Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 588 Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)

Nr. 17

VERSLAG

Vastgesteld 30 december 2016

De vaste commissie voor Binnenlandse Zaken, belast met het voorbereidend onderzoek van dit wetsvoorstel, heeft de eer als volgt verslag uit te brengen van haar bevindingen.
Onder het voorbehoud dat de regering op de gestelde vragen en de gemaakte opmerkingen tijdig en genoegzaam zal hebben geantwoord, acht de commissie de openbare beraadslaging over dit wetsvoorstel voldoende voorbereid.

INHOUDSOPGAVE **blz.**

kst-34588-17
ISSN 0921 - 7371
's-Gravenhage 2016

INHOUDSOPGAVE **blz.**

INHOUDSOPGAVE **blz.**

I. ALGEMEEN DEEL

De leden van de VVD-fractie hebben met belangstelling kennis genomen van het wetsvoorstel houdende Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) (hierna: het voorliggende wetsvoorstel). Het waarborgen van de nationale veiligheid en het beschermen van de Nederlandse rechtsstaat is een kerntaak van de overheid. Hierbij spelen de Nederlandse inlichtingen- en veiligheidsdiensten (hierna: de diensten), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), een cruciale rol. Risico's moeten in een zo vroeg mogelijk stadium gesigna-

leerd worden om de juiste acties te kunnen ondernemen. Zeker in een tijd waarin de terroristische dreiging substantieel is, onze buurlanden te maken hebben gehad met vreselijke aanslagen waarbij honderden doden zijn gevallen en in een tijd waarin Nederlanders vrijwillig uitreizen naar het kalifaat om daar mee te doen aan de gewapende strijd. Een tijd waarin sommige van deze mensen ook weer terug komen met het doel om aanslagen te plegen in het westen, met het doel om onze manier van leven aan te vallen. In deze tijd moeten we de opsporingsdiensten de juiste middelen geven om deze en andere gevaren voor onze nationale veiligheid op tijd te onderscheppen. Het is bovendien de verwachting dat deze dreiging voorlopig aan zal houden. Toch noopt niet alleen het huidige dreigingsniveau tot vernieuwing. De Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna: Wiv 2002) is verouderd. Deze wet is niet meer opgewassen tegen de dreiging en de moderne communicatiemiddelen van vandaag de dag. De technologische ontwikkelingen hebben de wet voorbij gestreefd. Het voorliggende wetsvoorstel moet daarom duurzaam bestand zijn tegen technologische ontwikkelingen. De techniekonafhankelijke bepalingen zijn noodzakelijk om de razendsnelle digitalisering voor te blijven. Het kan niet zo zijn dat hackers en criminelen uit beeld kunnen blijven van onze diensten puur en alleen omdat door gebruik te maken van (digitale) communicatiemiddelen waar onze diensten niet op toegerust zijn of ten aanzien waarvan zij geen bevoegdheden hebben. Daarom zijn de leden van de VVD-fractie een groot voorstander van de aanpassingen die in dit wetsvoorstel worden voorgesteld.
De leden van de VVD-fractie zijn zich bewust van het spanningsveld tussen privacy en veiligheid, de wetgeving en mensenrechten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (EVRM) en de maatschappelijke zorgen op dit gebied. De bevoegdheden van de diensten kunnen diep ingrijpen in iemand persoonlijke levenssfeer. Daarom is het van groot belang dat deze wet voorzien is van de juiste waarborgen.
De leden van de VVD-fractie hebben nog de volgende vragen.

De leden van de PvdA-fractie hebben met belangstelling kennis genomen van het voorliggende wetsvoorstel. Deze leden zijn van mening dat de diensten in het digitale tijdperk waarin wij leven een ruimere bevoegdheid moeten krijgen om ook kabelgebonden informatie te mogen onderscheppen en te gebruiken. De nationale veiligheid vergt dat de diensten niet op achterstand mogen staan ten opzichte van degenen die het internet gebruiken om diezelfde veiligheid te bedreigen. Dat neemt niet weg dat deze leden zich terdege bewust zijn van het feit dat het gebruik van dergelijke ruimere bevoegdheden kan ingrijpen op de persoonlijke levenssfeer van onschuldige burgers of gevolgen kan hebben voor de integriteit van het internet. Daarbij komt dat uit de aard van de activiteiten van deze diensten de democratische controle nooit volledig en in de openheid kan plaatsvinden. Dat maakt, samen met de bescherming van de privacy, dat de leden van de PvdA-fractie het voorliggend wetsvoorstel vooral zullen toetsen op de ingebouwde waarborgen dat de diensten hun bevoegdheden alleen dan kunnen gebruiken als dat nodig is en alleen onder strikte voorwaarden en waarborgen. De leden van de PvdA-fractie zijn van mening dat het voorliggend wetsvoorstel op meerdere punten verbetering of ten minste nadere uitleg verdiend. Deze leden hebben daarom de volgende vragen en kanttekeningen.

De leden van de SP-fractie hebben kennisgenomen van het voorliggende wetsvoorstel en hebben hierover verscheidende vragen en opmerkingen. De leden van de SP-fractie hebben begrip voor de stelling dat de huidige Wiv 2002 op punten gedateerd is. Ook begrijpen deze leden dat met de toenemende (cyber)dreiging en de snelheid waarmee technologische

vernieuwingen zich voordoen de roep om meer bevoegdheden voor de diensten toeneemt. Daarbij is voor deze leden altijd het uitgangspunt leidend dat de voorgestelde maatregelen proportioneel moeten zijn, dat moet worden voldaan aan het beginsel van subsidiariteit en dat de maatregelen praktisch uitvoerbaar moeten zijn. Deze leden zijn er niet van overtuigd dat het voorliggende wetsvoorstel in deze vorm aan deze uitgangspunten voldoet.
De leden van de SP-fractie lezen in de memorie van toelichting dat de regering beseft dat de bevoegdheden voor de diensten verregaand zijn, maar de regering verwijst ook naar het vertrouwen dat zij heeft dat de AIVD en de MIVD hier goed mee om zullen gaan. Deze leden merken op dat een wettelijke regeling vooral gebaseerd moet zijn op wettelijke waarborgen. Zeker nu de regering met een wetsvoorstel komt dat techniekonafhankelijk is en zij niet kan voorzien welke mogelijkheden er in de toekomst zullen zijn.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Deze leden onderkennen de noodzaak van modernisering van de bevoegdheden van de diensten in het licht van technologische en maatschappelijke ontwikkelingen, maar ook van toenemende terroristische dreiging, cyberdreigingen, de vele brandhaarden in de wereld en destabilisatie aan de grenzen van Europa. Een adequate informatiepositie van de diensten is noodzakelijk om te anticiperen op ontwikkelingen in de samenleving en bedreigingen van de nationale veiligheid in een zo vroeg mogelijk stadium te kunnen signaleren. Deze leden benadrukken dat nationale veiligheid een kostbaar goed is, waarvan het behoud investeringen vergt, zowel in financiële middelen als in wettelijke bevoegdheden en technische mogelijkheden. Deze leden onderkennen, dat een geavanceerde digitale samenleving en economie ongekende kansen en mogelijkheden biedt, maar tegelijkertijd in alle vitale belangen kwetsbaar is.
De leden van de CDA-fractie onderschrijven het uitgangspunt van de regering dat uitbreiding van bevoegdheden gepaard dient te gaan met uitbreiding van grondrechtelijke waarborgen en adequaat toezicht. Over het voorliggende wetsvoorstel hebben deze leden een aantal vragen.

De leden van de D66-fractie hebben met belangstelling kennisgenomen van zowel het voorstel tot een nieuwe Wet op de inlichtingen- en veiligheidsdiensten als de vele bezorgde reacties die erover zijn geuit. Voor deze leden staat voorop dat de diensten met adequate bevoegdheden zijn uitgerust, die niet verder gaan dan noodzakelijk, en dat deze in balans zijn met de waarborgen die daar tegenover staan. Zoals deze leden daarbij eerder verkondigd hebben, hanteren zij ten aanzien van de uitbreiding van bevoegdheden het «nee, tenzij»-principe. Over de in het voorliggende wetsvoorstel gemaakte keuzes hebben deze leden de nodige vragen en verbetervoorstellen, mede om uit te sluiten dat dit wetsvoorstel in enige reële interpretatie aanleiding zou kunnen geven tot National Security Agency (NSA)-achtige praktijken en sleepnetten.

De leden van de ChristenUnie-fractie hebben kennisgenomen van het voorliggende wetsvoorstel. Deze leden achten het van groot belang dat de diensten in staat worden gesteld dat te doen wat nodig is, maar hechten eraan dat daarbij zeer zorgvuldig wordt omgegaan met de vrijheden die alle burgers toekomen. Zij erkennen dat nieuwe bevoegdheden noodzakelijk kunnen zijn. Nieuwe bevoegdheden voor diensten moeten evenwel op effectieve wijze bijdragen aan de veiligheid en het belangrijke werk dat medewerkers van diensten iedere dag doen, zonder onnodig inbreuk te maken op vrijheden. Deze leden stellen daarom de volgende vragen.
De leden van de GroenLinks-fractie hebben met gemengde gevoelens kennis genomen van het voorliggende wetsvoorstel. Deze leden begrijpen

dat de Wiv 2002 gemoderniseerd moet worden. Tegelijkertijd constateren deze leden dat in dit wetsvoorstel verregaande bevoegdheden aan de veiligheidsdiensten worden toegekend, die het hen mogelijk maken om op grote schaal communicatie van Nederlandse burgers waar geen verdenking op rust, af te luisteren. De leden van de GroenLinks-fractie zijn nog niet overtuigd dat alle nieuwe bevoegdheden die in de wet worden gecreëerd noodzakelijk en proportioneel zijn voor het beschermen van de veiligheid van de samenleving. Deze leden vragen de regering per nieuw gecreëerde bevoegdheid op een concrete manier aan te geven waarom deze bevoegdheid noodzakelijk en proportioneel is in het kader van de bescherming van de veiligheid.
De leden van de GroenLinks-fractie voorzien dat de voorgestelde wet veel consequenties zal hebben op het gebied van ICT, bijvoorbeeld als het gaat om de zogenaamde onderzoeksopdrachtgerichte interceptie, en dat de naar aanleiding van het rapport van de tijdelijke commissie ICT door de Kamer betrachtte zorgvuldigheid met ICT-projecten ook in het geval van deze wet van toepassing dient te zijn. Deze leden verzoeken de regering dan ook het onderhavige wetsvoorstel voor te leggen aan het Bureau ICT-toetsing (BIT).

De leden van de SGP-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel om te komen tot een nieuwe wet op de inlichtingen- en veiligheidsdiensten. Deze leden vinden het belangrijk dat er in deze wet zowel aandacht is voor de waarborgen van de rechtsstaat als voor de bescherming van de veiligheid van onze samenleving. Het gaat om vergaande en ingrijpende bevoegdheden die gerechtvaardigd worden door het belangrijke doel van de veiligheid. Dat vraagt tegelijkertijd om voldoende effectieve waarborgen om misbruik van zulke bevoegdheden te voorkomen. Deze leden ontvangen graag verduidelijking over diverse aspecten van het wetsvoorstel.
De leden van de SGP-fractie hebben de indruk dat de regering in de toelichting minder duidelijk onderscheid heeft gemaakt tussen de algemene toelichting en de toelichting per artikel dan meestal gebruikelijk is. Deze leden 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 om te komen tot een duidelijker artikelsgewijze toelichting op het wetsvoorstel.

1. Inleiding

De leden van de CDA-fractie constateren dat de regering stelt dat de taakuitvoering van de diensten op dit ogenblik ernstig wordt belemmerd doordat de huidige wet niet techniekonafhankelijk is, terwijl de technologie zich onmiskenbaar heeft ontwikkeld (memorie van toelichting, blz. 9). Deze leden vragen welke consequenties de uitbreiding van bevoegdheden van de diensten zal hebben voor het benodigde budget, voor de benodigde formatie en voor de benodigde kennis en kunde van de medewerkers van de diensten. Deze leden stellen deze vraag mede in het licht van de conclusies en aanbevelingen van de Algemene Rekenkamer in het rapport Bezuinigingen en intensiveringen bij de AIVD (2015). Zijn de diensten voorbereid op de inzet van nieuwe bevoegdheden en op welke wijze worden de nieuwe bevoegdheden ingepast in het bestaande instrumentarium van de diensten?

1.1 Waarom de nieuwe wet?

De leden van de D66-fractie merken op dat de regering schrijft te willen voorkomen dat de balans tussen de nieuwe en bestaande bevoegdheden van de diensten en de grondrechtelijke waarborgen bij de uitoefening daarvan te zeer doorslaat naar de zorg voor de nationale veiligheid. In dat

kader verwondert het deze leden dat op 29 september 2015 een brief van de regering (Kamerstuk 33 989, nr. 8) met het navolgende verzoek is verschenen: «Het kabinet beraadt zich op het moment op de uitkomst van de consultatiefase van het voorstel van wet op de inlichtingen- en veiligheidsdiensten en geeft er de voorkeur aan vooraleerst de besluitvorming op dit punt af te ronden. Gelet hierop vraag ik u bij deze de plenaire behandeling van het herzieningsvoorstel voor artikel 13 Grondwet aan te houden.» Daarmee suggereert de regering dat zij eerst in de Wiv bevoegdheden voor de geheime diensten wil regelen, en daarna de grondwettelijke waarborgen ten aanzien van het brief- en communicatiegeheim daarop aanpast. Terwijl dit proces volgens deze leden uiteraard andersom moet zijn: de wet volgt de Grondwet. Klopt dit beeld van deze leden? Indien het niet klopt, erkent de regering dat dan op zijn minst de schijn gewekt is dat de zij voornemens is de Grondwet aan te passen aan de Wiv? Hoe beziet de regering 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?

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, met een tijdslijn waarin de hoeveelheid dataverkeer wereldwijd, plaatsgevonden aanslagen, ondernomen missies en technologische ontwikkelingen zijn afgezet op een tijd-as. Daarbij hebben deze leden een aantal vragen. Welke suggestie heeft de regering met deze infographic willen wekken? Welk verband is er tussen deze technologische ontwikkelingen en de dreigingen? In hoeverre is er niet alleen sprake van correlatie, maar ook van causale relatie? Wat is dan oorzaak van wat? In welke relatie staat de iPad tot de EU-antipirateriijmissie? Kan voor elk van de informatiecategorieën uitgelegd worden waarom deze is opgenomen in de infographic en hoe de selectie van mogelijk te vermelden informatie binnen die categorie gemaakt is? Welke schaal is gebruikt bij het weergeven van de toename van het dataverkeer?

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. Daarbij wordt een – begrijpelijk – voorbehoud gemaakt op, tegen wie of voor welk onderzoek de bevoegdheid ingezet wordt. Maar er wordt niets gezegd over het openbaar maken van geaggregeerde statistieken, zoals bijvoorbeeld de tapstatistieken van de AIVD waar deze leden al tijden om vragen en ten aanzien waarvan meerdere rechtszaken gestart zijn door journalisten en ngo's. Houdt de toegezegde «maximale transparantie» ten aanzien van onderzoeksopdrachtgerichte interceptie in dat over deze bevoegdheid wel samengevoegde data openbaar gemaakt worden? En wordt vervolgens ook het beleid ten aanzien van de huidige tapstatistieken gewijzigd? Indien één van deze vragen met nee wordt beantwoord, hoe moeten deze leden er dan vertrouwen in hebben dat de beloofde transparantie daadwerkelijk betracht zal worden? Hoe wordt «maximaal» dan precies gedefinieerd en ten uitvoer gelegd?

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

De leden van de PvdA-fractie hebben kennis genomen van de zienswijze van de Commissie van de Toezicht op de Inlichtingen- Veiligheidsdiensten (CTIVD) met betrekking tot het voorliggende wetsvoorstel. De conclusie van deze onafhankelijke toezichthouder dat de in het voorliggende

wetsvoorstel voorziene waarborgen onvoldoende zijn, ziet onder andere op de verwerking en analyse van de grote hoeveelheden data die er na inwerkingtreding van deze wet beschikbaar komen. Ten eerste wijst de CTIVD er op dat de nieuw voorziene «bulkinterceptie» risico's voor de bescherming van onze grondrechten met zich meebrengen, maar dat die beperkt zullen worden door een «verantwoorde databeperking». Dat wil zeggen «dat gegevens altijd zo gericht mogelijk dienen te worden verworven en dat verworven gegevens zo spoedig mogelijk moeten worden gereduceerd tot die gegevens die de diensten daadwerkelijk nodig hebben om hun taken goed uit te voeren. Niet meer en ook niet minder». De CTIVD wijst er echter op dat voor deze «verantwoorde databeperking» er in het voorliggende wetsvoorstel geen waarborgen of een duidelijke bepaling staan. Deze toezichthouder acht het van belang door het vereiste in de wet op te nemen dat de inzet van bevoegdheden «zo gericht mogelijk» moet zijn. Daarnaast zou er de doelgerichtheid bij de verwerking van gegevens in concrete wettelijke plichten moeten worden verankerd die ervoor zorgen dat de interceptie en verdere verwerking daadwerkelijk onderzoeksopdrachtgericht gebeurt, de opslag van gegevens daarmee wordt beperkt, vernietiging van gegevens tijdig plaatsvindt en dat op dit alles effectief toezicht kan worden gehouden. Dergelijke waarborgen komen de leden van de PvdA-fractie als bijna vanzelfsprekend over. Is daar op een andere wijze dan de CTIVD om vraagt al in voorzien? Zo ja, op welke wijze dan? Zo nee, waarom niet en kan hier dan alsnog in worden voorzien?

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. Daarnaast is het noodzakelijk dat meer vormen van geautomatiseerde data-analyse als bijzondere bevoegdheid worden aangemerkt met de daarbij passende waarborgen». Kam de regering ook hier nader op ingaan? De leden van de PvdA-fractie verwijzen voor een nadere toelichting van het bovenstaande graag naar de schriftelijke zienswijze met bijlagen die de CTIVD naar buiten heeft gebracht.

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

De leden van de D66-fractie lezen dat iedere inzet van bevoegdheden door de AIVD en MIVD moet voldoen aan de vereisten van proportionaliteit, subsidiariteit en doelgerichtheid. Als voorbeeld daarvan wordt gegeven dat geen onderzoeksopdrachtgerichte interceptie plaatsvindt om alle communicatie in de stad Den Haag een maand lang te verzamelen, om zo te bezien of voor de diensten relevante gegevens zijn binnengehaald. Deze leden zouden die toezegging graag nog willen aanscherpen. Wordt eveneens uitgesloten dat dit voor een kortere periode gebeurt of dat dit op wijk- of buurtniveau gebeurt? En kan verduidelijkt worden wat in dit kader «relevante» gegevens zijn? Wordt die «relevantie» enkel bepaald aan de hand van de gegeven last(en) conform artikel 48 of de artikelen 48 en 49 of kunnen andere onderzoek(sopdracht)en daarin meewegen? En stel dat één van de uitsluitingsvragen met een nee is beantwoord, onder welke omstandigheden wordt dit wel noodzakelijk, proportioneel en subsidiair geacht? Speelt in de proportionaliteitsafweging in dit voorbeeld dan niet slechts het belang van de inwoners van Den Haag mee, maar ook het algemene vertrouwen in het anoniem en veilig kunnen gebruiken van het internet?

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.
Ook vragen deze leden zich af hoe onderzoeksopdrachtgerichte interceptie gaat bijdragen aan de snelheid waarmee een beeld opgebouwd kan worden van de veiligheidssituatie in een gebied waar onze militairen naar toe uitgezonden worden?
In de Defensie Cyber Strategie staat: «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.» De leden van de VVD-fractie zouden hier graag een toelichting op hebben.

De leden van de D66-fractie merken op dat de regering spreekt over het techniekonafhankelijk maken van bevoegdheden. Voorts merken deze leden op dat de manier waarop in 2002 gebruik werd gemaakt van de verschillende infrastructuren – dat wil zeggen informatie via de ether en via de kabel – sterk van elkaar verschilden. Niet-kabelgebonden informatie betrof dikwijls telefoongesprekken of hoogfrequent (militair) radioverkeer dat werd opgevangen werd door de Nationale Sigint Organisatie, terwijl kabelgebonden informatie dikwijls informatie betrof die via het internet verstuurd werd, bijvoorbeeld voor internet bankieren, het versturen van e-mails, het opzoeken van informatie of het versturen van medische gegevens. Daardoor hadden de verschillende manieren van versturen van informatie ook verschillende doelen, en verschilde ook de mate van inbreuk op de persoonlijke levenssfeer van mensen, zo merken deze leden op. Pas sinds de opkomst van draadloos internet via 3G- en 4G netwerken is het gebruik van beide infrastructuren op elkaar gaan lijken, alhoewel er nog steeds qua omvang en gebruik belangrijke verschillen bestaan. Daarom, zo constateren deze leden, blijft het verschil in inbreuk op de persoonlijke levenssfeer van mensen bestaan. Het ongericht aftappen van informatie op de kabel is een grotere inbreuk op de persoonlijke levenssfeer dan het aftappen van informatie via de ether. Daarmee is ook het simpelweg «techniekonafhankelijk maken van bevoegdheden» volgens deze leden een te simplistische weergave van zaken. Is de regering het eens met de analyse van de leden van de D66-fractie? Is de constatering dat er verschil bestaat in de mate van inbreuk op de persoonlijke

levenssfeer tussen het ongericht aftappen van informatie uit niet-kabelgebonden en kabelgebonden bronnen, niet juist een reden om bevoegdheden techniek-afhankelijk in te richten? Is het feit dat de AIVD ook geen bevoegdheid heeft om briefverkeer ongericht te doorzoeken daar geen voorbeeld van?

