budget voor effectief toezicht op deze wet. Ik verwijs deze leden naar mijn eerdere antwoord op soortgelijke vragen van de D66-fractie in paragraaf 7.1.1 van deze nota. In aanvulling daarop, merk ik op, dat nu de overweging ten aanzien van het noodzakelijke budget voor effectief toezicht afdoende is meegenomen, ik een onderzoek door de Algemene Rekenkamer als door deze leden wordt voorgesteld overbodig acht.

De leden van de GroenLinks-fractie verzoeken de regering om inzicht te geven in het technisch onderzoek en ervaringsgegevens waarop de budgetverhoging van € 20 miljoen structureel is gebaseerd, voorzien van een uitsplitsing van de opbouw van de geraamde kosten. Het technisch onderzoek en de ervaringsgegevens die ten grondslag liggen aan de raming, geven inzicht in de werkwijze en capaciteiten van de AIVD en MIVD en zijn deels ook gebaseerd op informatie van buitenlandse partnerdiensten. Deze gegevens kunnen derhalve niet aan de Kamer worden verstrekt. De genoemde € 20 miljoen (waarvan € 1 miljoen bestemd is voor versterking van de TIB en de CTIVD) is kaderstellend voor implementatie en toepassing van de bevoegdheid. Het bedrag is opgebouwd uit enkele hoofdbestanddelen, namelijk vergoedingen naar redelijkheid aan de sector voor investerings-, personeels- en administratiekosten die direct samenhangen met de uitvoering van de bevoegdheid, en personeels- en materieelkosten bij AIVD en MIVD. Bij personeelskosten gaat het met name om het aantrekken van gespecialiseerd (technisch) personeel. Bij de materieelkosten gaat het onder andere om het inrichten van zogenaamde ‘access-locaties’, de technische voorzieningen bij aanbieders om interceptie te realiseren. De regering zal in 2017 één access-locatie gereedmaken voor onderzoeksopdrachtgerichte interceptie. Het dreigingsbeeld is daarbij bepalend: bezien wordt op welk punt van de Nederlandse infrastructuur zal moeten worden aangehaakt

om de noodzakelijke data te kunnen intercepteren. Dit gebeurt in goed overleg met de telecommunicatiesector. De kosten van het betreffende bedrijf worden vergoed. In de periode daarna wil de regering jaarlijks, in ieder geval tot 2020, uitbreiden met één access-locatie. De betrokken departementen zullen de mate waarin van onderzoeksopdrachtgerichte interceptie gebruik wordt gemaakt, de opbrengsten ervan voor de taakuitoefening van de diensten en de hiermee samenhangende kosten, jaarlijks evalueren en betrekken bij het bepalen van het ambitieniveau.

De leden van de GroenLinks-fractie vragen of de regering de financiële impact van het wetsvoorstel wil laten onderzoeken door een onafhankelijke partij. Bij het wetsvoorstel is een Bedrijfseffecten Toets (BET) uitgevoerd. Hieruit komt naar voren dat de impact op het bedrijfsleven zeer beperkt zal zijn. Ik zie derhalve geen aanleiding om de financiële impact nader te laten onderzoeken door een onafhankelijke partij.

12. Consultatie, privacy impact assessment en notificatie

De leden van de fractie van het CDA vragen, in verband met het regime voor opslag van gegevens, op welke wijze de regering garandeert dat de opslag van gegevens op servers of in de cloud ten alle tijden onder Nederlandse wetgeving geborgd is. Het is mij niet geheel duidelijk op welke situatie deze leden doelen. Ik kan wel opmerken dat onderhavig wetsvoorstel geen regels stelt over de opslag van gegevens op servers in de cloud en dus ook niet dat dat onder Nederlandse wetgeving is geborgd.

12.1 Consultatie (§12.2 m.v.t.)

12.1.1 Het nieuwe interceptiestelsel (§12.2.2 m.v.t.)

De leden van de VVD-fractie vragen of de regering kan toelichten waarom er met het voorliggende wetsvoorstel geen sprake is van sleepnet(bevoegdheid). Ik merk allereerst op dat het begrip ‘sleepnet’ geen term is die in de wet voorkomt. Indien met de term ‘sleepnet’ wordt beoogd te suggereren dat zonder een vooraf bepaald doel en zonder onderscheid data wordt vergaard, neem ik er krachtig afstand van. De inzet van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie geschiedt altijd voor een gespecificeerd doel. Onderzoeksopdrachtgerichte interceptie maakt het mogelijk om, indien dat in verhouding staat tot de dreiging en indien de inzet van lichtere middelen niet mogelijk is, specifieke datastromen te onderscheppen die passen binnen de onderzoeksopdrachten van de diensten. Daarbij geldt het uitgangspunt dat van deze datastroom uiteindelijk slechts de data wordt gebruikt die noodzakelijk is voor de taakuitvoering. Kortom, de diensten mogen geen ‘sleepnet’ uitgooien.

