Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2023-2024

36 263 Tijdelijke regels inzake specifieke wettelijke voorzieningen voor het uitvoeren van onderzoeken door de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen alsmede voorzieningen inzake de mogelijkheid tot vaststelling van een nieuwe eindtermijn voor gebruik door de diensten van in het kader van hun taakuitvoering met bijzondere bevoegdheden verworven bulkdatasets en de invoering van een bindende toets ex ante van verleende toestemmingen voor de real time interceptie van verkeers-en locatiegegevens (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen)

E **NOTA NAAR AANLEIDING VAN HET VERSLAG**
Ontvangen 24 januari 2024

Wij hebben met veel belangstelling kennisgenomen van de vragen en opmerkingen van de leden van de fracties van de GroenLinks/PvdA, CDA, D66 en BBB, PVV, ChristenUnie, PvdD en Volt. Wij gaan daar graag op in. Daarbij zal zoveel mogelijk de indeling van het verslag worden gevolgd. Waar dat dienstig is zullen gelijkluidende vragen van de leden van de diverse fracties worden samengenomen en worden beantwoord.

1. Inleiding
De fractieleden van GroenLinks-PvdA hebben kennisgenomen van het wetsvoorstel en hebben naar aanleiding daarvan een aantal vragen. De fractieleden van Volt sluiten zich graag bij deze vragen aan.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Daarover stellen zij nog graag een aantal vragen.

De D66-fractieleden hebben met betrekking tot het wetsvoorstel nog een aantal vragen. De leden van de BBB-fractie sluiten zich graag bij deze vragen aan.

De PVV-fractieleden hebben kennisgenomen van het wetsvoorstel en hebben een aantal vragen.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Deze leden willen geen twijfel laten bestaan over het belang en de urgentie die zij hechten aan onderzoek door de diensten naar landen met een offensief cyberprogramma dat is gericht tegen Nederland of Nederlandse belangen. De inzet van de daarvoor benodigde bevoegdheden gaat echter bijna noodzakelijkerwijs ook gepaard met het vergaren, verkrijgen, verwerken en bewaren van heel veel gegevens die de privacy van niet-betrokken burgers, bedrijven en organisaties raakt. Voor de leden van de ChristenUnie-fractie is dit een nadrukkelijk punt van aandacht en geeft het alle aanleiding voor scherpe juridische kaders, stevig toezicht en effectieve toetsing door de rechter. Zij hebben daarom nog enkele vragen.

De leden van de fractie van de PvdD hebben een aantal vragen. Zij verzoeken de regering om alle (sub)vragen afzonderlijk te beantwoorden.

De fractieleden van Volt hebben kennisgenomen van het wetsvoorstel en stellen graag nog enkele vragen.