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

De leden van de VVD-fractie vragen of u een overzicht kunt geven 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.
De leden van de D66-fractie zouden graag meer onderbouwing willen 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. De opgenomen lijst van voorbeelden klinkt immers zodanig ernstig, dat men zich afvraagt waarom er zo lang gewacht is om de Wiv 2002 aan te passen. Waarom gebeurt dit pas na evaluatie van de Wiv 2002 ruim 10 jaar later? En waarom wordt er drie jaar aan de nieuwe Wiv geschreven? Dat strookt slecht met het urgente beeld dat geschetst wordt in de toelichting, aldus deze leden Bovendien mag het geen verrassing heten dat de techniek zich sterk ontwikkeld heeft. Dat roept de vraag bij deze leden de volgende vraag op. Voor zover dreigingen nu niet tijdig onderkend worden, hadden die niet voorkomen kunnen worden? Sinds wanneer hebben de diensten – of heeft één van beide diensten – aangedrongen op een herziening van de Wiv 2002 om toegang te krijgen tot kabelcommunicatie? Hoe is daar aanvankelijk op gereageerd door de verantwoordelijke regering?
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) aangaf dat internettaps steeds minder nuttige informatie opleveren als gevolg van versleuteling. Wat is de reden dat de regering van mening is dat ongerichte internettaps door de inlichtingen- en veiligheidsdiensten wél nuttige informatie kunnen opleveren?

De leden van de ChristenUnie-fractie constateren dat het voorliggende wetsvoorstel techniekneutraal is vormgegeven. Dat lijkt deze leden verstandig, maar zij zien daarin ook het risico dat daarmee bevoegdheden meer opgerekt worden dan door de wetgever vooraf voorzien. Op welke wijze wordt de Kamer geïnformeerd over de ontwikkelingen in het gebruik van de bepalingen rond interceptie van data? En is de regering met deze leden van mening dat dit een bijzonder aandachtspunt moet zijn in het toezicht dat de CTIVD op de uitoefening van de bevoegdheden in deze wet houdt?

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

De leden van de D66-fractie lezen dat de regering schrijft dat zij niet kiest voor een samenleving waarin burgers zonder gerechtvaardigde redenen worden gevolgd en in de gaten gehouden worden. Dat juichen deze leden zeer toe. Zij vragen zich echter af wat de regering verstaat onder «gerechtvaardigde redenen». Is het toevallig over dezelfde etherband of fiber van een internetkabel lopen van jouw communicatie een reden dat jouw (meta)data gevolgd wordt? De waarborgen van het voorliggende wetsvoorstel lijken immers vooral te liggen in de sfeer van selectie en filters, en niet intrinsiek in een beperkte reikwijdte van de bevoegdheden. Aangezien het wetsvoorstel voor velen technisch zal zijn, en de toelichting bijzonder lang is, vragen deze leden of de regering in een alinea en voor

een ieder begrijpelijke taal kan uitleggen wat die gerechtvaardigde redenen zijn, 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.

1.3.3 Cybersecurity (§1.3.4. m.v.t.)

De leden van de D66-fractie constateren dat de regering van mening is dat het voorliggende wetsvoorstel kan bijdragen aan het verminderen van cyberspionage. Daarbij gebruikt de regering termen als «de tegenactie inzetten» en «digitale grensbewaking». Kan de regering op technisch- en beleidsmatig niveau toelichten hoe dit wetsvoorstel het verminderen van cyberaanvallen gaat bewerkstelligen? Is de regering met deze leden van mening dat het dichten (in plaats van het openhouden) van software-kwetsbaarheden, 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? Hoe gaan de diensten om met de constatering van het kabinet in de brief over 0-days dat het in stand houden van kwetsbaarheden kan leiden tot meer cyberaanvallen? Is de regering bekend met de daling van het aantal Chinese cyberaanvallen op de Verenigde Staten en op Amerikaanse bedrijven als gevolg van de diplomatieke aanpak van president Obama? Is de regering bereid een dergelijke aanpak in Europees verband op te zetten?

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 verantwoordelijkheid met zich meebrengt dat Nederland een internationale hub voor datacommunicatie is. Tegelijkertijd vrezen deze leden dat het voor onze regering en onze diensten erg verleidelijk wordt die «pot snoep» te openen. In die zin vragen deze leden hoe de titel van deze paragraaf begrepen moet worden: 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?

De leden van de D66-fractie krijgen de indruk dat Nederland mee wil doen aan de digitale wapenwedloop. Stilstaan is inderdaad geen optie, maar waar China 180.000 hackers heeft klaarstaan, hebben wij moeite om 150 cyberreservisten te vinden. Op welke wijze, anders dan dit wetsvoorstel, krijgt een goede cyberpositie aandacht van de regering? Enerzijds is het volgens deze leden denkbaar – zoals de regering doet – dat een land met beperkte interceptiemogelijkheden aantrekkelijker is voor cyberaanvallers, anderzijds is het niet onaannemelijk dat wie in de coulissen staat minder aandacht trekt dan de hoofdrolspelers.

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 filosoferen graag verder op de analogie van het kabelnetwerk met het waterleidingnetwerk. Er zit immer een fundamenteel en inherent verschil in hetgeen beide netwerken moeten leveren, aldus deze leden. Een waterleidingnetwerk moet water leveren, waaraan niets is toegevoegd (zie bijvoorbeeld de fluorideringszaak bij de Hoge Raad) en waar potentieel schadelijke stoffen (zoals landbouwgifresten, medicijnresten en degelijke) uitgefilterd zijn. Het internet daarentegen is naar zijn aard anders: ook hiervoor zijn kabels ter vervoer nodig, maar wat

vervoerd wordt is geen materie, maar communicatie. Voor waterfilters is objectief vast te stellen wat wel en niet mag worden doorgelaten in het belang van de volksgezondheid en vrijheid van de persoonlijke levenssfeer. Voor het internet is dit niet te doen. Waar dat wel geprobeerd wordt, duidt ook onze regering dat typisch gezien aan met «internetcensuur». In dat kader zouden deze leden graag een nadere beschouwing willen verkrijgen hoe dat «waterfilter van het internet» dat de regering voornemens is te gaan plaatsen, gaat werken.

1.5 Hoe heeft de regering het wetsvoorstel voorbereid?

De leden van de D66-fractie hebben met grote belangstelling kennisgenomen van de zienswijze van de CTIVD. Wat deze leden in het bijzonder opvalt aan deze zienswijze is dat de CTIVD als toezichthouder op de diensten aanzienlijke fundamentele bezwaren plaatst bij het voorliggende wetsvoorstel. Op meerdere cruciale aspecten van het wetsvoorstel ontbreken volgens de CTIVD waarborgen op onder meer de correcte uitoefening van de bevoegdheid, de rechtseenheid, de bescherming van privacy en andere grondrechten, de risico's van bulkinterceptie en goed toezicht op geautomatiseerde gegevensverwerking. Deelt de regering de zienswijze van de CTIVD? Is de CTIVD gevraagd om tijdens het vormgeven van het wetsvoorstel haar zienswijze reeds naar voren te brengen? Is de CTIVD op enigerlei wijze in het voortraject van het wetsvoorstel door de regering betrokken bij het opstellen daarvan? Zo ja, op welke wijze? Kan de regering toelichten 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?

1.6. Wat verandert er met het nieuwe wetsvoorstel?

De leden van de VVD-fractie vragen of de regering kan toelichten hoe de werkwijze van de Toetsingscommissie Inzet Bevoegdheden (TIB) en de ministeriele verantwoordelijkheid zich tot elkaar verhouden? Deze leden vragen of de TIB in staat zal zijn te oordelen over overwegingen rondom buitenlands beleid, bijvoorbeeld inzake het plaatsen van een tap in het buitenland.

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 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, aldus deze leden. Mogen deze leden opslaan in deze zin interpreteren? Zo nee, waarom niet?

Voorts schrijft de regering dat de diensten niet op zoek gaan naar mensen die het woord «bom» of «ISIS» gebruiken in hun e-mails en dat geen internetverkeer in bulk naar binnen getrokken wordt om te kijken welke mensen op zoek zijn naar «kunstmest». Wat verstaat de regering in dit kader onder «bulk»? Kan daarvan een exacte definitie gegeven worden, waarbij dit uitgedrukt wordt in hoeveelheid megabytes of in hoeveel personen wiens data daarin besloten zit? 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? Hoewel deze leden waarderen dat de regering zo strikt gericht de kabel wil aftappen, vragen zij zich wel af hoe dit zich verhoudt tot hetgeen de kabel-aftapbevoegdheid voor nodig zou zijn, namelijk het opsporen van onbekende dreigingen.

2. De diensten en de coördinatie tussen de diensten

De leden van de CDA-fractie merken op dat de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2002 (commissie Dessens) in haar rapport heeft aangegeven dat de rol van de coördinator van de inlichtingen- en veiligheidsdiensten onvoldoende uit de verf komt (memorie van toelichting, blz. 22). De regering stelt dat de ministeriële verantwoordelijkheid voor de operationele taakuitvoering zich niet verhoudt met een coördinerende taak van de coördinator op dit terrein. De coördinator zal evenwel een eigenstandige positie behouden met eenduidig belegde verantwoordelijkheden. De leden van de CDA-fractie vragen de regering nader uiteen te zetten, of de door de commissie Dessens gesignaleerde problemen met betrekking tot de rol van de coördinator met het voorliggend wetsvoorstel zijn ondervangen. Deze leden stellen deze vraag mede met het oog op de informatie-uitwisseling tussen de diensten, die immers niet alleen (wets)technische, maar ook culturele aspecten heeft.

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. De uitwerking daarvan vindt blijkens artikelen 8, tweede lid, onder f, en 10, tweede lid, onder g, plaats bij ministeriele regeling. Gegeven de gevoeligheden die gepaard gaan met dergelijke naslagen krijgen deze leden graag meer inzicht in de voorgenomen kring van personen die bevoegd is tot het doen van een dergelijk verzoek en ten aanzien van welke personen en onder welke omstandigheden dat verzoek gedaan kan worden. Daarbij zijn deze leden ook benieuwd aan welke personen een instemmingsverklaring als bedoeld in artikel 63, tweede lid, onder b, gevraagd zal worden. Immers, hoe wordt bepaald wanneer dit de effectiviteit van het onderzoek als bedoeld in het derde lid zou kunnen schaden? Daarover kan verschillend gedacht worden, zo merken deze leden op. Hoe was de procedure verlopen in het geval deze wet reeds had bestaan op het moment dat Prins Bernhard naslag verzocht (c.q. eiste) van Edwin de Roy van Zuydewijn? En op welk moment zal een eventuele relatie van onze kroonprises Prinses Amalia of één van haar zussen dusdanig serieus zijn dat naslag verricht zal worden? Zal daarvoor altijd eerst aan de betrokken persoon toestemming gevraagd worden? Voor zover dat niet het geval is, hoe is naar buiten toe voldoende kenbaar dat op een bepaald moment in de relatie naslag zal worden verricht? Deze leden vragen zich voorts af hoe vaak op dit moment naslag verricht wordt.

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. Deze functionaris valt onder het Ministerie van Algemene Zaken. In hoeverre is het logisch om deze taak bij een ander ministerie te beleggen dan een ministerie dat primair betrokken is bij de (nationale) veiligheid? Zorgt dit niet juist voor versnippering van de taken over verschillende ministeries? De Commissie Dessens stelde immers juist voor om de rol van coördinator niet alleen bij Algemene Zaken te leggen, maar bij een driemanschap van de secretarissen-generaals van de

ministeries van Algemene Zaken, Defensie en Binnenlandse Zaken, onder voorzitterschap van de secretaris-generaal van Algemene Zaken. Zou dat er niet toe kunnen leiden dat de coördinatietaak dichter bij de verschillende departementen komt te staan?

In dit verband is voor deze leden de vraag in hoeverre het logisch is om naast de Commissie Veiligheids- en Inlichtingendiensten (CVIN) nog een afzonderlijke coördinator te hebben. Zou deze rol niet juist verwarrend en als een doublure werken naast de CVIN? Zou het niet logischer zijn om deze CVIN te laten gelden als coördinerend orgaan, waarbij dan een voorzittersrol is weggelegd voor de coördinator vanuit Algemene Zaken? Zou dat niet juist de gemeenschappelijke betrokkenheid bij en het verantwoordelijkheidsgevoel voor de gezamenlijke veiligheid kunnen bevorderen? Er moet immers worden voorkomen dat de structuur van de diensten verwarrend is vormgegeven.

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

De leden van de SGP-fractie constateren dat bij de specifieke onderzoekstaken gericht op het buitenland (artikel 8, onderdeel d en 10, onderdeel e) geen aangegeven onderwerpen meer vereist zijn. De regering stelt dat dit valt onder de «Geintegreerde aanwijzing» op grond van artikel 5. Tegelijkertijd wordt er ook gesproken over de mogelijkheid voor de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie om onderzoeksopdrachten te geven. Deze leden constateren dat dit niet rechtstreeks voort lijkt te vloeien uit de tekst van de wet. Wat is anders de precieze waarde van de «geïntegreerde aanwijzing» als er ook nog afzonderlijke taken naast kunnen blijven bestaan? Er dient immers in de geïntegreerde aanwijzing ook een prioritering gegeven te worden. Hoe verhoudt die prioritering zich tot de specifieke onderzoeksopdrachten door beide ministeries? Hebben die onderzoeken voorrang op de vastgestelde prioriteiten?

3. De verwerking van gegevens door de diensten

3.1 Algemeen

De leden van de PvdA-fractie menen dat de verzameling van bulkgegevens en vooral de verdere verwerking en analyse daarvan een grote inzet en kennis van personeel zal vergen. Is dat een juiste veronderstelling? Zo ja, zijn de diensten daar op voorbereid en waar blijkt dat uit? Zo nee, waarom is dit geen juiste veronderstelling?

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. Daarnaast vragen deze leden waarom is gekozen voor de term «seksueel leven». Zij vragen hier om een nadere toelichting.

De leden van de SP-fractie lezen dat er alvast een voorschot wordt genomen op eventuele relevante informatiebronnen waar de diensten gebruik van kunnen maken, die nu nog niet te voorzien zijn (artikel 25, lid 2). In de memorie van toelichting wordt gesteld dat het voor de hand ligt dat de Kamer hierover wordt geïnformeerd door de Minister vanwege de actieve informatieplicht. Deze leden vragen zich af waarom hier niet gekozen is voor een wettelijke verankering, gelet op het belang van controle op extra bevoegdheden.

Daarnaast lezen de leden van de SP-fractie dat in deze gevallen de Minister toestemming kan verlenen om deze andere bronnen te gebruiken. Juist in deze technologisch snel veranderende wereld en de hoeveelheid data die over mensen en hun apparaten beschikbaar is, is het noodzakelijk dat er voldoende waarborgen zijn om de privacy van mensen te beschermen en te waarborgen. Alleen toestemming van de Minister om de diensten deze bevoegdheden te kunnen geven lijkt daarom niet voldoende. Waarom is er niet voor gekozen de TIB een rol te geven?

Door de grote hoeveelheden gegevens die verzameld kunnen worden, wordt het onmogelijk deze gegevens handmatig te controleren. Datamining en het gebruik van geautomatiseerde algoritmes kan afbreuk doen aan de betrouwbaarheid van de gegevens. In de Privacy Impact Assessment (PIA) worden daarom op dit gebied aanvullende aanbevelingen gedaan. De regering vindt deze aanvullingen te ver gaan. Juist nu de diensten meer bevoegdheden krijgen om deze grote hoeveelheden data te verzamelen lijkt het de leden van de SP-fractie niet overbodig ook hiervoor extra waarborgen in te bouwen. Kan de regering aangeven waarom zij het voorstel in de PIA te ver vinden gaan en wat de praktische bezwaren hiertegen zijn?

De leden van de SP-fractie lezen verder dat er een rechterlijke toets ingesteld wordt voor het gebruik van bevoegdheden bij journalisten en advocaten. Waarom is deze rechterlijke toets alleen bij advocaten en journalisten noodzakelijk en niet bij notarissen, artsen, geestelijken – en bijvoorbeeld ook bij Kamerleden?

3.2 De algemene bepalingen inzake de verwerking van gegevens

3.2.1. Algemene eisen aan gegevensverwerking

De leden van de D66-fractie delen de zorg van onder andere de CTIVD en de PIA dat gegevensverwerking zonder duidelijke en wettelijk vastgelegde eisen risico's met zich meebrengt. Die risico's kunnen wat deze leden betreft zowel gelegen zijn in de uitvoering als in het toezicht. Het lijkt deze leden daarom nodig om in de 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 34 588, nr. 15) ingediend. Graag horen deze leden van de regering hoe zij, indien dit amendement aangenomen of overgenomen zou worden, invulling gaan gegeven aan dit gegevensbeschermingsbeleid.
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 bestaat daarin? Welke foutmarge (qua false positives en qua false negatives) acht de regering daarbij acceptabel? Hoe verhoudt zich dat tot andere diensten in Nederland en het buitenland? Hoe wordt ten aanzien van de uitkomst van de verwerking en van de analyse duidelijk gemaakt wat de kwaliteit van de broninformatie en die van de verwerking ervan is en wat de context van die informatie is? Op welke wijze wordt bijvoorbeeld de betrouwbaarheid van informatie automatisch afgeschaald naarmate de tijd verstrijkt? 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. Graag

verkrijgen deze leden voorbeelden van hoe die informatie binnen het analyse-product vermeld wordt.

De leden van de SGP-fractie constateren dat de regering aangeeft dat gegevens die zijn verzameld zijn voor een bepaald doel, ook gebruikt mogen worden voor een ander onderzoek binnen dezelfde taak of ook voor een andere taak. Deze leden begrijpen dat dit logisch is, gezien het gegeven dat de veiligheid zoveel mogelijk beschermd moet worden. Zij vragen zich alleen wel af hoe dit precies uit de wettekst zelf blijkt. Op grond van artikel 27 moeten gegevens immers eerst onderzocht worden op relevantie. Niet-relevante gegevens moeten worden vernietigd. Betekent dit dat gegevens alleen gebruikt mogen worden voor onderzoeken die op het moment van het verkrijgen ook daadwerkelijk lopen? Hoe wordt dan precies bepaald of het inderdaad past binnen een lopend onderzoek? Wat dient er bijvoorbeeld te gebeuren als de gegevens nog niet vernietigd zijn, maar bijvoorbeeld een half jaar of negen maanden later alsnog blijkt dat een nieuw onderzoek nodig is waar deze gegevens voor gebruikt kunnen worden? Is dit criterium van «lopend onderzoek» niet voor meer uitleg vatbaar en te vaag?
Ook vragen de leden van de SGP-fractie naar het onderscheid tussen verwijderen, vernietigen en terstond vernietigen. In sommige artikelen van het wetsvoorstel (bijv. artikel 37 en 47 wordt bij vernietigen gesproken over «terstond vernietigd». Op andere plaatsen wordt gesproken over «vernietigd». Zij begrijpen dat de gegevens ten minste bewaard moeten blijven in een semi statisch archief zolang er de mogelijkheid van bezwaar of klacht is. Maar 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.

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. Wanneer is dit onvermijdelijk voor het doel van de gegevensverwerking? Moet dit een materiele onvermijdelijkheid zijn, of kan dit ook een onvermijdelijkheid zijn in de zin van «onze software, ons algoritme of ons model heeft dit kenmerk (bijvoorbeeld ras of seksueel leven) nodig om tot conclusies te komen»? Indien het ook dit tweede betreft, waarom is de regering van mening dat hier geen sprake is van echte onvermijdelijkheid, omdat er ook andere keuzes gemaakt hadden kunnen worden ten aanzien van de programmering of aanschaf van betreffende modellen/ICT/software? Kan voorts uitgesloten worden dat betreffende andere gegevens slechts verwerkt worden met als doel de bedoelde kenmerken te kunnen verwerken? Op welke wijze is dit in de systematiek van het voorliggende wetsvoorstel gewaarborgd?