De leden van de VVD-fractie vragen welke garanties er zijn om zeker te stellen aan buitenlandse bedrijven dat het opslaan van data in Nederland 100% veilig kan. Het internet brengt ons veel maar maakt ons ook kwetsbaar: vitale sectoren als energie en luchtvaart, telecombedrijven, havens maar ook het regulier bedrijfsleven, het MKB en overheidsorganisaties worden digitaal aangevallen. In het Cybersecuritybeeld Nederland 2015 is aangegeven dat de AIVD en de MIVD meerdere digitale spionageaanvallen hebben onderkend, die tal van Nederlandse bedrijven als doelwit hadden. Ook is sprake van de heimelijke verkenningen van systemen binnen de vitale infrastructuur en de overheid. Een deel van deze aanvallen is afkomstig van buitenlandse inlichtingendiensten. Een 100% garantie dat data in Nederland veilig is valt dan ook helaas niet te geven. Wel kan worden gesteld dat met de totstandkoming van de nieuwe

Wiv de inlichtingen- en veiligheidsdiensten adequate instrumenten in handen krijgen om in het cyberdomein weerwerk te bieden tegen digitale aanvallen.

12.1.2 Capita selecta (§12.2.7 m.v.t.)

De leden van de fractie van de PvdA vragen waarom de overweging dat de beroepsgroepen advocaten en journalisten een belangrijke rol in de borging van belangrijke aspecten van de democratische rechtsstaat spelen en in verband daarmee aan het gebruik van bevoegdheden jegens hen voorafgaande toestemming van de rechter is vereist, niet geldt voor andere verschoningsgerechtigden zoals notarissen. Deze leden verwijs ik graag naar hetgeen ik eerder in reactie op een vergelijkbare vragen van de leden van de SP-fractie en de leden van de fractie van D66 heb geantwoord. De leden van de fractie van de PvdA vroegen zich in dit verband af of de bronbescherming wel afdoende wordt geregeld. Wat is, aldus deze leden, de meerwaarde van het desbetreffende afzonderlijke wetsvoorstel tot bronbescherming in geval van de diensten, indien die diensten via de bulkverzameling toch al gegevens in handen hebben gekregen. Waarom hoeven de gegevens over de vertrouwelijke communicatie tussen een journalist en zijn bron, in tegenstelling tot de advocaat en de cliënt, niet vernietigd te worden als deze zijn vergaard zonder tussenkomst van de rechter? Voor de beantwoording van deze vraag verwijs ik naar mijn eerdere antwoord op een soortgelijke vraag van de leden van ChristenUnie-fractie.

De leden van de PvdA-fractie vragen zich voorts af of beveiligde journalistieke omgevingen niet dezelfde bescherming zouden moeten hebben als de journalisten zelf, waarbij bijvoorbeeld de medewerkingsplicht tot ontsleuteling niet voor beveiligde journalistieke omgevingen zoals Publeaks zou moeten gelden. Ik merk naar aanleiding hiervan allereerst op, dat niemand van een mogelijk onderzoek door de Nederlandse inlichtingen- en veiligheidsdiensten is uitgezonderd: dat geldt voor journalisten, maar evenzeer voor de journalistieke omgeving waarin men werkt. Indien het belang van de nationale veiligheid dat vergt, moet ook daar onderzoek mogelijk zijn. Echter een dergelijk onderzoek moet dan wel voorzien zijn van noodzakelijke waarborgen, mede vanwege het feit dat het hier om journalisten gaat en van (de mogelijkheid van) een dergelijk onderzoek een zeker chilling effect uit kan gaan. Achter een journalistieke omgeving gaan journalisten schuil, dus een onderzoek naar een journalistieke omgeving betekent naar mijn mening dat vrijwel per definitie de mogelijkheid aanwezig is dat daar kennis wordt genomen van gegevens waardoor zicht op de bron van de journalist ontstaat. De inzet van een bijzondere bevoegdheid op een journalist die daaraan participeert is, zoals bekend, ingevolge artikel 30, tweede lid, van het wetsvoorstel onderworpen aan toestemming van de rechtbank Den Haag. Waar het gaat om de plicht om mee te werken aan de ontsleuteling van gegevens, geldt ook hier dat de hiervoor geformuleerde hoofdregel van toepassing is. Het gaat dan om de opdracht om mee te werken aan de ontsleuteling van gegevens die reeds in bezit zijn van de diensten. Voor zover de medewerking wordt ingeroepen van journalisten, waarbij die medewerking kan leiden tot verwerving van gegevens inzake de bron van de journalist, dan geld ook hier dat eerst de toestemming van de rechtbank Den Haag dient te worden verkregen. Toestemming van de minister in deze gevallen volstaat dus niet; dat volgt uit de tekst van artikel 30, tweede lid, van het wetsvoorstel. De medewerkingsplicht tot ontsleuteling staat niet toe dat men de opdracht zou kunnen krijgen om de beveiligde journalistieke omgeving als zodanig via het aanbrengen van voorzieningen in ontsleutelde vorm toegankelijk te maken voor inlichtingen- en veiligheidsdiensten. Tot slot vragen de leden