Alvorens wij ingaan op de gemaakte opmerkingen en gestelde vragen willen we in algemene zin nog het volgende opmerken. Deze Tijdelijke wet is noodzakelijk omdat de dreiging van landen met een offensief cyberprogramma onverminderd groot is en zelfs toeneemt. In dit verband wordt verwezen naar de jaarverslagen van de AIVD en MIVD over het jaar 2022. De knelpunten die met de Tijdelijke wet opgelost moeten worden, worden groter. De cyberdreigingen zijn in de afgelopen jaren toegenomen, terwijl het zicht op de dreiging van landen met een offensief cyberprogramma verder is afgenomen.[1] Landen als China, Rusland, Iran en Noord-Korea zetten op grote schaal digitale aanvallen in. Deze landen opereren offensief, opportunistisch en houden zich niet aan de rechtstatelijke principes en regels zoals wij dat doen. Doelwitten zijn persoonsgegevens, belangrijke hightech innovaties, politieke standpunten, militaire geheimen, kwetsbaarheden van onze vitale infrastructuur, informatie over dissidenten en nog veel meer. Het gaat dus om economische schade, militaire schade, fysieke schade en/of geopolitieke schade veroorzaakt bij zowel Nederlandse organisaties als ook individuele Nederlanders. Bijvoorbeeld doordat routers van Nederlanders worden gebruikt vanuit Rusland door hackers van de GRU (Russische militaire inlichtingendienst). Of doordat persoonsgegevens van Nederlandse burgers worden buitgemaakt. De AIVD zag dit in 2022 gebeuren toen verschillende landen met offensieve cyberprogramma's probeerden data te stelen in de (Europese) reis- en luchtvaartsector.[2] Ook hebben de diensten in het afgelopen jaar gezien dat Russische staatshackers een cyberoperatie aan het voorbereiden waren waarbij de website van een Nederlandse overheidsinstelling zou worden misbruikt. De hackers maakten een kopie van deze overheidswebsite om bezoekers daarvan te kunnen infecteren met malware om ze hiermee te kunnen bespioneren. In potentie kunnen de gegevens van Nederlandse burgers die hackers buitmaken gebruikt worden voor allerlei doeleinden. Een ander voorbeeld zijn Russische desinformatiecampagnes rond MH17. Voor landen met een offensief cyberprogramma kunnen Nederlandse burgers een middel zijn om bepaalde doelen (beïnvloeding, spionage, sabotage) te bereiken. De Nederlandse infrastructuur is hier bij uitstek in het vizier vanwege het feit dat Nederland in het wereldwijde communicatienetwerk een belangrijk knooppunt is. Landen zetten een offensief cyberprogramma in de vorm van cyberoperaties veelal in als onderdeel van een bredere offensieve strategie, waarbij ook andere – meer klassieke – operaties worden ingezet, teneinde hun geopolitieke doelstellingen te bereiken. Deze operaties vormen ook onderdeel van een militaire strategie. Deze aanpak van die landen wordt ook wel een *whole-of-society* approach genoemd. Dat vergt van de AIVD en MIVD een integrale wijze van onderzoek naar die landen waar de dreiging vanuit gaat. De diensten doen daarbij onderzoek naar hun doelwitten, intenties, capaciteiten en wijze van aansturing. Om deze vragen te kunnen beantwoorden is het nodig om naar meer dan alleen de specifieke cyberaanval te kijken. Cyberaanvallen worden niet uitgevoerd als doel op zich, maar als onderdeel van een integrale strategie. De diensten moeten dan ook integraal onderzoek doen naar het land achter de aanval, zodat zij zicht krijgen op de herkomst, aansturing, politieke intenties, capaciteiten, doelwitten en slachtoffers van de cyberaanvallen. Het is nodig zicht te krijgen op welke infrastructuur cyberactoren gebruiken, welke personen of organisaties daarachter zitten en wat hun modus operandi is. Pas dan kunnen de diensten beter zicht krijgen op de dreiging die van de landen uitgaat. Dat zicht hebben de diensten nu onvoldoende. Deze wet gaat daar een belangrijke bijdrage aan leveren. In het wetgevingstraject is veel aandacht geweest voor een passend stelsel van waarborgen. In het wetsvoorstel is geborgd dat de waarborgen op een hoog niveau blijven, onder andere door de introductie van bindend toezicht door de CTIVD.

2. Inhoud van het wetsvoorstel op hoofdlijnen

De fractieleden van GroenLinks-PvdA stellen dat de Raad van State constateert dat met deze tijdelijke wet, naast de bestaande wet, de nodige complexiteit wordt geïntroduceerd. Deze leden vragen de regering hoe de verschillende (toezicht)regimes zich tot elkaar verhouden. Hierna volgt een voorbeeld van deze complexiteit. Op basis van het voorstel voor de tijdelijke wet betekent dit bijvoorbeeld bij de inzet van de hackbevoegdheid het volgende:
- de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB) beoordeelt het binnendringen in het geautomatiseerde werk vooraf (bindend);
- de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD) kan het verkennen van het geautomatiseerde werk tijdens de inzet beoordelen (bindend);
- de CTIVD kan tijdens het binnendringen de genomen technische risico's, de gebruikte onbekende

[1] AIVD Jaarverslag 2022, p. 29 en MIVD Jaarverslag 2022, p. 31.
[2] AIVD Jaarverslag 2022, p. 29.

kwetsbaarheden en bijgeschreven geautomatiseerde werken beoordelen (bindend);
- de CTIVD kan tijdens het binnendringen de verdere inzet en uitvoering beoordelen (niet bindend);
- de Afdeling bestuursrechtspraak van de Raad van State kan uitspraak doen in een beroep van een minister tegen een van de hierboven genoemde bindende oordelen van de toezichthouders (bindend);
- de afdeling klachtbehandeling van de CTIVD kan een klacht over de inzet beoordelen (bindend).