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

De leden van de D66-fractie constateren dat gegevensverwijdering niet een verwijdering in de zin van het normale taalgebruik inhoudt. De gegevens blijven immers totdat ze vernietigd worden bestaan, zij het dat ze niet langer toegankelijk zijn voor de normale taakuitvoering. Als voorbeeld van het nut van het toch bewaren van informatie wordt klachtbehandeling gegeven, maar ook dat de bewaarde informatie weer geactiveerd kan worden als dat voor een onderzoek nuttig blijkt. Dat roept bij deze leden een aantal vragen op. Artikel 20, derde lid, wekt namelijk vrij categorisch de indruk dat verwijderde gegevens vernietigd worden,

behoudens wettelijke verplichtingen. Welke wettelijke verplichtingen zijn dat? Deze leden vragen om een uitputtende lijst. Welke termijn geldt voor die vernietiging? Wie kan besluiten verwijderde gegevens niet te vernietigen, maar te her-activeren? Binnen welke termijn moet dat gebeuren? Is het mogelijk vernietiging op te schorten voor mogelijk gebruik bij een onderzoek? Zo ja, aan welke voorwaarden moet een dergelijk verzoek voldoen? Welke bewaartermijnen gelden vervolgens? Beginnen die opnieuw te lopen, of wordt de eerdere bewaartermijn voortgezet? Met andere woorden, stel dat de betreffende data een jaar bewaard mogen worden en na elf maanden verwijderd worden, mag na het opnieuw in de actieve systemen toegankelijk maken van die data, zij dan nog een maand of een jaar worden bewaard?
De leden van de D66-fractie vragen zich 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. Kan de regering deze interpretatie van de wet uitsluiten en precies aangeven hoe artikel 20, eerste lid, in dit opzicht gelezen moet worden en zo nodig daarbij differentiëren naar gelang via welke bevoegdheid de gegevens verworven zijn?
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. Dat waren bijzonder lange lijsten, waarvan lastig te beoordelen was of ze een goed evenwicht bewaarden tussen vernietigen en overbrenging, tussen openbaren en niet openbaren. Op welke wijze zal het voorliggende wetsvoorstel de, begin dit jaar na een ellenlang proces, vastgestelde selectielijsten beïnvloeden? Moet er, nu er meer en andere typen informatie verzameld worden, ook op een andere manier invulling gegeven worden aan die lijsten teneinde voldoende informatie voor toekomstig (historisch) onderzoek te bewaren? Valt er voorts te denken aan het anders inrichten van de selectielijsten, zodat buitenstaanders meer inzicht krijgen in de daarin besloten keuzes?

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.
Met betrekking tot de verwijdering en vernietiging van gegevens vragen de leden van de GroenLinks-fractie een algemene toelichting op de schijnbare willekeur waarmee op sommige plaatsen van het voorliggende wetsvoorstel is bepaald dat gegevens terstond dienen te worden vernietigd, zoals in artikel 27 lid 2, en dat het woord «terstond» op andere plaatsen ontbreekt, zoals in artikel 20 lid 1 en 3 en artikel 27 lid 1. Deze leden vragen de regering een toelichting te geven wat dit betekent voor de termijn waarop daadwerkelijke verwijdering c.q. vernietiging van gegevens dient plaats te vinden en waarom ervoor is gekozen om niet te bepalen dat dit altijd terstond dient te gebeuren. Deze leden ontvangen graag een overzicht van de regering waarin zij per verwijdering- en vernietigingsbepaling uiteen zetten wat de maximale termijn voor de uitvoering van deze verwijdering of vernietiging is.

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

De leden van de D66-fractie lezen dat de regering 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. Daarbij beroept de regering zich op de aard van het werk bij de diensten. Suggereert de regering daarmee dat dit door de onderzoekers van de PIA niet is meegenomen? Miskent de regering daarmee niet ook dat het op een privacy-vriendelijke manier inrichten van de systemen met autorisatieprocedures, compartimentering en dergelijke altijd zal plaatsvinden binnen een risico-afweging, namelijk gebruiksgemak in de dagelijkse praktijk versus de omvang van de schade als er een medewerker is die zonder rechtvaardiging gegevens opvraagt of wanneer er sprake is van een hack bij de dienst? Daarbij zal vanuit de praktijk, zo nemen deze leden aan, eerder gebruiksgemak en vertrouwen op de eigen beveiliging voorop staan, dan design en compartimentering uitgaande van misbruik of inbraak. De leden van de D66-fractie zouden het waarderen als dit aspect van de gegevensbescherming in antwoord in de nota naar aanleiding van het verslag nader uitgewerkt zou worden door de regering.

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 D66-fractie constateren dat artikel 25, eerste lid, limitatief op lijkt te sommen uit welke informatiebronnen de diensten mogen putten voor hun taakuitvoering, en dat het tweede lid regelt dat per ministeriele toestemming alternatieve bronnen aangewend mogen worden. Deze leden hebben daar nog enkele vragen over. Zo valt hen het woord «in ieder geval» in het eerste lid op. Dit impliceert dat er buiten de ministeriele toestemming van het tweede lid vallende informatiebronnen zijn die niet expliciet genoemd worden. Dit achten deze leden onwenselijk, vandaar dat deze woorden in het amendement van het lid Verhoeven over de informatiebronnen waaruit de diensten gegevens kunnen verzamelen (Kamerstuk 34 588, nr. 9) vervallen. Voor zover de regering deze lezing van het eerste lid bestrijdt, zou zij nader kunnen duiden welk nut deze drie woorden dienen en hoe elk misbruik daarvan uitgesloten is, of kan worden.

Verder zouden de leden van de D66-fractie de bevoegdheid van Onze Ministers om alternatieve informatiebronnen aan te wijzen graag nader inkaderen. Hoewel de geheime aard van het werk van de diensten het onmogelijk maakt volledige kenbaarheid en voorzienbaar na te streven, moet daar wel zoveel mogelijk sprake van zijn, aldus deze leden. Een onderdeel daarvan is het voeren van parlementair debat over de bevoegdheden die dergelijke diensten hebben en onder welke omstandigheden zij ingezet kunnen worden. Zowel voor het gebruikmaken van alternatieve, nu niet voorziene, informatiebronnen als voor nieuwe technische toepassingen van bijzondere bevoegdheden voor zover deze een substantiële en vergaande inbreuk op de persoonlijke levenssfeer kunnen maken, zou daarom sprake moeten zijn van de mogelijkheid tot debat hierover. Dit zou niet moeten afhangen van de vraag of de CTIVD dit opmerkt en opneemt in de geheime bijlage van haar toezichtsrapport aan de Commissie voor de Inlichtingen- en Veiligheidsdiensten(CIVD), zoals gebeurde bij toezichtsrapport nr. 46. Deze leden hebben daarom in voornoemd amendement ook een voorziening opgenomen dat de Kamer hierover altijd, zo nodig vertrouwelijk, geïnformeerd wordt. Graag

vernemen deze leden aan wat voor soort alternatieve informatiebronnen gedacht moet worden.

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. Het is deze leden echter in het kader van de Wet raadgevend referendum gebleken dat de term «zo spoedig mogelijk» rekbaar is. Zij horen daarom graag wat de regering in dit kader spoedig acht en wat niet en welke termijn daaraan is gekoppeld. Houdt dit ook in dat voor zover het schiften op relevantie automatisch gebeurt, hiervoor altijd het algoritme gekozen moet worden dat meer stappen verzet, daardoor langzamer werkt, maar wel nauwkeuriger is? Wordt, indien dat het geval is, ook in de berekening meegenomen dat gegevens die onterecht bewaard worden, de gemiddelde termijn van bewaring van deze niet-relevante data sterk kunnen verlengen? Indien dit niet zo absoluut gelezen hoeft te worden, hoe moet het dan wel geïnterpreteerd worden, zo vragen de leden van de D66-fractie. Wat acht de regering een redelijke termijn voor het filteren van gegevens die verkregen zijn via de navolgende bevoegdheden: het kopiëren van een webforum, het gedurende een half uur onderschepte internetverkeer met een nepwifi, een binnengedrongen laptop waarvan de gegevens niet versleuteld zijn en via de interceptiebevoegdheid van artikel 48 verkregen gegevens met als doel uit te vinden wie in een woning schuil gaat achter een nickname.
De leden van de D66-fractie lezen dat onvoldoende vertaalcapaciteit onder omstandigheden reden kan zijn om tot verlenging van de bewaartermijn als bedoeld in artikel 27 over te gaan. Welke omstandigheden heeft de regering daarbij precies op het oog? Heeft een dergelijke verlenging ook gevolgen voor de voortzetting of voor de aanvraag van lasten ten aanzien van diezelfde taak? Op het moment dat de verzamelde gegevens niet bruikbaar meer zijn voor de diensten, kunnen deze leden zich voorstellen dat daarmee de proportionaliteit die noodzakelijk is voor het toekennen van de last wegvalt. Er vindt dan namelijk wel een inbreuk op de persoonlijke levenssfeer plaats, maar het dient – in ieder geval voor zo lang er geen vertaalcapaciteit is – geen nut. Op welke wijze zal in dit kader worden omgegaan met de toestemming tot inzet van een bijzondere bevoegdheid?

De leden van de ChristenUnie-fractie constateren dat in artikel 27 een specifieke beroepsgroep (terecht) wordt beschermd tegen doorbreking van vertrouwelijke communicatie, te weten advocaten. Is overwogen om een bredere verschoningsgrond op te nemen in de wet? Waarom is daar vanaf gezien?
De leden van de ChristenUnie-fractie constateren dat de Studiecommissie Journalistieke Bronbescherming ernstige zorgen heeft geuit over het waarborgen van de journalistieke bronbescherming in het voorliggende wetsvoorstel. Journalistieke bronbescherming is van belang voor het werk van journalisten en kan, indien eenmaal in een bepaald geval doorbroken, ernstige schade berokkenen aan de betrokken bronnen en aan de toekomst van journalistiek onderzoekswerk. Heeft de regering overwogen de regeling in artikel 27 voor de communicatie tussen advocaten en cliënten ook van toepassing te verklaren op journalisten? Waarom wel of niet? Welke andere oplossingsmogelijkheden heeft de regering overwogen, maar niet toegepast, om journalistieke bronbescherming nader te waarborgen?
De leden van de ChristenUnie-fractie constateren dat in artikel 27 de rechtbank Den Haag beoordeelt of gegevens terstond moeten worden

vernietigd. Hoe wordt dat precies bij de rechtbank vormgegeven? Gebeurt dat door een enkelvoudige of meervoudige kamer?
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. Waarom is een jaar nodig om verzamelde gegevens op hun relevantie te beoordelen? En hoe inhoudelijk is de relevantietoets die moet plaatsvinden?
De leden van de GroenLinks-fractie zijn positief over de uitzondering die in artikel 27 lid 2 is gecreëerd voor communicatie tussen advocaten en hun cliënten. Deze leden delen de mening van de regering dat een extra toets door de rechtbank op het gebruiken van deze gegevens op zijn plaats is. Wel vragen deze leden 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 lid 2 toe te voegen dat bij algemene maatregel van bestuur groepen kunnen worden aangewezen die tevens onder de regeling komen te vallen.

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. Wat zijn voorbeelden van de soort dreiging en de targetgroep die wel voldoende concreet zijn om te kunnen leiden tot toestemming en een positief rechtmatigheidsoordeel? Indien dergelijke voorbeelden niet gegeven kunnen worden, kan de regering dan op zijn minst de lijst van omschrijvingen die in ieder geval niet concreet genoeg zijn aanvullen? Deze lezen vragen dit bij voorkeur te doen aan de hand van daadwerkelijk afgewezen verzoeken om toestemming, waarbij ook enkele voorbeelden van aanvragen conform artikel 27 Wiv 2002 gegeven worden.
De leden van de D66-fractie merken op dat bij deze paragraaf over de inhoud van een verzoek om toestemming slechts summier ingegaan wordt op de afwegingen met betrekking tot de eisen van proportionaliteit en subsidiariteit. Deze leden hopen dat dit geen voorbode zal zijn van de uitvoeringspraktijk. Zij zijn ook benieuwd welke maatregelen getroffen zijn, en getroffen gaan worden, om aan de motivatie-eisen te kunnen voldoen. Dit te meer nu ten aanzien van de in de huidige Wiv 2002 opgenomen eisen, de CTIVD geregeld onrechtmatigheden en onzorgvuldigheden constateert, bijvoorbeeld ten aanzien van de kenmerken op de selectielijsten. Aangezien met het voorliggende wetsvoorstel naast de signal intelligence ook de cable intelligence wordt ingevoerd, en beide een vergelijkbare manier van werken kennen, wordt die vraag pregnanter, aldus deze leden. Zeker nu de regering verwijst naar de aanbevelingen uit het CTIVD-toezichtsrapport nr. 35 uit juli 2013, en het CTIVD-toezichtsrapport nr. 46 uit januari 2016. De CTIVD constateert dat eerdere kritiekpunten nog steeds van toepassing zijn. Graag verkrijgen deze leden een overzicht van alle door de jaren heen door de CTIVD gedane aanbevelingen om de inzet en toepassing van selectie bij Signals Intelligence (SIGINT) te verbeteren, en op welke manier daaraan opvolging gegeven is.

De leden van de SGP-fractie constateren dat de regering aangeeft dat de omschrijving van het doel van het vragen van toestemming voor gebruik van een bijzondere bevoegdheid zo concreet mogelijk moet zijn. Deze leden vragen zich af in hoeverre dit in alle gevallen zo concreet te geven

is. Moet aan alle in artikel 29 gestelde voorwaarden zijn voldaan? Is het ook mogelijk dat nog niet bepaalde concrete personen of samenwerkingsverbanden duidelijk zijn, maar dat wel bepaalde indicaties ervoor zijn dat er mogelijk sprake is van een dergelijk samenwerkingsverband? Is er dan sprake van een voldoende concrete targetgroep? Kan bijvoorbeeld bij een weliswaar concreet doel, maar waarbij de precieze personen nog onduidelijk zijn er toch sprake zijn van een verzoek dat ingewilligd kan worden?

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

De leden van de D66-fractie maken zich zorgen over de bescherming van verschoningsgerechtigden onder het voorliggende wetsvoorstel. Deze leden begrijpen niet goed waarom dit is beperkt tot advocaten en journalisten. De redenen waarom notarissen en hulpverleners als artsen en reclasseringsmedewerkers er niet onder vallen achten zij onvoldoende. Weliswaar kennen advocaten en journalisten een bijzondere rol in onze democratische rechtsstaat, dat neemt niet weg dat andere beroepsgroepen met een vertrouwensfunctie dat vertrouwen waar moeten kunnen maken. Alleen zo zal immers een reclasseringsmedewerker een mogelijk radicaliserende jongere op het rechte pad kunnen houden. Daar is vertrouwen voor nodig. Kan de regering, mede in het licht van de adviezen van de Koninklijke Notariële Beroepsorganisatie (KNB) en de Raad voor de Rechtspraak nader reflecteren op de arbitrair lijkende keuzes op dit punt?

Voor zover er wel bescherming voor journalisten is opgenomen, constaterende de leden van de D66-fractie dat deze nog enkele te dichten gaten kent. Het lid Verhoeven heeft daarvoor een amendement ingediend over de bescherming van de journalistieke bron (Kamerstuk 34 588, nr. 10). Allereerst betreft dat het bieden van dezelfde bescherming aan journalisten als aan advocaten voor zover gegevens verworven worden via de bijzondere bevoegdheden, anders dan wanneer zij direct doel van onderzoek waren en er dus voorafgaande rechterlijke toestemming is. Wat betreft deze leden moeten in beide gevallen de betreffende gegevens direct (terstond) vernietigd worden. Daarnaast valt het deze leden op dat, net als in het voorliggende wetsvoorstel in verband met de invoering van een onafhankelijke bindende toets voorafgaand aan de inzet van bijzondere bevoegdheden jegens journalisten welke gericht is op het achterhalen van hun bronnen (Kamerstuknummer 34027), ten nadele van de bronbescherming van journalisten wordt afgeweken van de door het Europees Hof voor de Rechten van de Mens (EHRM) gehanteerde definitie van een journalist. Zij vragen zich af waarom de regering persisteert in een andere definitie. Waarom maakt het uit of de gegevens ter openbaarmaking verkregen zijn, of dat het doel daar niet op lag, maar het er wel toe leidt? Als informatie door de bron verstrekt worden ter achtergrond, maar ze uiteindelijk wel leiden tot een verhaal of zelfs daarin opgenomen wordt, is dat toch ook beschermen waardig, zo vragen de leden van de D66-fractie?

De leden van de D66-fractie zouden graag nadere informatie willen hebben over waarom een systeem van «nummerherkenning» niet mogelijk zou zijn. Enerzijds beroept de regering zich op het argument dat het niet technisch mogelijk is, anderzijds dat het onwenselijk is in het kader van de nationale veiligheid op voorhand communicatie uit te sluiten. Dat wekt de indruk dat de argumenten tegen het invoeren ervan gezocht worden bij het «standpunt», in plaats van dat gekeken wordt hoe een dergelijk technisch uitsluiten van het aftappen van verschoningsgerechtigden zonder toestemming geregeld kan worden. Kan de regering uitsluiten dat dit het geval is? Welke technische mogelijkheden zijn onderzocht? Hoe zijn die gewogen? En welk overleg met welke uitkomsten is er geweest met bijvoorbeeld de Nederlandse Orde van Advocaten?

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. De leden van de SGP-fractie vragen of een nadere duiding gegeven kan worden. Hoe ver reikt het begrip journalist zich precies? Geldt het ook voor personen die incidenteel een journalistieke productie leveren? Geldt het ook voor personen die bijvoorbeeld via een blog op internet werken? Vraagt de rechtszekerheid niet om ten minste een nadere duiding van de criteria die gelden?

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 zich af 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. Op welke wijze is de regering voornemens daar zoveel mogelijk openheid in te betrachten?

3.3.2 Toetsingscommissie inzet bevoegdheden (§3.3.3 m.v.t.)
De leden van de VVD-fractie vragen of de regering de vrees die bij sommigen bestaat dat de TIB een geheime rechtbank dreigt te worden kunt wegnemen.
Ook vragen deze leden of de regering kan reageren op de vrees dat de TIB onderbedeeld is en over te weinig know how, kennis en kunde beschikt. Kan de regering een toelichting geven op de onafhankelijkheid van de TIB? Hoe wordt voorkomen dat bijvoorbeeld over een paar jaar weer twijfel gaat ontstaan over de onafhankelijkheid van de TIB, waardoor weer een nieuw orgaan in het leven geroepen zou moeten worden om de TIB te controleren?

De leden van de SP-fractie vragen de regering waarom er voor gekozen is de toetsingscommissie alleen een marginale toets vooraf te laten doen op de inzet van de bijzondere bevoegdheden. Daarnaast vragen deze leden waarom er voor gekozen is drie mensen in deze commissie te benoemen die niet noodzakelijk een achtergrond hebben in of een gedegen kennis hebben van de werking van de diensten, te meer daar zij geen rechtstreekse toegang hebben tot gegevens van de AIVD of de MIVD. Daarnaast vragen deze leden waarom specifiek is gekozen voor een commissie van drie mensen.
De leden van de SP-fractie vragen de regering nader in te gaan op de kritiek van de Raad van State die vraagt hoe de verhouding tussen de TIB, als toetser vooraf, en de CTIVD, als toetser achteraf, vorm gegeven wordt. Ziet de regering ook dat hier spanningen kunnen ontstaan?

De leden van de CDA-fractie merken op dat de Afdeling advisering van de Raad van State van oordeel is dat de toetsing door de TIB in de praktijk zal neerkomen op een zeer marginale en abstracte rechtmatigheidsbeoordeling ex ante. De Afdeling stelt dat er zo afbreuk wordt gedaan aan de ministeriële verantwoordelijkheid voor het handelen van de diensten. De leden van de CDA-fractie vragen de regering nader in te gaan op het vraagstuk van de ministeriële verantwoordelijkheid voor de diensten en de parlementaire controle daarop.
Voorts constateren deze leden met de Afdeling, dat het naast elkaar bestaan van de TIB en de CTIVD de vraag oproept hoe de werkzaamheden van beide organen op elkaar moeten worden afgestemd. De CTIVD constateert dat het voorliggende wetsvoorstel niet voorziet in waarborgen ten behoeve van uniforme en consistente rechtstoepassing, de rechtseenheid. Het in dit wetsvoorstel beschreven systeem van voorafgaande toestemming (Minister) en toetsing (TIB of rechter) en van toezicht en klachtbehandeling achteraf (CTIVD), karakteriseert de CTIVD als gelaagd

en complex. Op welke wijze wordt uniforme en consistente rechtstoepassing in de nieuwe wet geborgd, zo vragen de leden van de CDA-fractie.

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 deze leden zorgen over de toerusting van de nieuw in te stellen TIB. Zij vragen de regering een onderbouwing 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.
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.
Voorts vragen de leden van de GroenLinks-fractie waarom de regering ervoor heeft gekozen om het oordeel van de CTIVD bij de toetsing achteraf niet bindend te laten zijn. Deze leden vragen de regering 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.
De leden van de GroenLinks-fractie vragen 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.