van de PvdA-fractie wat mijn mening is over het chilling effect – in concreto dat bij gebrek aan een goede bronbescherming bronnen er van af zullen zien om contact op te nemen met journalisten - dat op kan treden bij grootschalige verzameling, opslag en analyse van gegevens door de inlichtingen- en veiligheidsdiensten. Ik ben van mening dat de invulling van bronbescherming adequaat is en in lijn met de jurisprudentie van het EHRM.

12.2 Privacy Impact Assesment (PIA) (§12.3 m.v.t.)

De leden van de D66-fractie verwijzen naar uitspraken over privacy door de directeur-generaal van de AIVD in de Volkskrant in september 2016, en vragen de regering hierop te reageren, ook in relatie tot het gegeven dat in de PIA duidelijk naar voren komt dat de privacy-risico's op behoorlijk veel onderdelen van het voorliggende wetsvoorstel onvoldoende worden onderkend en waarborgen ontbreken om die risico's voldoende af te dekken. Ik verwijs naar mijn eerdere antwoord over de uitspraken van de directeur-generaal van de AIVD op vragen van de D66-fractie onder 3.3.3.3.5.4.

De leden van de D66-fractie vragen of expliciet kan worden toegelicht hoe het wetsvoorstel zich verhoudt tot de op 21 december 2016 gepubliceerde uitspraak van het Hof van Justitie over dataretentie. Allereerst merk ik op dat in artikel 4, tweede lid, van het EU-verdrag is vastgelegd dat de EU essentiële staatsfuncties eerbiedigt, waaronder de nationale veiligheid. De nationale veiligheid blijft een uitsluitende verantwoordelijkheid van elke lidstaat. Daar kan de EU dus niet in treden. De uitspraak inzake dataretentie heeft dan ook geen gevolgen voor hetgeen in onderhavig wetsvoorstel is geregeld. De gevolgen van de uitspraak voor het bij de Tweede Kamer aanhangige wetsvoorstel bewaarplicht zullen door de minister van VenJ in kaart wordt gebracht. Dat is echter een wetstraject dat geheel los staat van de herziening van de Wiv 2002. Ten overvloede wordt opgemerkt dat het wetsvoorstel – evenals de huidige wet - ook geen bewaarplicht (of plicht tot dataretentie) voor aanbieders van communicatiediensten kent.

De leden van de D66-fractie brengen in herinnering dat zij reeds eerder hebben gepleit voor een extra privacystoel bij de CTIVD, zodat die deskundigheid ook in het toezicht is geborgd. Zij vroegen waarom daaraan geen uitvoering wordt gegeven. Ik zie voor een dergelijke extra privacystoel bij de CTIVD geen aanleiding. Met dit voorstel wordt naar mijn mening miskend dat de CTIVD meer dan voldoende kennis en expertise op het vlak van privacy in eigen huis heeft. De CTIVD houdt immers toezicht op de rechtmatige uitoefening van de Wiv 2002 en de Wet veiligheidsonderzoeken, waarbij bij voortduring privacyvraagstukken aan de orde zijn. De door de CTIVD uitgebrachte rapporten geven daarvan blijk.