De leden van de fractie van GroenLinks-PvdA vragen een algemene reflectie van de regering op deze complexiteit. Wat gaat dit concrete voorbeeld betekenen voor operationele snelheid en wendbaarheid? Wat gaat de tijdelijke wet in algemene zin betekenen voor de gewenste operationele snelheid en wendbaarheid? Was deze geïntroduceerde complexiteit onderdeel van de uitvoeringstoets? Zo ja, wat was de conclusie? Zo nee, waarom niet? Wij reageren hierop graag als volgt.

Dit wetsvoorstel stelt de AIVD en MIVD in algemene zin in staat effectiever onderzoek te doen naar landen met een offensief cyberprogramma. Juist in het cyberdomein zijn snelheid en wendbaarheid de norm en cruciaal. In het cyberdomein is het immers, in tegenstelling tot het fysieke domein, voor personen en organisaties waar de diensten onderzoek naar doen zeer eenvoudig om snel en vaak te wisselen van locatie en wereldwijd en ongezien te werk te gaan. Het is van belang om daarop zicht te krijgen en te behouden en mee te kunnen bewegen met dergelijke veranderingen. De Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) biedt – zo blijkt ook uit het rapport van de evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017 (ECW) – de genoemde snelheid en wendbaarheid onvoldoende, waardoor de diensten onvoldoende in staat zijn de dreigingen in het cyberdomein op een adequate manier te onderzoeken en tegen te gaan.

Als het gaat om het door deze leden genoemde voorbeeld over de inzet van de hackbevoegdheid in de context van complexiteit, snelheid en wendbaarheid merken wij het volgende op. De Tijdelijke wet voorziet als het gaat om de hackbevoegdheid in drie aanpassingen op het bestaande stelsel in de Wiv 2017.

Ten eerste wordt het toestemmingsniveau voor de bevoegdheid tot verkennen bij hacken belegd bij het hoofd van de dienst, in plaats van bij de betrokken minister, en verdwijnt daarop de rechtmatigheidstoets van de TIB. Het toestemmingsniveau wordt op deze manier in overeenstemming gebracht met de zwaarte van de inbreuk die gepaard gaat met de verkenning (die in het geval van een verkenning zeer gering is). Daarnaast zorgt deze verschuiving van het toestemmingsniveau in combinatie met het wegvallen van de TIB-toets er voor dat sneller kan worden geopereerd. Daarbij wordt de TIB-toets vervangen door bindend toezicht tijdens en nadien van de afdeling toezicht van de CTIVD.

Ten tweede wordt mogelijk gemaakt dat kenmerken die niet exclusief aan het onderzoeksubject toebehoren, zonder voorafgaande rechtmatigheidstoets van de TIB bijgeschreven kunnen worden op een hacklast. De Tijdelijke wet verduidelijkt dat binnen de bandbreedte van een reeds lopende hackoperatie intern toestemming kan worden gegeven voor deze bijschrijvingen zodat niet telkens een nieuwe toestemming hoeft te worden verkregen waarvoor vervolgens het oordeel van de TIB ter zake moet worden afgewacht. Bijschrijven zorgt op deze manier voor de noodzakelijke snelheid en wendbaarheid tijdens de uitvoering van de hackoperatie, doordat tijdens de hackoperatie het binnendringen in een geautomatiseerd werk en het onderzoek van dit werk ononderbroken kan worden voortgezet. Indien echter – zoals in de huidige situatie - een nieuwe toestemming moet worden aangevraagd en vervolgens een TIB-toets moet plaatsvinden, komen operaties stil te liggen waardoor inlichtingenposities verloren gaan. De TIB oordeelt overigens wel weer over de bijgeschreven kenmerken in de toestemming voor verlenging die na akkoord van de minister aan de TIB ter toetsing worden voorgelegd.

Ten derde regelt de Tijdelijke wet dat alleen bekende technische risico's vooraf door de TIB worden getoetst en dat technische risico's, inclusief onbekende kwetsbaarheden, die tijdens de uitvoering van de hackoperatie bekend worden of zich manifesteren, onder het bindend toezicht van de afdeling toezicht van de CTIVD vallen. Deze wijziging beoogt snelheid in de opstartfase van hackoperaties te bewerkstelligen en het is tevens een praktijk die past bij de dynamiek van het cyberdomein.