De leden van de SGP-fractie begrijpen de achtergrond van de instelling van de TIB. Toch vragen deze leden zich af of dit niet teveel vertragend werkt. Aan de ene kant zal een dergelijke instantie om de taak serieus te nemen voldoende zicht moeten hebben dat er in een bepaald concreet geval sprake is van terechte inzet van bevoegdheden, wat vertragend kan werken. Aan de andere kant zal ook voorkomen moeten worden dat de zelfstandige verantwoordelijkheid van de Minister wordt uitgehold door een zeer uitvoerige toetsing door deze commissie die ook nog eens bindend is. Graag ontvangen deze leden een nadere beschouwing op de vraag hoe beide gevaren worden voorkomen.
De TIB moet zo spoedig mogelijk een oordeel uitbrengen over het uitoefenen van een bepaalde bevoegdheid. De leden van de SGP-fractie vragen of een indicatie te geven is van de termijn die hierbij beoogd wordt.
Het valt deze leden op dat er via artikel 99 een algemene bepaling is opgenomen over de verenigbaarheid van functies. Hier is geen nadere duiding aan gegeven anders dan dat de leden van de toetsingscommissie geen onderdeel uit mogen maken van de CTIVD en andersom. Zij vragen zich af of bijvoorbeeld iedere rijksambtenaar gezien moet worden als per definitie niet geschikt voor de invulling van deze functie. Geldt dit bijvoorbeeld ook voor bijvoorbeeld burgemeesters of commissarissen van de Koning?
De commissie bestaat uit drie personen die voor een periode van zes jaar (met de mogelijkheid van verlenging) worden benoemd. Betekent dit dat mogelijk na zes of na twaalf jaar de drie vacatures tegelijkertijd vrijkomen? Is dit gewenst? Moet er niet worden gekozen voor een verschillende termijn om de kwaliteit te handhaven en overdracht beter mogelijk te maken? Begint na een vervanging de periode van zes jaar opnieuw te lopen?
Bij de invulling van het secretariaat wordt niet de eis gesteld dat er sprake moet zijn van bijvoorbeeld onpartijdigheid en onafhankelijkheid. In

hoeverre gelden deze eisen ook voor de bemensing van het secretariaat? En geldt dit ook ten aanzien van de eis van de Nederlandse nationaliteit?

3.3.2.1 Algemeen (§3.3.3.1 m.v.t.)

De leden van de D66-fractie waarderen het dat de regering het verzet tegen een onafhankelijke en bindende toets vooraf aan het inzetten van bijzondere bevoegdheden die een ingrijpende inbreuk maken op de persoonlijke levenssfeer gestaakt heeft. Het doet hen evenwel verwonderden hoe zich dit verhoudt tot de eerder gestelde zorg dat daarmee geen invulling meer gegeven kan worden aan de ministeriele verantwoordelijkheid. Op welke wijze acht de regering die verantwoordelijkheid onder het voorgestelde systeem tot uiting te laten komen?
Deze leden lijken voorts uit het tweede argument voor een dergelijke toets op te maken dat de regering nog steeds niet geheel achter de invoering van de TIB staat, maar zij dit er omwille van het draagvlak voor het voorliggende wetsvoorstel wel onderdeel van hebben uitgemaakt. Klopt die indruk? Op welke wijze moet dat vertrouwen scheppen dat de verantwoordelijke ministers er straks op een goede en constructieve wijze mede zorg voor gaat dragen dat de TIB snel gezag en kennis opbouwt om goed en geloofwaardig te kunnen toetsen?

De leden van de ChristenUnie-fractie constateren dat de Raad van State ernstige twijfels heeft geuit over de effectiviteit van het toezicht zoals dat nu over het TIB en de CTIVD is verdeeld. In een open brief noemen 29 wetenschappers het toezicht «buitengewoon rommelig» georganiseerd. Deze leden constateren eveneens dat er een vrij onoverzichtelijke toezichts- en controle structuur ontstaat met betrokkenheid van het TIB, de CTIVD, het parlement, de CIVD en de rechtspraak. Welke scenario's zijn voor het toezicht allemaal door de regering overwogen? En welke vielen af en om welke redenen?
De leden van de ChristenUnie-fractie vragen of de regering heeft overwogen het toezicht vooraf zoveel mogelijk neer te leggen bij een college van gespecialiseerde rechters, met een formele inbedding in de rechterlijke macht. Wat vindt de regering van de suggestie van de eerder genoemde 29 wetenschappers om ook een «public advocate» aan te stellen binnen de toezichtstructuur?

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

Het is de leden van de PvdA-fractie niet duidelijk of de TIB steeds als college beslist, dan wel of ook individuele leden van de TIB kunnen beslissen. De Raad voor de Rechtspraak wijst ook op onduidelijkheid ten aanzien van de mogelijkheid om plaatsvervangende leden te benoemen. Kunt de regering daar op ingaan? Tevens vraagt de Raad op het belang om «inkapseling» van de leden van de TIB te voorkomen. De Raad acht het om die reden van belang «dat wordt vastgesteld dat de leden niet kunnen worden herbenoemd». De Raad heeft meerdere vragen over de omvang van de werkzaamheden, de vormgeving en de bemensing van de TIB. Kunt u hier de leden van de PvdA-fractie meer helderheid over bieden?
Uit de hoorzitting in de Kamer en de position papers daarbij hebben bij de leden van de PvdA-fractie enkele vragen opgeroepen ten aanzien van de TIB. Op grond van het voorliggend wetsvoorstel moet de door de Minister verleende toestemming aan de dienst om een bevoegdheid te gebruiken aan de TIB ter beoordeling wordt voorgelegd. De TIB heeft echter geen rechtstreekse toegang tot de gegevens bij één van de diensten. Dat wordt door de regering niet nodig geacht omdat, zo begrijpen deze leden, de TIB alleen op rechtmatigheid toetst. Toch delen deze leden de zorgen van de Raad voor de Rechtspraak op dit punt en vragen zij zich af toezicht vooraf door de TIB wel effectief kan zijn. Hoe kan de TIB aan de hand van het

verzoek van de dienst en de toestemming van de Minister opmaken of er terecht gebruik is gemaakt van die bevoegdheid? Beschikt de TIB daarvoor wel over voldoende informatie? Bovendien, zo vragen deze leden in navolging van de Raad voor de Rechtspraak en de Afdeling zich af, beschikt de TIB wel over voldoende kennis en een adequaat apparaat om de toetsing ook effectief te kunnen uitvoeren? Zo ja, waar blijkt dat uit? Zo nee, waarom niet en hoe gaat u hier alsnog in voorzien? De Raad voor de Rechtspraak doet de suggestie om de TIB als zelfstandige en onafhankelijke commissie binnen de CTIVD te positioneren. Kunt u ook hier op ingaan?

De leden van de D66-fractie vragen zich af 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. De leden van de D66-fractie vragen zich af aan wat voor expertise gedacht wordt voor het derde lid van de TIB. Op welke wijze wordt ICT-kennis geborgd bij deze leden? Zij 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?

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. Zijn er nota's beschikbaar waarin de bevoegdheden volgens die meetlat geordend zijn en waarbij gekeken is welke bevoegdheid daar wel en niet onder moest vallen? Zo ja, zijn deze voor de Kamer beschikbaar? Zo nee, hoe heeft die weging dan wel plaatsgevonden?
De leden van de D66-fractie zijn benieuwd hoe de oordeelsvorming binnen de TIB plaats zal gaan vinden. In de toelichting wordt gesteld dat de voorbereiding van het oordeel over een ter toetsing voorgelegd besluit door de TIB kan worden neergelegd bij één van haar leden, maar dat de TIB uiteindelijk het oordeel vaststelt. Deze leden zien echter in de artikelen onder paragraaf 3.2.2.2 van de memorie van toelichting de toetsing door de TIB niet expliciet opgenomen. Kan de regering desondanks verzekeren dat altijd van een besluit van de gehele TIB sprake zal zijn? Moet dat voorts een unaniem besluit zijn of mag dat ook een meerderheidsbesluit zijn?
De leden van de D66-fractie zouden graag nader in willen gaan op de oordeelsvorming binnen de TIB. Deze commissie heeft immers geen volledige toegang tot de systemen van de diensten, hetgeen de CTIVD wel heeft. De TIB zal dus – net als de Minister – moeten afgaan op de informatie zoals opgenomen in het verzoek om toestemming en zo nodig de onderliggende meegestuurde documenten. Voor zover de TIB behoefte heeft aan het inwinnen van nadere informatie, welke ruimte gaat de regering haar bieden? Hoe kan het horen van deskundigen – in geval de TIB twijfelt over noodzaak, proportionaliteit en subsidiariteit – met inachtneming van de benodigde vertrouwelijkheid en snelheid worden vormgegeven? Voorts vragen deze leden zich af of het voor haar oordeelsvorming over de ingezette bevoegdheden conform de artikelen 53, 54 en 57, onder omstandigheden niet verstandig zou kunnen zijn om de aanbieders van communicatiediensten te horen. Deze leden zijn benieuwd welke ruimte hiertoe bestaat.
De leden van de D66-fractie kennen voorbeelden waarin een toetsingsrechter verworden was tot stempelmachine. Het Amerikaanse FISA-Court is wellicht de meest bekende illustratie daarvan. Dat moet in de Nederlandse context voorkomen worden, aldus deze leden. Een aanknopingspunt daarvoor is het tegenspraak-principe zoals verwoord door Eskens, Van Daalen en Van Eijk in Ten Standards for oversight and

transparency of national intelligence services van het Instituut voor Informatierecht. Deze leden vragen zich af hoe binnen de toetsing van de TIB een dergelijke publieksadvocaat ingepast zou kunnen worden, waarom een dergelijk persoon niet is opgenomen in het voorliggende wetsvoorstel, wat daartoe de overwegingen geweest zijn en welke ervaring c.q. achtergrond voor een dergelijke functie vereist zou zijn, inclusief de met de inzet van deze persoon samenhangende kosten.
De leden van de D66-fractie begrijpen dat er een voorziening is voor het in het geval van onverwijlde spoed inzetten van een bevoegdheid alvorens daar toestemming toe verkregen is. Deze leden maken zich zorgen dat de gevolgen van een onterecht beroep op deze voorziening niet in de wet vastgelegd zijn, maar ter oordeel 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 TIB. Waarom is er niet voor gekozen dat alle verworven gegevens terstond vernietigd moeten worden, dat eventuele verwerkingen ongedaan moeten worden gemaakt en analyses voor zover gemaakt op grond van die verwerving en/of verwerking voor dat deel ongedaan gemaakt moeten worden, ongeacht of de inzet onrechtmatig was, of dat enkel de betoonde haast dat was? In beide gevallen hadden deze gegevens immers niet verworven kunnen worden bij het volgen van de wet, en een dergelijk ontduiken ervan zou niet beloond mogen worden. De leden van de D66-fractie verkrijgen hierop graag nadere reflectie van de regering, inclusief de exacte motivatie om niet wettelijk uit te sluiten dat de diensten beloond kunnen worden voor het omzeilen van de wet.

De leden van de ChristenUnie-fractie vragen of de regering meent dat het TIB straks toegang heeft tot alle relevante informatie die nodig is om tot een goed en onafhankelijk advies te kunnen komen. Zo ja, op welke gronden? En wat vindt de regering ervan dat veel experts menen dat dit niet het geval is?
De leden van de ChristenUnie-fractie vragen op welke wijze en in welke mate informatie over het voorafgaande toezicht openbaar gemaakt zal worden. Wordt het aantal afgewezen en toegewezen verzoeken tot toestemming openbaar gemaakt?

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. Dat roept bij hen enkele vragen op. Zoals de regering ongetwijfeld weet, is niet alles wat op het internet staat waar. Wanneer Kamerleden zichzelf bijvoorbeeld googelen wordt dit snel duidelijk. Op welke wijze wordt dan 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. Een social media-profiel zal vaak niet open ten aanzien van een ieder zijn, maar zodra een vriendschaps- of volgverzoek geaccepteerd is, dat wel zijn ten aanzien van die personen. In de memorie van toelichting is reeds aangegeven dat het inzetten van een profiel of hoedanigheid teneinde toegang te verkrijgen tot een besloten deel van een openbaar sociaal medium altijd beschouwd zal worden als de inzet van een agent, inclusief het daarbij horende waarborgenkarakter. Maar als men als gevolg van een hack op een geautomatiseerd werk of het aftappen van communicatie het

wachtwoord van zo'n profiel op social media verkrijgt, en de bron daarmee «open» ligt, valt dat dan ook onder deze bevoegdheid? De leden van de D66-fractie nemen aan van niet, maar willen hieromtrent graag zekerheid. Hoe valt bovendien deze bevoegdheid tot het stelselmatig verzamelen van gegevens over personen uit open bronnen te vergelijken met artikel 40, dat het observeren en volgen van personen regelt? In welke gevallen kunnen wel stelselmatig gegevens verzameld worden over een persoon zonder dat dit tot de observatie- en volgwaarborgen leidt? In hoeverre is gerechtvaardigd dat voor beide bevoegdheden dezelfde waarborgen gelden, terwijl met het verzamelen uit open bronnen niet enkel een beeld over het «nu» verworven kan worden, maar ook over «het verleden»?
De leden van de GroenLinks-fractie constateren dat in het voorliggende wetsvoorstel wordt geregeld dat de Minister toestemming dient te verlenen voor het raadplegen van informatie uit openbare bronnen door de Minister. Hoewel deze leden het uitgangspunt delen dat het op langere termijn volgen en opslaan van openbaar gepubliceerde informatie een impact kan hebben op de privacy van personen, vragen deze leden zich af 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. In dit kader vragen deze leden naar een inschatting van behaalde efficiëntie in de werkzaamheden van de diensten indien de ministeriële toets voor deze bevoegdheid wordt geschrapt, alsmede de juridische houdbaarheid hiervan in relatie tot de in de memorie van toelichting genoemde uitspraken van het EHRM.

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

De leden van de D66-fractie begrijpen uit het voorliggende wetsvoorstel 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 dat 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? Een grote communicatiedienstaanbieder zal mogelijk een dergelijk verzoek tot geautomatiseerde toegang weigeren, maar in welke positie staan kleinere of deels van de overheid afhankelijke aanbieders van die diensten?
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?

De leden van de GroenLinks-fractie constateren dat in artikel 39 de bevoegdheid wordt gecreëerd voor de diensten om zich op verzoek rechtstreekse toegang te verschaffen tot de geautomatiseerde gegevensbestanden van bestuursorganen en andere organisaties. Het verbaast deze leden dat deze nieuwe, verregaande bevoegdheid voor de regering geen aanleiding heeft gevormd om dit aan te merken als bijzondere bevoegdheid, en daarmee het toezicht op deze bevoegdheid adequaat te organiseren. Het gaat hier immers mogelijk om bijvoorbeeld opgeslagen DNA-gegevens, ziekenhuisgegevens of gegevens bij scholen, gegevens van een zeer persoonlijke en vertrouwelijke aard. Deze leden verzoeken de regering deze keuze nader te onderbouwen.

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 kunnen zich niet aan de indruk onttrekken dat dit wel is gepoogd, maar niet geheel is gelukt. Nog steeds geldt immers dat de waarborg primair gelegen is in een toets op de inzet van een bevoegdheid, waarbij de zwaarte van de toets gekoppeld is aan de mate waarin – met de huidige technische toepassingen – er een inbreuk op de persoonlijke levenssfeer is. Een voorbeeld: geautomatiseerde werken hebben de afgelopen 10 tot 20 jaar een geheel andere rol in onze samenleving gekregen, en die verandering zet zich door. Wie in 1995 een computer binnendrong, vond geheel andere – en veel minder gedetailleerde en persoonlijke – informatie dan wie nu een smartphone binnendringt. Het valt niet uit te sluiten dat binnen eenzelfde periode in de toekomst met het binnendringen van een geautomatiseerd werk ook de nu nog overwegende analoge aspecten van ons leven, zoals gezondheid, seksueel leven en eetpatroon, tot in detail zijn na te gaan. Toch zit er geen expliciete bepaling in het voorliggende wetsvoorstel waardoor de waarborg automatisch meestijgt met de indringendheid van de bevoegdheid. De leden van de D66-fractie verkrijgen daarom graag 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 enige waarborg die het wetsvoorstel in dat opzicht lijkt te bevatten is een verscherpte toets op noodzaak, subsidiariteit en proportionaliteit, klopt dat? Zijn er dan bijvoorbeeld technische hulpmiddelen, al dan niet aan het internet gekoppeld, waarvan de regering bereid is op voorhand het hacken of aftappen ervan uit te sluiten? Deze leden denken bijvoorbeeld aan een pacemaker.

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. Daarbij was het oordeel dat dit in beginsel rechtmatig was, maar ermee wel een substantiële en vergaande inbreuk gemaakt kan worden op de persoonlijke levenssfeer. In dit geval is de Kamer vertrouwelijk geïnformeerd door de CTIVD over deze onderzoeksmethode, maar het verdient de vraag 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 (Kamerstuk 34 588, nr. 9). Deelt de regering het uitgangspunt 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? Indien een van deze vragen met nee beantwoord wordt, waarom niet?

De leden van de D66-fractie tellen een behoorlijk aantal bevoegdheden waarvoor ministeriele toestemming vereist is alvorens zij ingezet kunnen worden. In hoeverre is het reëel om aan te nemen dat de betrokken Minister ook daadwerkelijk een grondig, verantwoord en overwogen oordeel kan vormen over al deze lasten? Hoeveel tijd besteedt de betrokken Minister daar onder de huidige wet wekelijks aan? Hoeveel toelichting en motivering kennen die verzoeken? Hoeveel fte's zijn er binnen de betreffende ministeries aangewezen om de Minister te

ondersteunen in zijn of haar toestemmingsoordeel? Hoe heeft het aantal verzoeken om ministeriele toestemming zich de afgelopen jaren ontwikkelt? Voor hoeveel bevoegdheden moet de betrokken Minister op dit moment persoonlijke toestemming verlenen, en voor hoeveel bevoegdheden zal dat straks het geval zijn? Zijn er bevoegdheden waar de Minister nu zelf nog toestemming verleent, maar waarbij dat onder het voorliggende wetsvoorstel gemandateerd zal worden aan het hoofd van de dienst? Graag verkrijgen deze leden hierop antwoord ten aanzien van zowel de Minister van Binnenlandse Zaken en Koninkrijksrelaties, als de Minister van Defensie.

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. Daarbij achten deze het begrijpelijk dat nu wettelijk geregeld is dat bestuursorganen zo nodig verplicht kunnen worden daaraan mee te werken. Wel hebben deze leden een vraag welke identiteiten en hoedanigheden aangenomen mogen worden. Wanneer deze identiteit geheel, deels of overwegend samenvalt met een bestaand persoon, kan dat die persoon schade berokkenen. Wordt weleens een bestaande identiteit aangenomen? Zo nee, 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?

De leden van de SP-fractie vragen de regering nader in te gaan op de bevoegdheid om gebruik te maken van agenten. Waarom is in dit wetsvoorstel niet gekozen om journalisten en hulpverleners uit te zonderen van een rol als agent? Waarom is de regering het niet met deze leden eens dat hun rol in de maatschappij zich niet goed verhoudt tot een rol als agent, vanwege hun rol als onafhankelijk controleur van de macht? Waarom deelt de regering niet de opvatting van deze leden dat vooral in het buitenland – en zeker in oorlogsgebieden – in het geval van ontmaskering van dit soort agenten andere journalisten of hulpverleners in gevaar zou kunnen brengen?

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.)

Bij DNA-onderzoek, zo lezen de leden van de SP-fractie, is niet gekozen voor een actieve notificatieplicht. Deze leden vragen de regering deze keuze nader toe te lichten. Daarnaast vragen deze leden waar zij aan moeten denken bij het terugplaatsen van een voorwerp dat DNA-materiaal bevat.