De leden van de fractie van D66 wijzen op de reactie die door de Autoriteit Persoonsgegevens is uitgebracht, waarin deze stelt dat de (nieuwe) bevoegdheden van de diensten onmiskenbaar gevolgen hebben voor de Nederlandse burgers, en in het bijzonder voor het recht op bescherming van de persoonlijke levenssfeer. Deze leden vragen of, in aanvulling op de analyse in de memorie van toelichting van de uitspraak van het EHRM in de zaak Weber en Saravia t. Duitsland, de regering kan reageren op de waarschuwing van het EHRM in diens uitspraak dat "a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it" (par. 106) en op welke wijze zij meent dat deze waarschuwing niet

aan dovemansoren is gericht van het voorliggende verstrekkende wetsvoorstel? Bij de voorbereiding van het wetsvoorstel is van meet af aan uitvoerig aandacht besteed aan zowel de grondrechtelijke als de mensenrechtelijke (EVRM) eisen die bij het vormgeven van een nieuw wettelijk kader van de activiteiten van de Nederlandse inlichtingen- en veiligheidsdiensten dienen te worden gesteld. Daarvan is specifiek in hoofdstuk 9 van de memorie van toelichting uitvoerig – en onder verwijzing naar relevante jurisprudentie - rekenschap afgelegd, maar ook in de toelichting op diverse andere onderdelen van het wetsvoorstel is daarop ingegaan. In het wetsvoorstel is niet alleen voorzien in een stringent kader voor de uitoefening van bevoegdheden door de diensten en de verdere verwerking van de aldus door hen verworven gegevens, maar ook in een robuust stelsel van toezicht. Dit geheel vormt naar mijn mening, tezamen met andere waarborgen, waaronder niet in het minst het systeem van parlementaire controle, de garantie dat de notie die in de geciteerde frase uit de uitspaak van het EHRM tot uitdrukking is gebracht, niet de kans krijgt om bewaarheid te worden. Tot slot vragen de hier aan het woord zijnde leden, of de regering bereid is in te gaan op alle punten die de Autoriteit Persoonsgegevens in diens reactie voor het rondetafelgesprek met de Tweede Kamer naar voren brengt over het wetsvoorstel. Ik heb met belangstelling kennis genomen van de reactie van de Autoriteit en stel vast dat een deel van de door haar aangesneden punten min of meer– zij het soms in wat andere bewoordingen - terug komen in de vragen die door de leden van de verschillende fracties die een bijdrage aan het verslag hebben geleverd, zijn gesteld. Ik beperk mijn reactie dan ook tot die onderdelen die nog niet eerder als zodanig aan de orde zijn gesteld. De Autoriteit Persoonsgegevens stelt in paragraaf 3.1 van haar reactie dat bij het onderbouwen van de noodzaak ten aanzien van de bevoegdheid van onderzoeksopdracht gerichte interceptie ook beoordeeld moet worden of er in een democratische samenleving als Nederland plaats is voor de bevoegdheden van de diensten, zoals voorgesteld in het wetsvoorstel. Nu echter zowel de Afdeling advisering van de Raad van State als de CTIVD de noodzaak van de nieuwe bevoegdheid afdoende onderbouwd achten, zie ik geen aanleiding een aanvullende weging uit te voeren. Voor wat betreft het punt aangaande het punt van de effectiviteit van "secret surveillance of grootschalige bulk interceptie" wordt nogmaals benadrukt dat daar met dit wetsvoorstel geen sprake van is. Er is sprake van onderzoeksopdrachtgerichte interceptie. Voor verdere toelichting hieromtrent verwijs ik naar de beantwoording van vragen van de verschillende leden. In paragraaf 3.4.2 van haar reactie geeft de Autoriteit Persoonsgegevens haar reactie op de voorstellen voor een effectief en onafhankelijk toezicht. Zij stelt daarbij vraagtekens bij de effectiviteit van de TIB, de waarde van de voorafgaande rechtmatigheidtoets en hoe de oordelen van de TIB zich zullen verhouden tot die van de CTIVD. Meer specifiek noemt de Autoriteit Persoonsgegevens in dit verband de beperkte omvang van de TIB en het ontbreken van eigen onderzoeksbevoegdheden. Ook acht zij onduidelijk wat de introductie van de TIB voor gevolgen zal hebben voor de mate waarin de betrokken ministers eigenstandig verantwoording kunnen afleggen aan het parlement. Het geheel overziend betwijfelt de Autoriteit Persoonsgegevens of het wetsvoorstel – in totaliteit bezien – wel voorziet in een stelsel van toezicht dat daadwerkelijk effectief is en alle facetten van de activiteiten van de diensten omvat, zoals bedoeld in artikel 8 EVRM. Zij is van oordeel dat de verhouding tussen ex ante en ex post toezicht opnieuw nadrukkelijk onder de loep genomen zou moeten worden. In reactie op dit onderdeel, merk ik op dat waar het gaat om (een deel van) de genoemde bedenkingen, deze reeds eerder – niet alleen in het advies van de Afdeling advisering van de Raad van State, maar ook in de vragen van leden van de diverse fracties – aan de orde zijn gesteld. Ik meen dan ook op dit onderdeel te kunnen volstaan met hetgeen, zowel in het nader rapport naar aanleiding