Bij de voorbereiding van dit wetsvoorstel is doorlopend aandacht geweest voor de uitvoerbaarheid. Zo zijn er verschillende uitvoeringstoetsen uitgevoerd op basis van (op dat moment beschikbare) concepten van het wetsvoorstel. De uitvoeringstoetsen bestonden onder meer uit ketentesten met de TIB, de afdeling toezicht van de CTIVD en de Afdeling bestuursrechtspraak van de Raad van State. Bij deze ketentesten is het conceptwetsvoorstel met alle betrokken partners doorlopen aan de hand van fictieve casussen. Met de uitkomsten van de uitvoeringstoetsen is rekening gehouden bij het opstellen van het wetsvoorstel.

Ten opzichte van het bestaande wettelijke kader worden met deze Tijdelijke wet geen bevoegdheden geïntroduceerd die niet al onder de Wiv 2017 door de diensten zouden kunnen worden ingezet. De belangrijkste wijzigingen zien op het bevorderen van de effectieve inzet en uitvoering van enkele belangrijke bevoegdheden. De organisaties zijn daar al op toegerust. Wel wordt de werking van het stelsel van toetsing en toezicht gewijzigd. Een van de wijzigingen betreft de introductie van een beroepsmogelijkheid bij de Raad van State. Hiervoor zullen de diensten extra juridische expertise werven.

De diensten zijn momenteel bezig met het finaliseren van nieuw en aanvullend beleid, werkinstructies, processen en techniek om effectief de Tijdelijke wet te kunnen uitvoeren, waarbij als uitgangspunt het aangenomen wetsvoorstel van de Tweede Kamer wordt genomen. Ook moeten aanpassingen worden gedaan aan verschillende technische verwervings- en verwerkingsketens. Het is binnen de bestaande omvang van de organisaties mogelijk om deze implementatie te realiseren. Dit zal echter wel verdringingseffecten hebben op andere IT-veranderdoelstellingen van beide organisaties. De diensten werken via diverse IT-trajecten aan het eigen informatielandschap. Dat volgt mede uit de bevindingen van de afdeling toezicht van de CTIVD bij de implementatie van de Wiv 2017. De aanvullende eisen die de Tijdelijke wet aan de diensten stelt worden waar mogelijk bij deze IT-trajecten betrokken. Deze verdringingseffecten zijn in kaart gebracht en wordt actief gestuurd op prioritering.

Opgemerkt dient te worden dat de beoogde operationele snelheid en wendbaarheid als gevolg van dit wetsvoorstel niet altijd zal leiden tot een vermindering van administratieve lasten, omdat er nog steeds toestemmingsaanvragen geschreven moeten worden, de diensten een aantekeningsplicht hebben en het toezicht verschuift van vooraf naar tijdens de uitvoering.

De regering erkent dat het introduceren van een Tijdelijke wet-regime, in aanvulling op het Wiv 2017-regime, een (beperkte) toename van complexiteit betekent doordat twee wettelijke regimes naast elkaar bestaan. Daar staat tegenover dat wordt voorzien in passend toezicht. Door op enkele punten de toetsing vooraf te verschuiven naar bindend toezicht tijdens de uitvoering van bevoegdheden, zal er aan de voorkant sprake zijn van minder administratieve lasten, maar zal er in totaal een toename van administratieve lasten zijn vanwege de aangepaste rol van de afdeling toezicht van de CTIVD in het kader van de uitvoering van bindend toezicht en daarnaast vanwege de beroepsmogelijkheid bij de Afdeling bestuursrechtspraak.

Wij hebben er vertrouwen in dat de Tijdelijke wet zal bijdragen aan de effectiviteit van de uitvoering van de taken van de diensten en een toezichtstelsel dat aansluit bij de operationele praktijk zonder afbreuk te doen aan de waarborgen. De praktijk zal moeten uitwijzen of de met het wetsvoorstel beoogde doelen worden bereikt waarbij het succes van het voorgestelde stelsel in sterke mate zal afhangen van de bereidheid van de betrokken instanties tot rolvaste en constructieve samenwerking.