De leden van de D66-fractie constateren dat het voorliggende wetsvoorstel een expliciete basis gaat bieden voor het verrichten van DNA-onderzoek aan celmateriaal gericht op het vaststellen en de verificatie van de identiteit van een persoon. Daarmee wordt tegemoet gekomen aan CTIVD toezichtsrapport nr. 42, waarin geconcludeerd wordt dat hiervoor een expliciet wettelijke basis nodig is. Evenwel vragen deze leden of aan alle aanbevelingen in de volle breedte is voldaan. Waar de CTIVD aanbeveelt om in de regeling waarborgen op te nemen voor gebruik en toegang van derden, zijn deze in het wetsvoorstel procedureel van aard, namelijk de betrokken Minister moet toestemming verlenen. Welke materiele waarborgen bestaan er? Verder moeten in de wet waarborgen ten aanzien van de procedures voor het behoud van integriteit en vertrouwelijkheid van de data opgenomen zijn. In het

voorliggende wetsvoorstel krijgt dat vorm door middel van een voorgehangen algemene maatregel van bestuur. Daarmee is op moment van stemming over dit wetsvoorstel echter nog niet duidelijk of aan de waarborgen voldaan zal zijn. Bovendien betreft de voorhang slechts een lichte waarborg, want de Kamer heeft geen recht tot blokkeren. De leden van de D66-fractie zijn daarom benieuwd naar de voorgenomen inhoud van deze regeling. Kunnen de inhoudelijke hoofdpunten alvast gedeeld worden ten behoeve van de behandeling van het voorliggende wetsvoorstel? Zo nee, waarom niet? Mede gegeven de aanbevelingen in de PIA ten aanzien van de noodzaak van de DNA-databank achten deze leden dat van grote waarde.
De leden van de D66-fractie zijn benieuwd naar waarom gesteld wordt dat de resultaten van onderzoek naar vingerafdrukken in de praktijk niet altijd bruikbaar zijn. In welke gevallen is dit niet nuttig gebleken? Hoe verhoudt zich dat tot andere vormen van onderzoek aan een voorwerp, gericht op de vaststelling van de identiteit van een persoon (artikel 42, eerste lid, aanhef en onder c)? Gegeven het wel in dit wetsvoorstel opnemen van een bevoegdheid tot DNA-onderzoek vragen deze leden zich af in hoeverre de problemen bij vingerafdrukonderzoek ook aanwezig zijn bij DNA-onderzoek. Betreft het bijvoorbeeld de betrouwbaarheid van het sample? Hoe wordt zeker gesteld dat de vingerafdruk respectievelijk het DNA afkomstig is van de persoon waarvan wordt vermoed c.q. wordt gehoopt dat het deze persoon is? In hoeverre bestaat bij DNA in verhouding tot vingerafdrukken de mogelijkheid een vals spoor met het materiaal van een ander achter te laten? Hoe wordt dat in dit wetsvoorstel ondervangen?
De leden van de D66-fractie vragen hoe het vierde en vijfde lid van artikel 42 zich tot elkaar verhouden. Waarom is ervoor gekozen dit in twee afzonderlijke leden onder te brengen?
De leden van de D66-fractie vragen zich in het kader van de bevoegdheid tot het meenemen van objecten uit doorzochte plaatsen af, hoe het redelijk belang omtrent terugplaatsing van dat object gewogen wordt. Dat een meegenomen sigarettenpeuk of haar niet hoeft te worden teruggeplaatst, is evident. Maar wat moet wel worden teruggeplaatst? «Het met terugplaatsing geen redelijk belang dienen» roept immers twee vragen op. Wat is een redelijke inspanning tot terugplaatsing in dit kader en wiens belang moet dit dienen? Gaat het in dat laatste geval dan om het belang van één van de diensten, degene van wie het object is, de eigenaar van de woning waaruit het gehaald is, de omgeving van de betreffende persoon (in familiaire of fysieke zin) of een willekeurig ander persoon? In welke gevallen kan voorts het redelijk belang tot terugplaatsing zodanig sterk zijn dat het risico op verstoring van de goede taakuitvoering op de koop kan worden toegenomen?

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. Deze leden 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. 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.

De leden van de SGP-fractie vragen naar het onderscheid tussen het doorzoeken van besloten plaatsen en het doorzoeken van gesloten

voorwerpen. Uit de toelichting blijkt bijvoorbeeld dat het openen van een kast ook valt binnen de definitie van het doorzoeken van gesloten plaatsen. Kan worden gesteld dat er, zodra er sprake is van het verbreken of stukmaken er sprake is van het doorzoeken van gesloten voorwerpen? Valt bijvoorbeeld het openen van een kast waar de sleutel in zit onder het doorzoeken van een besloten plaats (artikel 42, onder a) en het openen van een kast die opengebroken dient te worden onder het doorzoeken van gesloten voorwerpen (artikel 42, onder b)? Want wat is immers anders het verschil tussen het openmaken van een kast en het openmaken van een koffer als beide voorwerpen niet op slot zitten?
Er is ook een specifieke bepaling opgenomen voor het verrichten van DNA-onderzoek. De leden van de SGP-fractie vragen hoe de termijn van bewaren van vijf jaar zich verhoudt tot de termijn van drie maanden waarbinnen het onderzoek plaats dient te vinden. Betekent dit dat het bewaarde DNA-materiaal weliswaar opnieuw gebruikt mag worden, maar pas na een nieuwe toestemming? Waarom is hiervoor gekozen?

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 enkele vragen over de praktische uitwerking van het voorgenomen artikel 44. Indien één van de diensten vraagt om een zending uit te leveren, geldt daarvoor zowel een medewerkingsplicht als een geheimhoudingsplicht? Tegelijkertijd zijn de meeste pakketjes tegenwoordig met een track&trace-systeem van minuut tot minuut te volgen. Zodra een pakket even stilligt, kan een consument dat dus zien. Wat is de verwachte benodigde tijd die nodig is alvorens het pakket aan de vervoerder geretourneerd wordt? Voor zover dat te lang zou zijn, en de ontvanger van het pakket reeds contact heeft opgenomen om te vragen waar het pakket blijft of – bij gebreke aan zending – een vervangende levering aanvraagt, wordt dan niet het vervoersbedrijf benadeeld? Deze zal immers of zelf of via de verzekering bij de verzender de kosten voor de vervangende levering moeten aanvragen. Op welke wijze zal daarvoor compensatie plaatsvinden? Of ziet de regering andere wegen voor postvervoerders om zonder dit risico aan de geheimhoudingsplicht te voldoen?

De leden van de SGP-fractie constateren dat bij het openen van brieven (artikel 44) toestemming van de rechter is vereist. Bij het binnendringen in geautomatiseerde werken (artikel 45) is dit niet het geval. Kan worden toegelicht wat de verklaring voor dit verschil is?

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 lichaam wordt aangetast. Zijn de bevoegdheden in het voorliggende wetsvoorstel beperkt tot het inzetten van technische hulpmiddelen buiten het lichaam?

De leden van de PvdA-fractie hebben begrepen dat het mogelijk moet worden dat de bevoegdheid tot verkennen van en binnendringen in geautomatiseerde werken ook gebruikt gaat worden ten aanzien van derden. Hoe dat begrip «derde» moet worden begrepen is deze leden niet geheel duidelijk. Betreft dat een derde waarbij er sprake is van een directe technische band met het target? Of kunnen er tussen het target en de derde nog veel schakels zitten? En zo ja, hoeveel schakels dan? Deelt de regering de mening dat het begrip «derde» niet zover mag worden opgerekt dat daarmee in feite bij alles en iedereen gehackt zou kunnen gaan worden? Zo ja, hoe gaat de regering dit begrip nader inkaderen? Zo nee, waarom deelt de regering die mening niet?

De leden van de PvdA-fractie lezen dat artikel 48, eerste lid, van het wetsvoorstel, dat tot de bevoegdheid op grond van dit artikel ook de bevoegdheid wordt gerekend «tot het ongedaan maken van de versleuteling van de telecommunicatie of gegevensoverdracht». Met het oog de berichtgeving dat de AIVD reeds bezig is met het doorbreken van de encryptie van Whatsapp vragen deze leden zich af op basis van welke bestaande wettelijke grondslag dit nu al gebeurt. Wat zijn de huidige bevoegdheden ten aanzien van decryptie en hoe gaan die wijzigen? Hoeveel van het kabelgebonden verkeer is op dit moment naar schatting versleuteld? En deelt de regering de verwachting 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? Kan versleutelde data zonder dat die ontsleuteld wordt toch nog van nut zijn voor de diensten, bijvoorbeeld om metadata te analyseren?
Kan worden gegarandeerd dat de diensten zo gericht mogelijk zullen werken en niet middels decryptie de digitale veiligheid van grote groepen gebruikers zullen ondermijnen? En hoe wordt dit gegarandeerd, zo vragen de leden van de PvdA-fractie.

De leden van de SP-fractie vragen de regering waarom het voorliggende wetsvoorstel techniekneutraal is geformuleerd. Deze leden lezen dat dit is gedaan vanuit het oogpunt een toekomst vaste regeling te bewerkstelligen. Deze leden vragen de regering of zij hierin hebben meegenomen dat technologie zich bijzonder snel ontwikkelt en steeds meer persoonlijke data van mensen wordt opgeslagen. Het is zeer goed voorstelbaar dat in de nabije toekomst de techniek nog veel verder gaat dan nu het geval is. Wat als lichaamsgebonden technologie als smartbrillen, smartwatches of andersoortige chips (kunnen) worden geïntegreerd in het lichaam? Is de regering dan nog steeds voorstander van deze toekomst vaste regeling? Ziet de regering ook andere ethische bezwaren dan alleen de schending van de privacy? Heeft de regering nagedacht om voor dit soort nieuwe technieken een uitzonderingsbepaling op te namen? Zo nee, waarom niet? Zo ja, wat waren de overwegingen, los van een toekomst vaste regeling, om dat niet op te nemen? Hoe wordt de Kamer op de hoogte gesteld van het gebruik van nieuwe technologieën die nu nog niet zijn te voorzien? Verder lezen de leden van de SP-fractie over het binnendringen van een geautomatiseerd werk van een derde. Daar stelt de regering dat er malware aangebracht kan worden in het werk van een derde om zo bij de gegevens van het target te komen. Begrijpen deze leden goed dat dit een bewuste verzwakking betekent van de digitale veiligheid van het geautomatiseerde werk van een derde? Ziet de regering ook de bezwaren hiertegen, omdat met deze verzwakking ook andere belanghebbenden van deze verzwakking gebruik kunnen maken? Hoe wordt de veiligheid van een derde in dat geval gewaarborgd? Deze leden vragen de regering nader in te gaan op de vraag wat en wie precies onder een derde worden verstaan. Waarom is er geen verplichting opgenomen dat de derde gewezen wordt op de zwakheid in het systeem, eventueel na de hack, om het systeem veiliger te kunnen maken?

De leden van de D66-fractie vragen of de regering nader kan toelichten wat «een technisch gerelateerde partij» precies inhoudt in het kader van het hacken via een derde. Deze leden delen de kritiek die de CTIVD uitte op het voorgestelde hack-stelsel. Het lid Verhoeven heeft daartoe een amendement ingediend over binnendringen met een valse hoedanigheid (Kamerstuk 34 588, nr. 8), om enkele verbetervoorstellen van de CTIVD in het voorliggende wetsvoorstel te verankeren. Gegeven de mogelijkheid om via een derde een geautomatiseerd werk binnen te dringen, roept bij de leden van de D66-fractie de vraag op hoeveel stappen je daartoe mag

zetten. De minste voorwaarden voor het gericht toepassen van deze bevoegdheid lijkt wel het hebben van een directe technische relatie tussen beide geautomatiseerde werken te zijn en dat het gebruik maken van een derde voorkomt uit noodzaak, niet uit gemakzucht. Deze leden zouden graag van de regering vernemen hoe zij de hiervoor geformuleerde criteria in de praktijk zal gaan invullen.
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. Zo ja, hoe wordt dan invulling gegeven aan de invulling van de verzoeken tot inzet? Beide vereisen een voorafgaande instemming van de TIB, maar deze leden kunnen zich voorstellen dat het afwegingskader toch anders ligt, al is het alleen maar omdat ten aanzien van het binnentreden in een woning zonder medeweten van de bewoner een actieve notificatieplicht bestaat op grond van artikel 59, maar niet voor het binnendringen in een geautomatiseerd werk. Als deze bepalingen zouden samenlopen, moet dan voor elke woning waar betreffende gehackte smartphone waarbij de microfoon is afgeluisterd, een dergelijke notificatie plaatsvinden? Hoe wordt voorts bepaald of überhaupt op het moment van meeluisteren/meekijken men zich in een woning bevindt, zo ja welke? Indien de GPS aanstaat, zal dit mogelijkerwijs nog gemakkelijk te bepalen zijn, maar hoe gebeurt dat bij telefoons waarvan die functie niet (onopgemerkt) aan valt te zetten?
De leden van de D66-fractie constateren dat de regering van mening is dat «bij onderzoek naar cyberaanvallen […] het van belang is om hetzelfde gereedschap te hebben als de digitale aanvaller». Kan de regering nader toelichting wat zij bedoelt met «hetzelfde gereedschap»? Bedoelt de regering hiermee kennis over dezelfde softwarekwetsbaarheden die gebruikt worden in een cyberaanval, of bedoelt de regering dezelfde mogelijkheden om te hacken via al dan niet bekende softwarekwetsbaarheden? Waarom is dit gereedschap nodig om cyberaanvallen te kunnen onderkennen?
Voorts constateren de leden van de D66-fractie dat de regering, in tegenstelling tot bij de behandeling van het wetsvoorstel tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), zich bij deze wetsbehandeling wél bewust is van de grote maatschappelijke gevolgen van het gebruik en misbruik van softwarekwetsbaarheden. De regering stelt bijvoorbeeld dat derden gebruik kunnen maken van door de diensten aangebrachte malware. Geldt dit ook voor de malware die de politie zal gaan gebruiken? Kan de regering aangeven hoe de coördinatie verloopt tussen de diensten en de politie met betrekking tot de verschillende hackbevoegdheden? Wat voor risico's ziet de regering als zowel de diensten als de politie geautomatiseerde werken van terrorismeverdachten hacken? Hoe kijkt de regering aan tegen de wenselijkheid vanuit nationaal veiligheidsbelang dat de politie «exploits» voor onbekende kwetsbaarheden in gaat kopen die buitenlandse mogendheden ook in kunnen kopen. Ziet de regering het zo veilig mogelijk maken van «het internet» en alle daarop aangesloten apparaten als nationaal veiligheidsbelang? Hoe past het toestaan van de handel in «exploits» van bekende en onbekende kwetsbaarheden daarin? Welke criteria gebruiken de diensten voor het al dan niet melden van onbekende kwetsbaarheden in software? Hoe wordt de afweging gemaakt om een kwetsbaarheid in veelgebruikte consumentensoftware al dan niet te melden aan de maker van de software? Hoe wordt deze afweging gemaakt als het gaat om veelgebruikte encryptie software? Wanneer weegt het belang van nationale veiligheid in een dergelijk geval zwaarder dan de collectieve veiligheid van gebruikers van de software ten opzichte van criminelen,

buitenlandse mogendheden en andere kwaadwillenden? Voorziet de regering situaties waarin het wenselijk is om kwetsbaarheden in de encryptie van chatapps als Whatsapp of Signal of andere veelgebruikte consumentensoftware achter te houden in plaats van te dichten? Is de regering bereid hiervoor een richtlijn op te stellen en de CTIVD hierop toezicht te laten houden?

De leden van de GroenLinks-fractie begrijpen de keuze van de regering om de wet technologieneutraal te formuleren in het kader van de duurzaamheid van de wet in de toekomst. Tegelijkertijd achten deze leden het van belang dat de wet waarborgen biedt tegen opgerekte definities, zoals bijvoorbeeld het begrip «geautomatiseerde werken», met het oog op bescherming van de privacy bij toekomstige technologische ontwikkelingen. Deze leden vragen de regering dan ook of zij bereid is een mogelijkheid tot nadere regelgeving in artikel 45 te creëren, waarin een heldere definitie kan worden gegeven van wat verstaan dient te worden onder geautomatiseerde werken.
Voorts zijn de leden van de GroenLinks-fractie bezorgd over de nieuwe bevoegdheid voor de diensten om te hacken via (onschuldige) derden. Deze leden begrijpen dat een dergelijk vergaand middel in sommige situaties de enige uitkomst kan zijn en dat de CTIVD om die reden enkele malen reeds een dergelijke hack heeft toegestaan als uitzondering op de regel. Deze leden zijn echter van mening dat door het expliciet opnemen van deze bevoegdheid 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. Zij vragen de regering op welke wijze dit gevaar is meegewogen in artikel 45.
In het bijzonder zijn de leden van de GroenLinks-fractie kritisch op de in het leven geroepen meewerkplicht van personen aan de ontsleuteling van gegevens. Deze leden vragen of niet een principiële grens wordt overschreden door derden te dwingen medeplichtig te worden aan de modus operandi van de diensten.
De leden van de GroenLinks-fractie vragen de regering uit te sluiten dat zogenoemde «zero day»-beveiligingslekken worden aangekocht door de diensten in het kader van de hackbevoegdheid. Voorts vragen de leden van de GroenLinks-fractie aan de regering om te bevestigen dat beveiligingslekken 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.

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 vragen zich af waarom de diensten de huidige bewaartermijnen als een knelpunt ervaren, en waarom langere bewaartermijnen van belang zouden zijn voor Defensie.
Deze leden vragen hoe de bewaartermijn zich verhoudt tot de duur van militaire missies.
De leden van de VVD-fractie vragen wat er gebeurt met de data die niet relevant zijn en niet voldoen aan het filter. Hoe worden deze verwijderd en hoe wordt dit ook zo gedaan dat het kan worden gecontroleerd?
De leden van de VVD-fractie vragen zich af of de regering het belang van historische metadata kan aangeven en hoe hiermee om te gaan. Deze leden vragen zich het volgende af: indien de bewaartermijn korter zou zijn dan 3 jaar, kan de regering aangeven wat voor effect dit mogelijk heeft t.a.v. militaire missies en informatie uit MIVD-onderzoek? Kunt u dezelfde vraag beantwoorden voor informatie uit AIVD-onderzoek?
De leden van de VVD-fractie merken op dat in het voorliggende wetsvoorstel wordt uitgegaan van het systeem collect before you select.

Deze leden vragen waarom er geen gebruik wordt gemaakt van een zogeheten rolling buffer waarbij de verzamelde gegevens na bepaalde tijd automatisch overschreven worden door wat nieuw binnenkomt. Kan de regering uitleggen waarom het in het werk van de diensten niet werkt om met het uitgangspunt select before you collect te werken?

De leden van de PvdA-fractie lezen dat de voorziene bewaartermijn in het geval van onderzoeksopdrachtgerichte interceptie op drie jaar zou moeten worden gezet. Deze leden begrijpen de behoefte van de diensten aan een dergelijke lange bewaartermijn. Het kan immers pas na verloop van langere tijd duidelijk worden of de bewaarde gegevens van nut kunnen zijn. Echter, zo menen deze leden, levert een dergelijk lange bewaartermijn van drie jaar ook een risico voor de privacy op. Naar de mening van deze leden mag het vermoeden dat gegevens eventueel later bruikbaar kunnen worden er niet toe leiden dat die ongeclausuleerd allemaal drie jaar bewaard zouden mogen worden. Hoe denkt de regering in dit verband 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?
In dit verband zouden de leden van de PvdA-fractie ook willen wijzen op een opmerking van de Autoriteit Persoonsgegevens die er op wijst dat de aan de ene kant de diensten de onderzoeksopdracht gerichte interceptie zo gericht mogelijk zullen inzetten om te voorkomen dat men niet-relevante gegevens binnenhaalt. Maar aan de andere kant wordt echter tegelijkertijd benadrukt dat het voor de diensten van belang is om lange tijd te beschikken over grote datasets, om op die manier inzicht te verkrijgen in nog onbekende dreigingen.
Dit komt de leden van de PvdA-fractie als tegenstrijdig over: of er is echt sprake van «select while you collect» en kan er dus nauwelijks sprake zijn van gegevens die voor latere doeleinden geschikt zijn of er wordt wel al bewust ruime data verzameld met het oog op latere toepassing. Kan de regering hier op in gaan?

De leden van de SP-fractie constateren dat zowel de CTIVD als de Raad van State aangeven dat de scheiding tussen verwerving, verwerking en nabewerking van gegevens niet altijd even duidelijk zal zijn. Kan de regering hier nader op in gaan? Hoe wordt voldoende uitdrukking gegeven aan het principe van «select while you collect» en zijn er andere mogelijkheden om meer recht te doen aan dit principe, zo vragen de leden van de SP-fractie.
De leden van de SP-fractie begrijpen dat er wordt afgeweken van de standaard bewaartermijn voor niet-ontsleutelde data. De bewaartermijn van drie jaar lijkt echter tegenstrijdig met het principe «select while you collect». Hoe verhoudt dit principe zich met de wens om een historisch archief op te bouwen? Waarom is niet gekozen voor een onderscheid, zoals voorgesteld door de CTIVD, tussen metadata en inhoudelijke gegevens?
De leden van de SP-fractie hebben ook vragen over de medewerkingsplicht van bedrijven bij het ontsleutelen van informatie. Waarom acht de regering dit proportioneel? Wanneer ontsleuteling van encryptie vereist wordt betekent dat ook dat voor alle andere gebruikers van een bepaalde dienst de veiligheid en privacy niet meer gewaarborgd is, bijvoorbeeld als het gaat om de sleutel tot end-to-end-encryptie. Daarnaast wordt een medewerkingsplicht voorgesteld voor bedrijven op verschillende terreinen van informatieverschaffing. De leden van de SP-fractie vragen zich af of hier voldoende rekening is gehouden met bedrijfsgevoelige informatie en hoe bedrijven hiertegen in bezwaar kunnen gaan. Worden bedrijven gehoord voor zij moeten voldoen aan een dergelijk verzoek,

zodat zij ook duidelijk kunnen maken waarom het eventueel onmogelijk of onwenselijk is om hieraan te voldoen?
Daarnaast vragen de leden van de SP-fractie 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? Kan de regering nader uiteenzetten wanneer bedrijven moeten meewerken aan de informatieplicht?