van het advies van de Afdeling advisering ter zake als in antwoord op de vragen van de leden van de verschillende fracties, in deze nota naar aanleiding van het verslag is gesteld. Alleen op het onderdeel van het afleggen van verantwoording aan het parlement wil ik nog afzonderlijk reageren. Anders dan de Autoriteit Persoonsgegevens ben ik van oordeel dat de introductie geenszins afdoet aan de mogelijkheid van ministers eigenstandig verantwoording af te leggen aan het parlement. De desbetreffende ministers zijn volledig verantwoordelijk voor en aanspreekbaar op hetgeen de onder hen ressorterende diensten doen en nalaten, ook indien de TIB negatief besluit op een verzoek. Dan is het immers primair aan de diensten en uiteindelijk aan de verantwoordelijke ministers om te bezien of aan de bezwaren van de TIB kan worden tegemoet gekomen en de aanvraag van een toestemming voor de inzet van een bijzondere bevoegdheid zodanig kan worden geformuleerd, zodat deze de rechtmatigheidstoets kan doorstaan. Ik ben dan ook van oordeel dat meer rechtmatigheidstoezicht aan de voorkant zeker geen vermindering van de parlementaire controle aan de achterkant zou betekenen. De parlementaire controle blijft onverkort overeind.

II. ARTIKELEN

Artikel 2

De leden van de SGP-fractie vroegen naar de betekenis van de bepaling dat de diensten en de coördinator hun taak in gebondenheid aan de wet uitvoeren. Hoewel deze bepaling ook in de huidige wet staat, vragen zij zich af of dit een logische bepaling is. Zij geven aan het uitgangspunt uiteraard te delen. Mag niet van elke (overheids)dienst verwacht worden dat binnen de regels van de wet wordt gewerkt? Waarom is gekozen voor opneming van deze bepaling en wordt met het slotformulier van de wet niet hetzelfde beoogd?
De leden van de SGP-fractie hebben gelijk dat van elke (overheids)dienst verwacht mag worden dat binnen de regels van de wet wordt gewerkt. Genoemde bepaling stamt dan ook uit een van de verre voorlopers van de huidige wettelijke regeling, te weten het koninklijk besluit van 5 augustus 1972 (Stb. 437), waarin regels werden gesteld met betrekking tot de taak , de organisatie, de werkwijze en de samenwerking van de inlichtingen- en veiligheidsdiensten. De hierin verwoorde notie was wellicht in die tijd (nog) niet gemeengoed en het waard bevonden om te worden vastgelegd. In de nadien tot stand gekomen wettelijke regelingen is deze bepaling telkens opnieuw opgenomen. Uit de wetsgeschiedenis valt ter zake weinig tot niets op te maken; wel is in het kader van de parlementaire behandeling van het voorstel van wet, dat uiteindelijk tot de Wet op de inlichtingen- en veiligheidsdiensten van 1987 heeft geleid, een opmerking gemaakt over het andere element van de bepaling, namelijk dat de diensten hun werkzaamheden verrichten in ondergeschiktheid aan de betrokken minister. Ten aanzien van dat element werd toentertijd al opgemerkt dat het mogelijk een overbodige bepaling leek, maar dat het ertoe strekte om buiten twijfel te stellen dat de diensten voor alle facetten van hun taakuitvoering onder de verantwoordelijkheid van de betrokken

minister vallen, die daarvoor op zijn beurt weer in volle omvang – politieke – verantwoordelijkheid aan het parlement verschuldigd is.[12] Gelet op de deels historische en deels symbolische waarde die het binnen de Nederlandse inlichtingengemeenschap vervult, stel ik voor deze in het wetsvoorstel te handhaven.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

[12] Kamerstukken II 1981/82, 17 363, nr. 3, p. 5.