Overeenkomstig het advies van de Afdeling advisering zullen de ervaringen met de voorgestelde maatregelen dan ook worden gemonitord. Een jaar na inwerkingtreding zal conform de motie Hammelburg[3] een invoeringstoets worden uitgevoerd die ziet op de balans tussen passende waarborgen en effectieve taakuitvoering en tevens wordt er periodiek een uitvoeringsverslag opgesteld. De resultaten hiervan zullen vervolgens worden betrokken bij de herziening van de Wiv 2017.

[3] *Kamerstukken II 2022/23, 36 26, nr. 25.*

De leden van de fractie van GroenLinks-PvdA stellen vervolgens dat het wetsvoorstel dat voorligt, oorspronkelijk is gemaakt voor werk van de diensten met betrekking tot landen met een offensief cyberprogramma. In de nota van wijziging[4] wordt deze reikwijdte verbreed. De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft op 16 oktober 2023 in de Tweede Kamer het volgende gezegd:

"*Dat maakt dat de reikwijdte van de tijdelijke wet is beperkt tot onderzoeken van de diensten naar landen met een offensief cyberprogramma. Dat kan gaan over cyberoperaties, maar het kan ook gaan over interceptie op de kabel. Alle andere onderzoeken van de diensten vallen onder de Wiv.*"[5]

Dit leidt mogelijk tot verwarring en onduidelijkheid. Ook de toezichthouder TIB gaf tijdens de deskundigenbijeenkomst van 21 november 2023 in de Eerste Kamer aan dat er onduidelijkheid is over onder welk regime gegevens verzameld worden en op welke wet de dienst een beroep doet bij het inzetten van bevoegdheden. Dit kan de bron zijn van een groot aantal (uitvoerings)problemen, waarvan de implicaties lastig te overzien is. De leden vragen wat de verbreding van de reikwijdte van de tijdelijke wet betekent voor de in te zetten bevoegdheden van de diensten ten aanzien van 'verkennen'. Onze reactie hierop luidt als volgt.

De verbreding van de reikwijdte van de Tijdelijke wet als gevolg van de nota van wijziging ziet op slechts twee onderdelen die ook zijn ondergebracht in een afzonderlijk hoofdstuk (hoofdstuk 3: Overige tijdelijke voorzieningen in het kader van de taakuitvoering van de AIVD en MIVD). Uitsluitend deze voorzieningen gelden voor alle inlichtingentaken van de diensten.[6] Ten eerste is dit de regeling voor het (opnieuw) vaststellen van een eindtermijn voor het gebruik van bulkdatasets die met bijzondere bevoegdheden (met uitzondering van verkennen ten behoeve van OOG-interceptie en OOG-interceptie) zijn verworven. Ten tweede een regeling voor de real time interceptie van verkeers- en locatiegegevens (de zogeheten stomme tap). Ten aanzien van deze bevoegdheid wordt een regeling getroffen voor een bindende ex ante toets door de TIB op verleende toestemmingen voor de uitoefening van de bijzondere bevoegdheid. Aanleiding voor het opnemen van deze bepaling is een uitspraak van het Hof van Justitie van de Europese Unie.[7] De verbreding van de reikwijdte van de Tijdelijke wet heeft dus geen gevolgen voor de voorzieningen in het kader van het verkennen ten behoeve van OOG-interceptie of de bevoegdheid tot verkennen bij de hackbevoegdheid, zoals in hoofdstuk 2 van de Tijdelijke wet opgenomen.

De hiervoor gegeven uitleg is onderdeel van de parlementaire geschiedenis en beoogt duidelijkheid te verschaffen over de uitleg van de Tijdelijke wet zodat een beroepsprocedure bij de Afdeling bestuursrechtspraak op dit punt voorkomen kan worden.

De fractieleden van GroenLinks-PvdA vragen vervolgens of de regering de door de TIB voorziene onduidelijkheden ziet. Zo ja, hoe is dit te voorkomen? Zo nee, waarom niet? Wij beantwoorden deze vragen graag als volgt.