De leden van de CDA-fractie onderkennen dat het onderscheid tussen ether en kabelgebonden informatie door de technologische ontwikkelingen achterhaald is. Deze leden onderschrijven het uitgangspunt dat het onderscheid tussen de ether en de kabel wordt losgelaten. Deze leden zijn overtuigd van de noodzaak, dat de diensten de bevoegdheid krijgen om zogenoemde onderzoeksopdrachtgerichte interceptie te verrichten in het kabelgebonden domein. Wel vragen deze leden de regering nader uiteen te zetten, zo mogelijk aan de hand van concrete voorbeelden, wat precies moet worden verstaan onder «onderzoeksopdrachtgericht».
De CTIVD stelt in haar zienswijze over het voorliggende wetsvoorstel, dat het voorgestelde interceptiestelsel nog geen adequaat systeem van wettelijke waarborgen bevat. De leden van de CDA-fractie vragen de regering met name in te gaan op de suggestie van de CTIVD, om de risico's voor de bescherming van grondrechten, die bulkinterceptie met zich meebrengt, te beperken door middel van «verantwoorde databeperking». De kern hiervan is dat gegevens altijd zo gericht mogelijk dienen te worden verworven en dat verworven gegevens zo spoedig mogelijk moeten worden gereduceerd tot die gegevens die de diensten daadwerkelijk nodig hebben om hun taken goed uit te voeren. Deelt de regering het standpunt van de CTIVD dat het van essentieel belang is dat «verantwoorde databeperking» nadere invulling krijgt? Enerzijds door het vereiste in dit wetsvoorstel op te nemen dat de inzet van bevoegdheden «zo gericht mogelijk» moet zijn. Anderzijds door de doelgerichtheid bij de verwerking van gegevens te verankeren in concrete wettelijke plichten die ervoor zorgen dat de interceptie en verdere verwerking daadwerkelijk onderzoeksopdrachtgericht gebeurt, de opslag van gegevens daarmee wordt beperkt, vernietiging van gegevens tijdig plaatsvindt en dat op dit alles effectief toezicht kan worden gehouden. Deze leden ontvangen graag een reactie van de regering op de voorstellen van de CTIVD.
De leden van de CDA-fractie vragen de regering ook in te gaan op het pleidooi van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), dat juist de analysefase veel sterker onder toezicht zou moeten komen te staan. De WRR pleit voor een wettelijke zorgplicht waarin het borgen van de kwaliteit en de toegankelijkheid van de analyse voor het toezicht centraal staan. Centrale elementen daarvan zijn:

a. Zorgen dat gegevens up to date zijn en dat gecorrigeerd wordt voor de bias in datasets. Deze plicht strekt zich ook uit tot gegevens die de diensten van derden verkrijgen.
b. De algoritmes en methoden die bij data-analyses worden gebruikt moeten deugdelijk zijn, aan de wetenschappelijke criteria voor goed (statistisch) onderzoek voldoen en voor toezicht toegankelijk zijn.
c. Onderzoeksresultaten, profielen en foutmarges moeten op hun merites worden beoordeeld: de diensten moeten duidelijk kunnen maken hoe zij tot bepaalde uitkomsten komen.

De leden van de CDA-fractie vragen de regering in te gaan op de mogelijkheden voor het opnemen van een dergelijke zorgplicht in het voorliggende wetsvoorstel.
Onderzoeksopdrachtgerichte interceptie van communicatie zal in de meeste gevallen versleutelde data opleveren. Crypto- en signaalonderzoek en ontcijfertechnieken zijn nodig om versleutelde data leesbaar te maken (memorie van toelichting, blz. 98).

De leden van de CDA-fractie vragen, of de regering voornemens is hiervoor extra middelen te investeren. Zo ja, hoeveel? Zo nee, waarom niet?

De leden van de D66-fractie constateren dat over de regeling voor onderzoeksopdrachtgerichte interceptie van communicatie veel onrust bestaat. Die zorgen bestaan in de kern uit de vraag of de diensten nu zij niet alleen toegang tot de ether, maar ook tot de kabel krijgen, op grote schaal en ongericht data van personen gaan verzamelen.
De leden van de D66-fractie merken op dat steeds gesteld wordt dat toegang tot de kabel nodig is om gegeven de technologische ontwikkelingen voldoende relevante informatie te kunnen blijven verzamelen om Nederland en onze militairen veilig te kunnen houden. Tegelijkertijd blijkt dat onze diensten het in toenemende mate moeilijk hebben met het gegeven dat steeds meer communicatie versleuteld verstuurd wordt. In hoeverre is het inzetten op interceptie van communicatie dan een toekomstbestendige keuze? Welk nut kennen die data dan? Moet dan niet geprobeerd worden de communicatiegegevens bij de verzender of ontvanger te onderscheppen in plaats van onderweg?
Daarnaast lazen de leden van de D66-fractie in het toezichtsrapport nr. 46 van de CTIVD op pagina 20 dat uit navraag bij de AIVD bleek dat de inhoudelijke opbrengst van toepassing van de selectiebevoegdheid bij SIGINT voor operaties (zeer) gering was. In bepaalde operaties bleek zelfs geheel geen sprake van inhoudelijke opbrengst. Dat roept gecombineerd met de aanhoudende zorgen van de CTIVD over de motivatie bij de inzet van SIGINT vragen op aangezien de kabelinterceptie een soortgelijke bevoegdheid is. Waarom worden SIGINT-bevoegdheden ingezet zonder dat daar opbrengst uit voortvloeit? Wat betekent dit voor de zorgvuldigheid van de motivatie en van de gegeven toestemming? Als dit geregeld een niet effectieve bevoegdheid blijkt, waarom is het dan noodzakelijk om onderzoeksopdrachtgerichte interceptie op de kabel te kunnen verrichten? Bestaat in deze noodzaak nog een verschil tussen de AIVD en de MIVD, of is de SIGINT-bevoegdheid juist nier meer effectief, omdat communicatie zich verschoven heeft van ether naar kabel? Indien op deze vraag een bevestigend antwoord gegeven wordt, op welke wijze onderbouwt de regering dat? Is het mogelijk om verschuiving van de communicatie niet alleen te correleren aan afnemend nut van de SIGINT-bevoegdheid, maar daar ook een oorzakelijk verband in te vinden?
De leden van de D66-fractie merken op dat de term «onderzoeksopdrachtgerichte interceptie» veel ruimte openlaat. Mogelijkerwijs is daar ook bij velen de vrees voor een sleepnet uit ontstaan. Kan de regering aan de hand van voorbeelden duidelijker maken wat de onderzoeksopdrachten in de praktijk inhouden en in hoeverre sprake is van die «onderzoeksopdrachtgerichte interceptie»? Klopt het dat «onderzoeksopdrachtgerichte interceptie» tevens mogelijk is zonder concrete aanwijzingen of verdenkingen?
De leden van de D66-fractie hebben in het kader van de inzet nog wat aanvullende vragen ten aanzien van de samenhang van de verwervings-, verwerkings- en analysefase. Zoals enkele deskundigen opmerken zullen deze fasen in de praktijk vaak in elkaar overlopen, en kondigde de regering al aan dat hiervoor dan een gecombineerde last afgegeven zal worden. Kan er een garantie gegeven worden dat daarmee de motivatie niet vervlakt en dat een dergelijk gecombineerde last getoetst zal worden als ware het drie afzonderlijke lasten? Wordt uitgesloten dat over en weer de lasten elkaars noodzaak, subsidiariteit en proportionaliteitsoordeel zullen beïnvloeden? Indien blijkt dat uit de verworven gegevens geen verwerking kan plaatsvinden aan de hand van de toegestane selectiecriteria, vervalt dan de toestemming tot analyse? Of kan dat met een aanvullende specifiek op de verwerkingsfase gerichte last hersteld worden? Hoe zou dat zich weer verhouden tot het feit dat niet-relevante

gegevens vernietigd dienen te worden en de gegevens zolang er geen aanvullende verwerkingslast is ontstaan, niet relevant meer zijn?
De leden van de D66-fractie constateren dat in artikelen 48 en 49 geen termijn is opgenomen waarbinnen de als niet-relevant bestempelde gegevens voor toepassing van gegevensbewerking zoals bedoeld in artikelen 49 en 50 vernietigd moeten worden. Om te voorkomen dat deze informatie dan toch (al dan niet in verwijderde staat) bewaard wordt in de hoop dat ze ooit wel nuttig blijken, regelt het amendement van het lid Verhoeven over dataminimalisatie bij het verwerven en verwerken van gegevens (Kamerstuk 34 588, nr. 11) dat deze gegevens terstond vernietigd moeten worden. Graag vernemen deze leden hoe de regering daar technisch invulling aan wil geven binnen de systemen van de diensten om zeker te stellen dat dit gebeurt.
De leden van de D66-fractie lezen in enkele commentaren op het voorliggende wetsvoorstel dat de diensten een kopie van de gehele glasvezelkabel krijgen, waaruit zij zelf het meest interessante kanaal selecteren. Anderzijds begrijpen deze leden juist 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. Welk van deze opvattingen acht de regering het meest juist? Voor zover één van de beweringen (deels) onjuist is, hoe heeft die indruk kunnen ontstaan? Is de regering bereid dit aspect in het wetsvoorstel te verduidelijken?
Een in dit kader steeds terugkerende term is «select while you collect». De leden van de D66-fractie zijn in dat kader benieuwd hoeveel data in elke stap vernietigd wordt. Kan de regering daarvan een zo nauwkeurig mogelijk gemiddelde, inclusief bandbreedte, geven waarin alle communicatie die in een tijdvak x door een internetkabel stroomt 100% is? Deze leden horen dan in ieder geval graag hoeveel procent daadwerkelijk getapt wordt, hoeveel procent daarvan vervolgens daadwerkelijk binnengehaald wordt (verwerving), hoeveel er overblijft na verwerking en welk deel uiteindelijk geanalyseerd wordt.
Daarnaast zijn deze leden benieuwd 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. Kan het «select while you collect-principe» bij dit soort toepassing van de artikel 48-bevoegdheid zodanig worden opgevat dat alleen de anomalieën waarnaar men op zoek is daadwerkelijk bij de diensten binnengehaald worden, dat al het overige internetverkeer ongestoord en ongehinderd door de «zeef» heen zal komen en dat hiervan dus geen enkel spoor binnen de databestanden van de diensten terug te vinden zal zijn?
De leden van de D66-fractie lezen in de paragraaf over het belang van onderzoeksopdrachtgerichte interceptie dat de samenwerking met buitenlandse collega-diensten onder druk komt te staan zonder vergelijkbare informatiepositie. Deze leden krijgen de indruk dat de regering hiermee bedoelt «met dezelfde bevoegdheden». Klopt dat? Zo nee, waarom niet? Houdt «vergelijkbaar» niet ook in dat er specialisatie kan plaatsvinden en dat de diensten omwille van hun satellietstation Burum en goed gekwalificeerde medewerkers op gelijke voet staan met diensten die zich meer op massale en geautomatiseerde dataverwerking richten?
Deze opmerking in de memorie van toelichting kan volgens de leden van de D66-fractie ook de indruk wekken dat er vanuit het buitenland druk op de regering en/of de diensten is uitgeoefend om de bijzondere bevoegdheden van de diensten uit te breiden naar communicatie over de kabel. Deze leden zouden graag willen dat de regering uitsluit dat dit direct noch indirect, expliciet noch impliciet aan bod geweest is. En dat voor zover andere landen en/of hun diensten daartoe wel aanzet gegeven zouden hebben, hen te verstaan is gegeven dat zij niet over de Nederlandse wet gaan noch over de bevoegdheden die onze diensten toegekend worden.

Deze leden krijgen graag bevestiging hiervan. Ook horen zij het graag wanneer een buitenlandse dienst heeft gedreigd c.q. heeft medegedeeld dat het niet toegang krijgen tot de kabel door de Nederlandsen diensten gevolgen zou hebben voor de samenwerking.
De leden van de D66-fractie constateren dat voor verkregen, maar niet verwerkte gegevens, een verlengde bewaartermijn van drie jaar geldt. Evenwel wordt niet sluitend gemotiveerd waarom die gehele termijn noodzakelijk zou zijn; er wordt slechts aangegeven dat een jaar in de praktijk bijzonder krap gebleken is, maar niet dat het onmogelijk is. Deze leden schrappen daarom in amendement van het lid Verhoeven van de D66-fractie over dataminimalisatie bij het verwerven en verwerken van gegevens (Kamerstuk 34 588, nr. 11) de uitzondering grotendeels. De bewaartermijn wordt voor de inhoud van communicatie teruggebracht naar de standaard (één jaar) en voor metadata teruggebracht naar anderhalf jaar in plaats van drie jaar. Deze leden staan echter open voor een aanpassing waarbij onderscheid valt te maken tussen data verzameld voor de taakuitvoering van de diensten. Waarom heeft de regering niet voor een dergelijk gedifferentieerd model in het voorliggende wetsvoorstel gekozen? Argumenten aangaande benodigde bewaartermijnen voor militaire missies zijn immers voor de taakuitvoering van (en bewaartermijnen bij) de AIVD niet relevant.
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 zijn benieuwd naar de wijze waarop de balans gevonden is tussen snel wisselende omstandigheden en communicatiewijzen enerzijds, en de termijn waarvoor een interceptielast afgegeven wordt anderzijds. Met andere woorden, waarom is gekozen voor een termijn van een jaar, en niet korter of langer? Wat is verder het zodanig grote verschil tussen de selectie van gegevens (artikel 50, eerste lid, onder a) en metadata-analyse (idem, onder b), dat een toestemmingsduurverschil van een factor vier tussen voor de analyse-last beide rechtvaardigt? Uit de toelichting kunnen deze leden daar weinig dragende argumenten voor vinden, terwijl vanuit verschillende instanties hier wel kritiek op geuit wordt.
De leden van de D66-fractie lazen in het artikel «Select while you collect» van de heer Jacobs van de Radboud Universiteit Nijmegen in het Nederlandse Juristenblad dat in recente Amerikaanse wetgeving in-bulkverzameling beperkt is tot bepaalde thematische doelen. Volgens de heer Jacobs ontbreken dergelijke themagerichte bepalingen in de Nederlandse wet. Graag verkrijgen deze leden daarop een reactie. Zij vragen dit mede nu de Geïntegreerde Aanwijzing volgens hen zou moeten bepalen ten aanzien van welke onderwerpen de diensten onderzoek mogen verrichten binnen hun taken. In welke mate wordt daarmee ook geborgd dat slechts over een beperkt aantal thema's gegevens per bulk, of onderzoeksopdrachtgerichte interceptie, naar binnen gehaald kunnen worden? Dit te meer nu in de memorie van toelichting wordt aangegeven dat de onderzoeksthema's en de onderzoeksdoelstellingen die worden toegewezen aan één of beide diensten in de geheime bijlage van de Geïntegreerde Aanwijzing zullen worden opgenomen. Zal die geheime bijlage in de CIVD besproken worden? En in hoeverre verhouden de openbaar aangeduide onderzoeksthema's in de openbare versies van de jaarplannen AIVD (bijv. Kamerstukken II, 2014/15, 30 977 nr. 119 en Kamerstukken II, 2015/16, nr. 135) zich tot de onderzoeksthema's die in de

geheime bijlage van de Aanwijzing staan? Valt er, gegeven het Amerikaanse voorbeeld, wellicht meer te openbaren? Graag een gemotiveerde reactie.
De leden van de D66-fractie vragen zich af welke verhouding tussen geautomatiseerde (meta)data-analyse en human intelligence de regering voorstaat. Kan de regering ingaan op het gevaar dat een te grote focus binnen de diensten op relatief laagwaardige aanwijzingen uit bulkinterceptie de aandacht wegnemen van relatief hoogwaardige «human intelligence»? Hoe wil de regering dit voorkomen? Hoe kijkt de regering aan tegen de woorden van Bill Binney die stelt «bulk surveillance kills people»? Is het niet ook zo dat veelal wanneer na een aanslag in de systemen teruggezocht wordt, er over de daders wel informatie aanwezig bleek, maar deze nog niet verwerkt was of nog niet tot opvolging had geleid? Daarnaast bestaat het risico dat fouten in de algoritmes en modellen ertoe leiden dat iemand onterecht aangemerkt wordt als gevaar. In dat kader waarderen deze leden de in artikel 60, derde lid, opgenomen waarborg dat het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een gegevensverwerking als bedoeld in het tweede lid niet is toegestaan. Zij vragen zich echter af, wat deze waarborg en de antwoorden op voorgaande vragen betekenen voor de benodigde verhoudingen binnen de AIVD en MIVD ten aanzien van het investeren in mensen (analisten en vertalers) versus het investeren in ICT (dataopslag, ICT, it'ers). Kan de regering daar, uiteraard binnen de grenzen van het beschermen van de modus operandi, meer licht op doen schijnen? Kan gegarandeerd worden dat human intelligence ook onder dit wetsvoorstel de leidende bron van informatieverwerving, gegevensverwerking en analyse blijft?
De leden van de D66-fractie vragen zich af welke gevolgen 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. Als zij de enigen zijn die weten welke data er zijn, wordt het dan niet lastig gericht selectiecriteria in het kader van artikel 49 aan te wijzen en vervolgens het risico bestaat dat meer communicatie verworven wordt dan strikt noodzakelijk. Hoe is de regering voornemens dat te ondervangen? Voor een gerichte onderzoeksopdrachtgerichte interceptie zal in de praktijk toch immers een wisselwerking tussen verwerven en verwerken bestaan?
Voorts constateren de leden van de D66-fractie dat de diensten zogeheten «access locaties» gaan gebruiken. Kan de regering nader toelichten wat er onder access locaties wordt verstaan? Geldt de medewerkingsverplichting ook voor buitenlandse aanbieders van communicatie? Voorts geeft de regering aan dat er wordt aangegeven dat er bij het selectieproces bij interceptie gekeken kan worden naar specifieke versleuteling. Kan daaruit worden afgeleid dat gebruik van bepaalde vormen van versleuteling een reden kan vormen om geselecteerd te worden, zoals bijvoorbeeld PGP? Hoe en door wie vindt de controle plaats of de gebruikte analyse- en verwerkingssoftware wel veilig genoeg is en of de gebruikte algoritmes naar behoren functioneren?

De leden van de ChristenUnie-fractie constateren dat meer ongerichte interceptie (onderzoeksopdrachtgerichte interceptie) van telecommunicatie mogelijk wordt met dit wetsvoorstel, waardoor grote hoeveelheden informatie kunnen worden binnengehaald voor analyse. Deze leden vragen of de regering nader kan onderbouwen waarom de huidige bevoegdheid tot gerichte interceptie van telecommunicatie onvoldoende is.
Deze leden vragen of de regering de noodzaak van de lengte van de bewaartermijnen bij onderzoeksopdrachtgerichte interceptie nader kan onderbouwen. De casus die de regering daarbij ter illustratie geeft lijken

er op te wijzen dat het gaat om een grote bulk aan data en om aspecifieke gegevens, terwijl aan de andere kant de suggestie wordt gewekt dat al een nadere specificering heeft plaatsgevonden van de te bewaren gegevens via de in de memorie van toelichting beschreven fases van onderzoeksopdrachtgerichte interceptie. Kan de regering dit verschil nader verklaren? De leden van de ChristenUnie-fractie constateren daarbij dat de Raad van State en de CTIVD concluderen dat de drie fases van onderzoeksopdrachtgerichte interceptie nauw zijn verweven. Kan de regering nader aangeven wat dan in dit kader de betekenis is van de opmerking dat de gegevens die worden bewaard reeds «significant gereduceerd» zouden zijn?
De leden van de ChristenUnie-fractie vragen of gegevens die zijn verzameld in de eerste of tweede fase van onderzoeksopdrachtgerichte interceptie, op enigerlei wijze mogen worden gedeeld met het buitenland.

De leden van de GroenLinks-fractie vragen waarom de regering met betrekking tot de sleepnetbevoegdheid die in het voorliggende wetsvoorstel wordt gecreëerd, de term «onderzoeksopdrachtgerichte interceptie» is gegeven. Deze leden vragen of het woord «gerichte» in dezen niet enigszins misleidend is, aangezien de bevoegdheid juist het ongericht aftappen van communicatie behelst.
De leden van de GroenLinks-fractie vragen waarom geen gehoor is gegeven aan het advies van de Raad van State om de bewaartermijn voor via de sleepnetbevoegdheid binnengekregen gegevens te beperken tot één jaar in plaats van drie.
De leden van de GroenLinks-fractie vragen een precieze definitie te ontvangen van de regering van hetgeen een «onderzoeksopdracht» in het kader van de sleepnetbevoegdheid kan behelzen. Deze leden vragen aan welke vereisten deze opdrachten dienen te voldoen en of de CTIVD in voldoende mate in staat zal zijn om te bezien of de middels het sleepnet verkregen gegevens daadwerkelijk alleen ten behoeve van deze onderzoeksopdracht zullen worden verwerkt.
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.
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.
De leden van de GroenLinks-fractie vragen met betrekking tot de verplichting die de diensten in het kader van de sleepnetbevoegdheid kunnen opleggen aan derden om hieraan mee te werken, of hiermee niet een principiële grens wordt overschreden door het gedwongen medeplichtig maken van derden aan de modus operandi van de veiligheidsdiensten.

De leden van de SGP-fractie onderkennen het belang van onderzoeksopdrachtgerichte interceptie. Adequate samenwerking met andere diensten en het zoveel mogelijk onderkennen van bedreigingen voor de veiligheid rechtvaardigen naar hun opvatting deze vorm van onderzoek. Wel dienen hierbij steeds de waarborgen van de rechtsstaat in acht genomen te worden. Is de regering van mening 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?
Er is in dit verband ook een mogelijkheid om iemand die kennis heeft van de wijze van versleuteling te dwingen om mee te werken aan het doorbreken hiervan. Hoe is gewaarborgd dat deze persoon zo min mogelijk te maken krijgt met negatieve consequenties hiervan?

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 horen graag 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. Uit de binnengekomen reacties op (conceptversies van) het wetsvoorstel hebben zij namelijk niet de indruk dat het overleg tussen de regering en deze aanbieders soepel is verlopen. Hoe kijkt de regering terug op dat overleg? Welke lessen zijn daarin geleerd? Ziet de regering ook in dat voor het efficiënt en effectief inzetten van de interceptiebevoegdheid er goed en constructief overleg nodig zal zijn? In welke mate zijn bij de diensten en de betrokken ministeries ambtenaren aanwezig die (uitgebreide) kennis hebben van de communicatiedienstensector?

De leden van de D66-fractie vinden het zeer terecht dat er alsnog een vergoeding voor de door communicatiedienstaanbieders gemaakte kosten in het wetsvoorstel is opgenomen. Over de formulering ten aanzien van die vergoeding hebben deze leden echter nog enige zorgen. Er wordt steeds gesteld dat dit een vergoeding naar redelijkheid is en niet een volledige vergoeding. Waarom is dat? Is het niet ook zo dat bij het externaliseren van kosten een dempende prikkel om onderzoeksopdrachten zo gericht mogelijk te formuleren wordt weggenomen? Behelst dat niet een risico op sluipenderwijs steeds meer data binnenhalen?

De leden van de D66-fractie zouden graag van de regering vernemen in hoeverre een medewerkingsplicht een aanbieder van een telecommunicatiedienst mag belasten. Er kan weliswaar een vergoeding tegenover de gemaakte kosten staan, maar als er dankzij de uitvoering van het gevraagde een niet op te lossen tekort aan specialisten bij dat bedrijf bestaat of de concurrentiekracht in gevaar komt, dan zou daar volgens deze leden een oplossing voor gevonden moeten worden of anders naar redelijkheid mee omgegaan moeten worden. Hoe beziet de regering dat? Op welke wijze kan een dergelijke aanbieder laten weten dat zij onevenredig getroffen wordt? Wordt een aanbieder door de TIB gehoord voorafgaand aan hun beslissing over de ministeriele toestemming? Of is het wellicht zelfs zo dat het ontbreken van overleg over het opleggen van de plicht een reden is de ministeriele toestemming niet te accorderen?

De leden van de D66-fractie merken op dat enkele telecommunicatiebedrijven zich afvragen hoe het gevraagde maatwerk ten aanzien van de medewerkingsplicht zich verhoudt tot de gewone bedrijfsprocessen zoals upgrading van de systemen, het implementeren van nieuwe beveiliging of het anders c.q. nieuw inrichten van netwerken en systemen om een groeiende hoeveelheid dataverkeer goed te kunnen afwikkelen. Sluit de regering uit dat bedrijven in het bieden van veiligheid aan hun consumenten of in hun technologische ontwikkeling geremd worden ten gevolge van het in stand moeten houden van technische voorzieningen ten behoeve van de diensten? Zo ja, hoe is dat geborgd? Zo nee, hoe worden beide belangen dan tegen elkaar gewogen? Hoe wordt bijvoorbeeld de veiligheid die potentieel gewonnen wordt dankzij de communicatieverstrekking afgewogen tegen de vergrote onveiligheid dankzij 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. Zo staat in de memorie van toelichting dat het mogelijk is om met de analyse van mastgegevens in geval van een heimelijke ontmoeting inzicht te verkrijgen in welke communicatieapparatuur op moment van de ontmoeting in de buurt aanwezig was. Maar gaat het dan om een straal

van 10 meter, 100 meter, 1 kilometer of 10 kilometer? Gaat het dan om elke ontmoeting waar de dienst in geïnteresseerd is, of enkel om ontmoetingen waarbij niet iemand kan observeren wie er aanwezig zijn? Daarnaast merken deze leden op dat bij algemene maatregel van bestuur de gegevens worden aangewezen waarop het verzoek betrekking kan hebben. Zij verkrijgen graag alvast enig inzicht om wat soort type gegevens dat zal gaan.

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 lezen in de memorie van toelichting dat de regering benadrukt dat de medewerkingsplicht bij ontsleuteling van communicatie geen bevoegdheid betreft om te verzoeken tot het afzwakken van de encryptie van de systemen en/of het inbouwen van toegang tot de systemen om ontsleutelde gegevens te verkrijgen. Maar als dat het geval is, waarom is dat dan niet expliciet in het wetsvoorstel opgenomen? Op die manier wordt elke onduidelijkheid erover uitgesloten. Het lid Verhoeven heeft daarom een amendement ingediend over de medewerkingsplicht bij ontsleuteling van communicatie (Kamerstuk 34 588 nr. 13). Kan dit amendement rekenen op steun van de regering?
De leden van de D66-fractie hebben via de media begrepen dat de AIVD druk bezig is de encryptie van Whatsapp te verbreken. Hoe zal, gegeven de beperking dat er geen achterdeurtjes ingebouwd worden of systemen verzwakt, een eventueel verzoek aan de makers van Whatsapp om mee te helpen communicatie te ontsleutelen vorm krijgen? Wanneer wordt verder volstaan met het meewerken aan het ongedaan maken van versleuteling, en wanneer wordt vereist dat een persoon actief zelf de versleuteling ongedaan maakt?
De leden van de D66-fractie herinneren zich dat de regering in januari 2016 onmiskenbaar heeft vastgesteld dat het doorbreken en afzwakken van encryptie niet aan de orde is. Niettemin hebben zowel de Directeur Generaal (DG) van de AIVD (Volkskrant, 17 september 2016) als de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) (De Telegraaf, 16 december 2016), gemeend dat zij zich beiden in media moesten uitlaten over hun wens om toch encryptie te mogen doorbreken. Kunt u toelichten waarom beide personen de noodzaak zagen om in de media te verkondigen dat voor de bestrijding van terrorisme in hun ogen noodzaak bestaat voor het doorbreken van encryptie, terwijl het kabinetsstandpunt glashelder is dat dit niet aan de orde is? Is er met de AIVD en NCTV gesproken over encryptie en het kabinetsstandpunt? Op grond waarvan menen de AIVD en NCTV dat via de media toch door hen gelobbyd moet worden voor het doorbreken en afzwakken van encryptie? Of hadden hun uitlatingen een ander doel? En wat is uw opvatting over deze gang door deze overheidsdiensten waarmee zij iets verkondigen dat haaks staat op kabinetsbeleid? Vindt u dergelijke uitlatingen in de media bovendien gepast wanneer een wetsvoorstel aan de Kamer voorligt dat voorziet in uitbreiding van bevoegdheden voor de diensten?
Daarnaast herinneren de leden van de D66-fractie zich de volgende uitspraak van de DG AIVD in de Volkskrant van 17 september: «Ik wil van diegenen die een bedreiging vormen de communicatie inzien.» Over het standpunt van het kabinet zegt hij: «Dan moet je als regering ook accepteren dat we niet meer bij de communicatie van terroristen kunnen.» Wat vindt u van deze uitlating? En in hoeverre doet de DG AIVD daarmee naar uw opvatting het voorliggende wetsvoorstel te kort waarin de regering juist wil voorzien in een uitbreiding van bevoegdheden voor de diensten die de opsporing van terroristen moet bevorderen?
Ook verkondigde hij in de media: «Ik vind bescherming van privacy ook uitermate belangrijk, maar zouden mensen die privacy als hoogste doel hebben, dat net zo enthousiast nastreven als zij slachtoffer zijn van een aanslag?» Hoe verhoudt naar uw opvatting deze uitlating zich tot de

zienswijze van de CTIVD die stelt dat essentiële privacy waarborgen bij de bulkinterceptiebevoegdheden ontbreken?
Hoe beschouwt u deze uitlating van de NCTV over mensen die vrezen dat de AIVD teveel macht heeft («Het is nodig voor de strijd tegen terrorisme en er is goed toezicht op» in De Telegraaf van 16 december 2016) in het licht van de uitvoerige zienswijze van de CTIVD bij voorliggend wetsvoorstel die juist stelt dat essentiële waarborgen die effectief toezicht mogelijk maken, ontbreken?
De leden van de D66-fractie lezen achterin de memorie van toelichting (rond pagina 236) dat als de diensten stuiten op significante kwetsbaarheden die de belangen van gebruikers op het internet kunnen schaden, de diensten de belangendragers zullen informeren. Maar ook dat er wettelijke argumenten of operationele redenen kunnen zijn die openbaarmaking van kwetsbaarheden (tijdelijk) in de weg staan. Deze leden vragen zich daarom af of er ten aanzien van dit soort kwetsbaarheden (en zero-days) op schrift neergelegd beleid bestaat, of dat dit gemaakt zal worden. Wordt een gevonden kwetsbaarheid als hoofdregel terstond gemeld, of zit daar een vertraging op? Zo ja, hoe lang duurt het alvorens tot melding wordt overgegaan? Welke wettelijke argumenten bestaan er die die melding in de weg zouden staan? Onder welke omstandigheden zou bronbescherming daar één van kunnen zijn? Een kwetsbaarheid kan toch door een ieder gevonden worden? Wanneer kan bescherming van het actueel kennisniveau ingeroepen worden? Is dat niet een zodanig uitgebreide grond dat die altijd ingeroepen kan worden, en de toezegging zoals opgenomen in de memorie van toelichting waardeloos maakt?
De leden van de D66-fractie vragen zich gegeven de discussie bij de Wet computercriminaliteit III af of de diensten ook zelf kwetsbaarheden inkopen. Zo ja, alleen bij betrouwbare partnerdiensten of ook op de zwarte markt? Wordt een ontdekte kwetsbaarheid alleen gemeld boven een bepaald impactniveau, of is die schaal vloeiend? Gaat impact alleen om de hoeveelheid geraakte mensen c.q. bedrijven of ook om de ernst van de schade die kan ontstaan op individueel niveau?

De leden van de GroenLinks-fractie zijn blij dat de regering in de memorie van toelichting ondubbelzinnig bevestigt dat geen sprake is of kan zijn van een verplichting tot het (doen) inbouwen van zwakheden in software of het verzwakken van encryptie. Tegelijkertijd zijn deze leden bezorgd dat er wel sprake kan zijn van het uitoefenen van druk jegens de aanbieders van communicatiediensten om dit (te laten) doen. Deze leden vragen de regering of zij de mening deelt dat het uitoefenen van dergelijke druk onwenselijk is met het oog op mogelijk misbruik van kwaadwillenden van eventueel ingebouwde zwakheden, en of zij de CTIVD zal laten toezien opdat de diensten nooit een dergelijke druk zullen uitoefenen.
De leden van de GroenLinks-fractie vragen de regering 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. Voorts vragen de leden van de GroenLinks-fractie aan de regering om 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.

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

Het is de leden van de D66-fractie niet geheel duidelijk op welke grond van welke criteria de lijst van bijzondere bevoegdheden waarvoor een actieve notificatieplicht geldt tot stand gekomen is. Het lijkt alsof de lijst (grotendeels) gekopieerd is uit de huidige wet, zonder hernieuwde

integrale afweging van welke bevoegdheden daartoe in aanmerking zouden kunnen komen. Klopt dat? Welke bevoegdheden zouden volgens de regering als eerste in aanmerking komen om ook onder de notificatieplicht te gaan vallen?

3.5 Geautomatiseerde (big) data-analyse door de diensten

De leden van de D66-fractie merken op dat er risico's zitten aan geautomatiseerde big data-analyses, waarvan het van belang is dat deze in het wetsvoorstel voldoende ondervangen worden. Zowel de Wetenschappelijke Raad voor het Regeringsbeleid en de Afdeling advisering van de Raad van State zijn op dit aspect kritisch. In dat kader vragen deze leden zich af of het niet verstandig is om in dit wetsvoorstel expliciet op te nemen – zoals gebeurt met het amendement van het lid Verhoeven over de technische, personele en organisatorische maatregelen (Kamerstuk 34 588, nr. 15) – dat onder de zorgplicht van de diensthoofden ook een schriftelijk gegevensbeschermingsbeleid en de nodige voorzieningen vallen met betrekking tot het waarborgen van de kwaliteit en betrouwbaarheid van de gegevensvergadering, van de gebruikte gegevens(bestanden), van de toe te passen modellen, algoritmes, technieken en methoden en van de resultaten van de verwerking?

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?

3.6 De verstrekking van gegevens

De leden van de CDA-fractie merken op dat artikel 64 van het voorliggende wetsvoorstel de mogelijkheid biedt voor de diensten om in het kader van een goede taakuitvoering ongeëvalueerde gegevens te verstrekken aan buitenlandse collegadiensten (memorie van toelichting, blz. 138). Deze leden vragen of hier 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. Onder welke voorwaarden kunnen ongeëvalueerde gegevens worden verstrekt aan buitenlandse collegadiensten? Op welke wijze wordt gegarandeerd dat de waarborgen die van toepassing zijn op het verzamelen en verwerken van gegevens door de AIVD en de MIVD, ook van toepassing zijn als gegevens worden verstrekt aan buitenlandse collegadiensten?

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

De leden van de GroenLinks-fractie vragen de regering nader te motiveren waarom geen nadere definitie is gegeven van het begrip «daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen». Deze leden vragen waarom in de memorie van toelichting slechts een beperkt aantal internationale organen wordt genoemd dat hieronder kan vallen, in plaats van aan te geven waar de grens dient te liggen bij de beoordeling

welke organisaties hieronder kunnen vallen en welke niet. Deze leden vragen de regering deze grens alsnog te beschrijven.
De leden van de GroenLinks-fractie hebben ernstige bedenkingen bij de bevoegdheid tot het verstrekken van niet-geëvalueerde gegevens aan buitenlandse diensten. Deze leden vragen de regering of zij zich rekenschap heeft gegeven van het feit dat door het verstrekken van niet-geëvalueerde gegevens het aanmerkelijke risico van onbedoelde negatieve effecten met grote consequenties ontstaan. Deze leden 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, al dan niet via een derde veiligheidsdienst.
De leden van de GroenLinks-fractie 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. Zij vragen waarom het niet mogelijk is dat de betreffende gegevens met spoed worden geëvalueerd.
Voorts vragen de leden van de GroenLinks-fractie 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.

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

De leden van de D66-fractie maken zich zorgen over het bepaalde in artikel 64. Daarmee wordt ruimte geboden voor het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten. Onder welke omstandigheden acht de regering het werkelijk verantwoord om gegevens te verstrekken aan een dienst met wie geen samenwerkingsrelatie bestaat, waarvan geen uitgebreide risicoweging heeft plaatsgevonden en aan wie ook nog eens een pakket gegevens wordt verstrekt waarvan men niet zeker en/of volledig weet wat de inhoud ervan is? Deze leden kunnen zich geen situatie voorstellen waarin dit voor een goede taakuitoefening van de dienst in strikte zin noodzakelijk is. Weegt zelfs in dat geval het individuele nadeel dat kan ontstaan (bijvoorbeeld een serie doodstraffen doordat per ongeluk gegevens omtrent een groep homoseksueel georiënteerde personen gedeeld wordt) wel op tegen het verkregen voordeel voor het algemeen belang? Graag vernemen zij voorbeelden waaruit dit anderszins zou blijken.
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. Zijn de telefoongesprekken die (waarschijnlijk) via GCHQ bij een gesprekanalyse bedrijf in Australië terecht kwamen afkomstig van de Nederlandse diensten? Acht de regering het mogelijk dat Nederlandse diensten ongeëvalueerde gegevens, inclusief persoonlijke gegevens van onschuldige mensen, uit ongerichte kabeltaps delen met andere landen? Acht de regering dit wenselijk? In hoeverre is de mogelijkheid uitgesloten dat ongeëvalueerde kabelgebonden informatie direct doorgestuurd wordt naar andere landen? In hoeverre biedt het doorsturen van ongeëvalueerde gegevens naar andere landen, waar ruimere bevoegdheden tot analyse van gegevens bestaan, mogelijkheden om de Nederlandse wet te omzeilen?
De leden van de SGP-fractie vragen naar de onderlinge verhouding tussen artikel 64 en artikel 69. De uitwisseling van gegevens met diensten in het buitenland wordt in artikel 69 niet verbonden aan een «dringende en gewichtige reden». Is er bewust gekozen voor dit verschil? In welke situaties zijn beide bevoegdheden van toepassing?

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 vragen zich af wat voor maatregelen de Kamer feitelijk autoriseert op het moment dat zij dit artikel zou aannemen. Zou de regering daarvan enkele exemplarische voorbeelden kunnen geven? Zo nee, waarom niet? Hoe worden bij deze maatregelen voorts de proportionaliteit en subsidiariteit gewogen? Hoe gaat het vereiste «voor de betrokkene het minste nadeel oplevert» concreet toetsbaar gemaakt worden?

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

Het valt de leden van de SGP-fractie op dat er in artikel 76 niet een vergelijkbare uitzondering is opgenomen als in het tweede lid van artikel 78. Deze leden vragen zich af of de geheimhouding van bronnen niet kan spelen bij de inzage van gegevens op grond van artikel 76?

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. Kan de regering aangeven welke voorwaarden en waarborgen er zijn en welke stappen doorlopen dienen te worden alvorens data kunnen worden gedeeld met buitenlandse veiligheids-diensten?

Ook de leden van de PvdA-fractie begrijpen dat in deze tijden van toegenomen internationale dreiging en de (mogelijke) invloed daarvan op de nationale veiligheid, dat de contacten met diensten van andere landen van groot belang zijn. Daarbij passen wettelijke waarborgen die in de huidige WIV 2002 deels nog ontbreken. Het feit dat in het voorliggend wetsvoorstel bepalingen worden opgenomen voor het doen van verzoeken om ondersteuning en voor het verstrekken van ongeëvalueerde gegevens zien deze leden dan ook als winst. De vraag is we echter of deze wettelijke waarborgen niet nog beter kunnen. Zo vragen de leden van de PvdA-fractie 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. Zo wordt een dergelijke informatieverstrekking niet getoetst aan de hand van samenwerkingscriteria en een afweging omtrent risico's in de samenwerkingsrelatie. Kunt u nader ingaan op hoe in dit soort gevallen er nog sprake is van rechtsbescherming? Wat is de verantwoordelijkheid van de Minister in het geval er sprake is van gegevensverstrekking aan diensten waarmee geen samenwerkingsverband bestaat?

De leden van de SP-fractie maken zich zorgen over het eventuele uitwisselen van grote hoeveelheden niet geanalyseerde data met inlichtingendiensten uit andere landen. Deze mogelijkheid biedt het voorliggende wetsvoorstel ook voor de uitwisseling van deze data met inlichtingendiensten uit landen waarbij bijvoorbeeld de democratische rechtsorde en de borging van mensenrechten niet gewaarborgd is. De leden van de SP-fractie vragen waarom de regering niet de gevaren ziet

van het massaal delen veel privacygevoelige informatie van Nederlanders met andere landen. Waarom vindt de regering de veiligheid van de eigen burgers voldoende gewaarborgd? Hoe gaat de regering voorkomen dat door onderlinge uitwisseling van informatie door diensten gegevens van burgers worden «witgewassen»?

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, en 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.
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 (onderzoeksopdrachtgerichte interceptie volgens de regering) in Nederland uit te laten voeren. 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.

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 benadrukken reeds lange tijd het belang van samenwerking met andere inlichtingen- en veiligheidsdiensten op grond van duidelijke keuzes gemaakt aan de hand van vaststaande samenwerkingscriteria. Daartoe zijn moties aangenomen en daarover heeft de CTIVD gerapporteerd in het toezichtsrapport nr. 48. Uit dat rapport kan echter niet opgemaakt worden waarom het nodig zou zijn na inwerkingtreding van de wet nog twee jaar de wegingsnotities die ten grondslag liggen aan de samenwerking uit te stellen. Ook in de artikelsgewijze toelichting wordt slechts gesteld dat op dat moment de notities nog niet allemaal klaar zullen zijn, niet waarom ze niet klaar zullen zijn. Deze leden vernemen daarom graag waarom deze notities niet überhaupt al gereed zijn. Ligt dat aan, zoals de CTIVD in haar conclusies over de wegingsnotities stelt, de AIVD en MIVD die tot medio 2015 weinig prioriteit hieraan gaven? Ligt het dan in de rede dat dergelijke prioriteitstelling beloond wordt door de verplichting dit goed te regelen uitgesteld wordt? Op welke concrete, niet-ondervangbare en ook niet provisorisch oplosbare onmogelijkheden zouden de AIVD en MIVD stuiten om niet per bijvoorbeeld 1 januari 2018 (wat op dit moment volgens deze leden een niet geheel onwaarschijnlijke datum van inwerkingtreding lijkt) de wegingsnotities gereed te hebben? Totdat er bevredigende antwoorden op deze vragen zijn, zal het lid Verhoeven het amendement over de wegingscriteria bij samenwerkingsrelaties (Kamerstuk 34 588, nr. 16) in ieder geval handhaven.

Ook over de inhoud van de wegingsnotitie hebben de leden van de D66-fractie enkele vragen. Waarom is daarin niet mede expliciet een beschrijving van de wettelijke bevoegdheden en technische mogelijkheden van een buitenlandse dienst, en het door die dienst geboden niveau van gegevensbescherming opgenomen? Zijn dat, in het kader van het delen van gegevens die vaak de persoonlijke levenssfeer (diep) raken, niet relevante aspecten?

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 ten behoeve van hun taakuitvoering elke keer opnieuw aan toestemming onderhavig is, of dat de betreffende Minister een toestemming kan geven voor meerdere verstrekkingen. Indien dat laatste plaatsvindt, voor hoeveel verstrekkingen uitgedrukt in aantal of tijdsduur geldt dat dan?
De leden van de D66-fractie vragen zich af of alvorens besloten wordt tot het verlenen van technische of een andere vorm van ondersteuning 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? Zo ja, hoe vindt de toets plaats nu niet expliciet in de wegingsnotitie opgenomen hoeft te worden welke wettelijke bevoegdheden en technische mogelijkheden die dienst heeft? Zo nee, waarom werkt Nederland mee aan het omzeilen van in andere landen opgenomen waarborgen in de uitoefening van de bevoegdheden door die dienst?
De leden van de ChristenUnie-fractie constateren dat wetenschappers in hun open brief adviseren om ook besluiten tot het delen van informatie met het buitenland vooraf te laten toetsen. Waarom heeft de regering daarvoor niet gekozen?

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.
De leden van de PvdA-fractie hebben kennis genomen van hoe het voorliggende wetsvoorstel het toezicht op deze wet vorm geeft. Deze leden hebben daarbij enkele vragen. Het wetsvoorstel voorziet in een gecompliceerd systeem van voorafgaande toestemming door de Minister, toetsing door het TIB of de rechter en achteraf toezicht en klachtbehandeling door de CTIVD. Evenals de CTIVD menen deze leden dat deze partijen zich – tenminste voor een deel – bezig zullen gaan houden met dezelfde rechtsvragen. Hoe denkt de regering er over om in het belang van een uniforme en consistente rechtstoepassing de TIB en de CTIVD de gezamenlijke taak te geven de rechtseenheid te bevorderen? En hoe zou dit vormgegeven kunnen worden?

De leden van de SP-fractie lezen dat de klachtbehandeling nu wordt ondergebracht bij de CTIVD en niet langer bij de Nationale ombudsman. Deze leden vragen waarom de Nationale ombudsman hierover niet is geconsulteerd. De Raad van State, de Nationale ombudsman en de Raad voor de Rechtspraak spreken over de onwenselijkheid van de schijn van belangenverstrengeling en partijdigheid. Kan de regering hier nader op in gaan? Waarom voldoet de Nationale ombudsman niet als klachteninstituut?

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

De leden van de CDA-fractie constateren dat in het voorliggende wetsvoorstel de CTIVD niet langer zal fungeren als klachtadviseur, maar wordt gepositioneerd als onafhankelijke, zelfstandige klachtinstantie. De regering motiveert dit met een verwijzing naar het kabinetsstandpunt naar aanleiding van het advies van de commissie Dessens. Deze leden 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 komt te vervallen. Hoeveel klachten over de AIVD en de MIVD behandelt de Nationale ombudsman jaarlijks? Zijn er problemen geconstateerd ten aanzien van de klachtbehandeling door de Nationale ombudsman, en zo ja, van welke aard waren die?

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. Deelt de regering de mening van deze leden dat daarom elke vorm van schijn van partijdigheid bij het afhandelen van deze klachten dient te worden vermeden? Deelt de regering de mening, dat bij klachtbehandeling onafhankelijkheid en onpartijdigheid essentieel zijn? Deelt de regering de mening, dat zelfs elke schijn van afhankelijkheid en partijdigheid dient te worden vermeden? Deelt de regering dat het onderbrengen van klachtbehandeling bij dezelfde instantie die toezicht houdt, de schijn van partijdigheid heeft?

Verder vragen deze leden, 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?

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

De leden van de D66-fractie hebben in het openbare gesprek met de CTIVD begrepen dat de CTIVD versterkt moet worden om haar taken ook na invoering van voorliggend wetsvoorstel goed te kunnen uitvoeren. Dat ziet niet alleen op de toegenomen rol in de klachtbehandeling, maar ook op de uitoefening van het toezicht. Wat deze leden betreft onderkent de CTIVD terecht de noodzaak om naast juristen ook ICT-deskundigen te werven, om zodoende ook op de technische werking van de interceptie en data-analyse goed (systeem)toezicht te kunnen houden. Van de in de financiële paragraaf van de toelichting vermelde extra middelen – 1 miljoen euro voor de CTIVD en TIB tezamen – vrezen deze leden dat het ontoereikend zal zijn. Alleen al de eerste slagen ter versterking van de CTIVD omvatten zo begrepen deze leden al bijna dat bedrag. Kan de regering garanderen dat de CTIVD en de TIB toereikende middelen tot hun beschikking hebben voor toezicht (en autorisatie in het geval van de TIB) dat van minstens hetzelfde niveau is als momenteel plaatsvindt? Op welke wijze wil de regering inzichtelijk maken dat dit bedrag ook daadwerkelijk het benodigde bedrag voor goed toezicht is? Hoe wordt er zorg voor 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?

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

De leden van de D66-fractie hebben een brief ontvangen van de Nationale ombudsman waarin hij zijn onvrede uit over het bij hem wegvallen van de klachtbehandeling ten aanzien van de diensten. Eén van zijn zorgpunten is de onafhankelijke klachtbehandeling. Kan de regering 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? Kan daarbij ook ingegaan worden 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? Indien niet totale onafhankelijkheid gegarandeerd kan worden, waarom is er dan toch voor gekozen de klachtbehandeling in zijn geheel bij de CTIVD te leggen? Daarnaast wijst de Nationale ombudsman op het feit dat burgers mogelijkerwijs niet weten dat zij voor klachten over de AIVD en MIVD niet

bij hem maar bij de CTIVD moeten zijn. Dat lijkt deze leden een oplosbaar probleem, wanneer goed doorverwezen wordt. Is de regering zo nodig bereid daarover het gesprek met de CTIVD en de Nationale ombudsman aan te gaan teneinde hiervoor een goede oplossing te vinden?

De leden van de PvdA-fractie lezen dat de klachtbehandeling zoals die nu is belegd bij de Nationale ombudsman, overgaat naar de CTIVD. Bij de CTIVD zal daarvoor een aparte afdeling worden ingericht. Aangezien de CTIVD ook toezicht op de diensten houdt, krijgt de CTIVD daarmee dus twee taken. Hoewel de afdeling klachtafhandeling en de afdeling toezicht strikt gescheiden zullen worden, kunnen de leden van de PvdA-fractie in navolging van de Raad voor de Rechtspraak en de Afdeling (Raad van State) zich toch voorstellen dat het tenminste in de ogen van (potentiële) klagers er de schijn van partijdigheid kan bestaan. In het licht daarvan begrijpen deze leden dan ook niet waarom het niet toch beter zou zijn als de klachtbehandeling bij de Nationale ombudsman zou blijven. Kan de regering hier nader op in gaan?

8. Geheimhouding

De fracties hebben hierover geen vragen en opmerkingen.

9. Grondrechtelijke en mensenrechtelijke aspecten

De leden van de CDA-fractie merken op dat de regering aangeeft dat het stellen van limieten aan de bewaartermijnen van gegevens bij de inzet van interceptiebevoegdheden een belangrijke waarborg is volgens de jurisprudentie van het EHRM (memorie van toelichting, blz. 209). Hoe verhoudt deze bewaartermijn (maximaal drie jaar voor gegevens die zijn verkregen door middel van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie) zich tot de eis van proportionaliteit, zoals die voortvloeit uit het EVRM, zo vragen deze leden. Kan de regering aangeven op basis van welke objectieve criteria de bewaartermijn van drie jaar voor de inhoud van communicatie niet bekort kan worden en waarom deze strikt noodzakelijk is?

Deze leden vragen de regering daarbij in het bijzonder te reflecteren op het feit dat landen als het Verenigd Koninkrijk en Duitsland weliswaar 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 (memorie van toelichting, bijlage 5). In de praktijk kan het Britse GCHQ grote verzamelingen metadata ongeveer zes maanden bewaren; het metadatasysteem van de Duitse BND slaat deze gegevens slechts 90 dagen op.

Deze leden vragen de regering ook te reageren op de suggestie van de CTIVD om onderscheid te maken tussen de bewaartermijn voor metadata en voor de inhoud van gegevens.

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? Kan de regering ook 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? Waarom is massale inbreuk op de privacy en grondrechten van Nederlanders dan nog gerechtvaardigd?

De leden van de D66-fractie constateren dat veel Europese landen de diensten ruimere bevoegdheden of minder toezicht toekennen voor de inzet van bevoegdheden in het buitenland. Kan de regering toelichten wat voor bevoegdheden de diensten van de in de memorie van toelichting genoemde landen in Nederland kunnen uitoefenen? Kan de regering toelichten of de bevoegdheden van de diensten sinds de Snowden onthullingen over het algemeen zijn ingeperkt of uitgebreid? In hoeverre is daarbij, en ook in het voorliggende wetsvoorstel, rekening gehouden met de zorgen van mensen over massa-surveillance n.a.v. de Snowden onthullingen?
De leden van de D66-fractie hebben recent met veel interesse het boek Global Intelligence Oversight. Governing Security in the Twenty-First Century (Goldmann en Rascoff (ed.), OUP, 2016) gelezen. Uit dat boek volgt een visie waarin diensten zich wereldwijd aan elkaar spiegelen, waarin best practices elkaar kunnen versterken, maar worst practices eveneens. Kent de regering dit boek? Hoe beziet zij de in de verschillende bijdragen gedane analyses? Hoe draagt dit wetsvoorstel eraan bij dat de Nederlandse diensten hun buitenlandse collega's ten positieve beïnvloeden aangaande de uitoefening van hun taken met respect voor de wet en voor burgerlijke vrijheden?

10.1 Duitsland (§10.2 m.v.t.)

De leden van de D66-fractie vragen de regering toe te lichten op welke vlakken de recente aanscherping van de wetgeving omtrent de diensten is veranderd. Deze leden constateren voorts dat Duitse diensten een verzoek tot bulkinterceptie moeten motiveren met antwoorden op de vragen wat? (welke zoektermen, type internetverkeerd, etc.), waar? (welke regio/stad/wijk), hoeveel? (hoeveel van de totale informatie stroom met een maximum van 20%) en hoe lang? (met een maximum van 3 maanden). Waarom heeft de regering niet voor deze criteria gekozen?

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

De leden van de VVD-fractie zouden graag willen weten of omringende landen gebruik mogen maken van kabelinterceptie. En zo ja, hoe het toezicht daarop is geregeld en hoe dit zich verhoudt tot het voorliggende wetsvoorstel.

11. Financiële gevolgen voor het Rijk en het bedrijfsleven

De leden van de SP-fractie denken dat met de uitbreiding van de bevoegdheden, vooral waar het gaat om het verwerken van grote hoeveelheden data, ook een personeelsuitbreiding bij de diensten noodzakelijk is. Kan de regering garanderen dat de vrijgemaakte € 21 miljoen voldoende is om zowel het uitgebreide toezicht als de noodzakelijke toename in fte's te financieren? Kan de regering garanderen dat dit niet ten koste zal gaan van de inzet van het huidige personeel en de capaciteiten van de diensten?

De leden van de CDA-fractie merken op dat de regering stelt dat de financiële gevolgen van het voorliggende wetsvoorstel voor het bedrijfsleven zeer beperkt zullen zijn (memorie van toelichting, blz. 224). Deze leden onderkennen dat de overheid in principe niet de investeringskosten vergoedt aan bedrijven waaraan de verplichting wordt opgelegd om mee te werken aan de uitvoering van een overheidstaak. Deze leden onderschrijven het standpunt van de regering, dat in dit geval een kostenvergoeding naar redelijkheid wel opportuun en aan de orde is.
De kring van aanbieders bestaat in het voorliggende wetsvoorstel niet alleen uit de traditionele aanbieders van openbare telecommunicatienet-

werken en openbare telecommunicatiediensten, maar ook andersoortige aanbieders van communicatiediensten, zoals aanbieders van hosting- en clouddiensten. De leden van de CDA-fractie zijn het met de regering eens, dat het voor deze groep aanbieders – anders dan voor openbare aanbieders – niet redelijk is te verwachten dat vooraf reeds organisatorische en technische maatregelen worden getroffen om interceptie te kunnen faciliteren. Is de conclusie van deze leden juist, dat alleen een concreet verzoek om interceptie voor de bedoelde aanbieders kosten met zich meebrengt?

De leden van de D66-fractie constateren dat veel bedrijven – van grote technologie bedrijven zoals Google en Microsoft, tot ICT-bedrijven als KPN en Tele2 en digitale infrastructuur bedrijven samengebracht in DINL – zorgen hebben over het digitale vestigingsklimaat van Nederland en aantasting van de positie van de Digitale Mainport. Ook constateren deze leden dat de regering verzuimd heeft de economische gevolgen van dit wetsvoorstel te onderzoeken. Is de regering bereid 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? Is de regering van mening dat dergelijk onderzoek bijdraagt aan een zorgvuldige afweging van alle verschillende belangen (privacy, economisch, veiligheid) die geraakt worden door dit wetsvoorstel?

De leden van de ChristenUnie-fractie constateren dat de wettelijke bevoegdheden flink uitbreiden. Geldt dat ook voor de middelen die beschikbaar komen om daarop toezicht te houden? Kan de regering de door haar verwachte budgettaire effecten voor het toezicht op die bevoegdheden nader onderbouwen en aangeven waarom zij meent dat daarmee effectief toezicht mogelijk is? Bent u bereid de Algemene Rekenkamer te vragen een toets te doen op het noodzakelijk budget voor effectief toezicht op deze wet?

De leden van de GroenLinks-fractie lezen in de memorie van toelichting dat voor het voorliggende wetsvoorstel een verhoging van het budget van € 20 miljoen structureel voor de diensten is geraamd, en dat dit volgens de regering gebaseerd is op «technisch onderzoek en ervaringsgegevens». Deze leden verzoeken de regering om de Kamer inzicht te geven in dit technisch onderzoek en deze ervaringsgegevens, opdat de Kamer kan controleren of deze financiële raming toereikend is. Deze leden vragen een uitsplitsing van de opbouw van de geraamde kosten.
De leden van de GroenLinks-fractie vragen of de regering bereid is om de financiële impact van het voorliggende wetsvoorstel te laten onderzoeken door een onafhankelijke partij. Deze leden constateren dat er aan de hand van dit wetsvoorstel aanzienlijke wijzigingen zullen plaatsvinden in de modus operandi van de diensten, en achten het daarom noodzakelijk dat goed wordt onderzocht welke financiële risico's zijn gemoeid met het invoeren van het voorliggende wetsvoorstel.

12. Consultatie, privacy impact assessment en notificatie

De leden van de CDA-fractie 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 te allen tijde onder Nederlandse wetgeving geborgd is.

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 een sleepnet(bevoegdheid). Kan de regering garanderen dat er geen sleepnet wordt ingezet?

In de publieke opinie wordt gesproken over het sleepnet. Deze leden zouden graag willen weten of dit terecht is. Is dit naar de mening van de regering een terecht of onterecht gebruikte term?

Nederland kent een digitale infrastructuur van formaat. Daarom vestigen veel bedrijven zich hier ook en slaan hier in Nederland hun data op. Graag zouden de leden van de VVD-fractie willen weten welke garanties zijn er om zeker te stellen aan buitenlandse bedrijven dat het opslaan van data in Nederland 100% veilig kan.

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

De leden van de PvdA-fractie begrijpen dat indien er verschoningsgerechtigden betrokken zijn, de toestemming voor het gebruik van bevoegdheden voorafgaande toestemming van de rechter vereist is. Tot de kring van verschoningsgerechtigden worden in het voorliggend wetsvoorstel advocaten en journalisten gerekend. Dit omdat deze beroepsgroepen een belangrijke rol in de borging van belangrijke aspecten van de democratische rechtsstaat spelen. Waarom geldt deze overweging niet ten aanzien van andere verschoningsgerechtigden, zoals notarissen?

In dit verband vragen de leden van de PvdA-fractie zich ook af of de bronbescherming wel afdoende wordt geregeld. Wat is de meerwaarde van het desbetreffende afzonderlijke wetsvoorstel tot bronbescherming in geval van de diensten, indien die diensten via de bulkinzameling 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 zijn cliënt, niet vernietigd te worden als deze zijn vergaard zonder tussenkomst van de rechter?

Ook in dit verband van verschoningsrecht en bronbescherming vragen de leden van de PvdA-fractie zich af of beveiligde journalistieke omgevingen niet dezelfde bescherming zouden moeten hebben zoals de journalisten zelf. Bijvoorbeeld dat de medewerkingsplicht tot ontsleuteling net voor beveiligde journalistieke omgevingen, zoals Publeaks zou moten gelden. Wat is de mening van de regering hierover?

Onder andere de Autoriteit Persoonsgegevens wijst er op dat de grootschalige verzameling, opslag en analyse van gegevens door de diensten, ertoe kan leiden dat burgers hun gedrag hierop aanpassen. Journalisten vrezen bij gebrek aan een goede bronbescherming, bronnen er van zullen afzien om contact met journalisten op te nemen. Wat is de mening van de regering over een dergelijk «chilling effect»?

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

De leden van de D66-fractie vinden het terecht dat de regering een PIA heeft laten uitvoeren op het voorliggende wetsvoorstel. Dit wetsvoorstel biedt de diensten immers de mogelijkheid om persoonsgegevens van burgers te onderscheppen en te analyseren en om apparatuur van

burgers te hacken en verzamelde gegevens uit te wisselen met de Nationale politie en met buitenlandse diensten.

Allereerst willen de leden van de D66-fractie aanhalen wat door de DG AIVD is gezegd over gegevensverzameling door de AIVD en privacy. In een interview met de Volkskrant in september 2016 zegt de DG AIVD het volgende: «Zouden mensen die privacy als hoogste goed zien, dat nog zo hebben als zij slachtoffer van een aanslag zijn?» Deze leden hebben zich gestoord aan deze bedreigende uitlating van de DG AIVD. Niet alleen doet dat het grondrecht privacy in onze rechtsstaat ernstig tekort, het wekt bovendien de misplaatste suggestie van een correlatieve causaliteit tussen privacybescherming en terroristische aanslagen. Deze leden vragen de regering hierop te reageren en te verduidelijken hoe we deze opmerking moeten zien tegen 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.

Kan de regering naast een reactie op de PIA ook expliciet toelichten hoe dit wetsvoorstel zich verhoudt tot de op 21 december 2016 gepubliceerde uitspraak van het Hof van Justitie over dataretentie?

De leden van de D66-fractie brengen in herinnering dat zij reeds eerder hebben gepleit voor een extra privacy-stoel bij de CTIVD, zodat die deskundigheid ook in het toezicht goed is gewaarborgd. Waarom wordt daaraan geen uitvoering gegeven?

Alhoewel een formeel advies van de Autoriteit Persoonsgegevens bij de memorie van toelichting naar mening van de leden van de D66-fractie onterecht ontbreekt merken deze leden op dat in een aparte reactie de autoriteit stelt dat de (nieuwe) bevoegdheden van de diensten onmiskenbaar gevolgen zullen hebben voor Nederlandse burgers, en in het bijzonder voor het recht op bescherming van de persoonlijke levenssfeer. Er bestaat volgens de autoriteit een reële kans dat de introductie van deze bevoegdheden een negatieve invloed heeft op fundamentele vrijheden die ten grondslag liggen aan de Nederlandse rechtsstaat. De autoriteit verwijst daarbij naar een belangrijke waarschuwing van het EHRM dat «a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it».(EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 106.) Kan de regering, in aanvulling op zijn analyse van deze uitspraak in de memorie van toelichting, reageren op deze waarschuwing en op welke wijze zij meent dat deze waarschuwing niet aan dovemans oren is gericht van het voorliggende verstrekkende wetsvoorstel? Is de regering voorts bereid om in te gaan op alle punten die de autoriteit in een aparte reactie ten behoeve van het rondetafelgesprek in de Kamer naar voren brengt over dit wetsvoorstel?

II. ARTIKELEN

Artikel 2

De leden van de SGP-fractie vragen naar de betekenis van de bepaling dat de diensten en de coördinator hun taak uitvoeren in gebondenheid aan de wet. Hoewel deze bepaling ook in de bestaande wet staat, vragen zij zich af of dit een logische bepaling is. Deze leden delen uiteraard dit uitgangspunt. Maar wel vragen zij zich af of niet van iedere (overheids-)dienst verwacht mag worden dat binnen de regels van de wet wordt

gewerkt? Kan worden aangegeven waarom in deze wet in het verleden is gekozen voor het opnemen van deze bepaling? Wordt met het gebruikelijke slotformulier van de wet niet hetzelfde beoogd?

De voorzitter van de commissie,
Pia Dijkstra

De griffier van de commissie,
Van der Leeden