Wij zien die onduidelijkheden niet. De Tijdelijke wet ziet op onderzoeken van de diensten naar landen met een offensief cyberprogramma dat is gericht op Nederland of Nederlandse belangen. In de Geïntegreerde Aanwijzing (GA) is bepaald welke landen dit zijn. Het is de taak van de diensten te achterhalen of, hoe en waarom landen een offensief cyberprogramma uitvoeren. Daarom doen de diensten onderzoek naar de doelwitten, capaciteiten, intenties en wijze van aansturing van de betreffende statelijke actoren waarbij verder gekeken wordt dan naar een specifieke aanval. Cyberaanvallen worden door landen immers niet uitgevoerd als doel op zich, maar, naast andere meer klassieke inlichtingenmiddelen, als onderdeel van een integrale strategie gericht op het realiseren van militaire, economische of geopolitieke doeleinden. Daarbij vinden aanvallen niet uitsluitend plaats vanuit een inlichtingendienst of krijgsmacht, maar ook door of via burgers, bedrijven of instellingen of meer diffuse proxy-organisaties. Dit betekent dat de onderzoeken van

[4] *Kamerstukken II 2022/23, 36 263, nr. 10.*
[5] *Kamerstukken II 2023/24, 36 263, nr. 35, p. 50.*
[6] Daartoe worden gerekend: de in artikel 8, tweede lid, onder a en d, en artikel 10, tweede lid, onder a, c en e Wiv 2017 bedoelde taken.
[7] Hof van Justitie van de Europese Unie, 6 oktober 2020, gevoegde zaken C-511/18, C-512/18 en C-520/18 (Quadrature du Net e.a.).

de diensten ook hierop gericht dienen te zijn. De Tijdelijke wet is dus van toepassing op elk onderzoek van de diensten naar landen met een offensief cyberprogramma die worden genoemd in de GA met een dergelijke doelstelling, gericht op Nederland of Nederlandse belangen. Daarnaast kan de Tijdelijke wet van toepassing zijn als een digitale aanval (nog) niet (direct) te attribueren is aan een land, maar er wel een vermoeden is dat deze te attribueren is aan een statelijke actor.

De hiervoor gegeven uitleg is onderdeel van de parlementaire geschiedenis en beoogt duidelijkheid te verschaffen over de uitleg van de Tijdelijke wet zodat een beroepsprocedure bij de Afdeling bestuursrechtspraak op dit punt voorkomen kan worden.

Ingeval een target van de dienst in verschillende onderzoeken van de dienst is betrokken, waaronder een onderzoek naar landen met een offensief cyberprogramma, en vanuit die verschillende onderzoeken de inzet van een bijzondere bevoegdheid jegens dat target wordt overwogen, dan zal een ad hoc afweging dienen plaats te vinden voor welk onderzoek de inzet van die bijzondere bevoegdheid en de daarmee te verkrijgen gegevens het grootste belang heeft oftewel waar het zwaartepunt van het onderzoek naar het target ligt. Als dat zwaartepunt bij het onderzoek naar landen met een offensief cyberprogramma ligt, dan kan de toepasselijkheid van de Tijdelijke wet worden ingeroepen. Of de diensten hierin een juiste afweging hebben gemaakt kan, nu de toepasselijkheid van de Tijdelijke wet altijd expliciet in een verzoek om toestemming voor de inzet van een bijzondere bevoegdheid moet worden bepaald, door de TIB worden getoetst.

De leden van de GroenLinks-PvdA-fractie vragen ook of het klopt dat de bevoegdheden onder het regime van de tijdelijke wet ook mogen worden ingezet voor onderzoeken die niet onder de tijdelijke wet vallen. Ons antwoord op deze vraag luidt als volgt.

Het wetsvoorstel bevat een aantal specifieke voorzieningen ten behoeve van onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Deze voorzieningen betreffen een aantal reeds in de Wiv 2017 geregelde bijzondere bevoegdheden en gelden bij toepassing van de Tijdelijke wet deels in aanvulling en deels in afwijking van de Wiv 2017. Alleen artikel 6 (verkennen ten behoeve van OOG-interceptie) is een zelfstandige bijzondere bevoegdheid die alleen op grond van de Tijdelijke wet kan worden toegepast. De hier bedoelde aanvullingen c.q. afwijkingen van de in de Wiv 2017 geregelde bijzondere bevoegdheden kunnen alleen worden ingeroepen indien sprake is van een onderzoek naar een land met een offensief cyberprogramma en indien dit overeenkomstig artikel 2, derde lid, van de Tijdelijke wet in een verzoek om toestemming is aangegeven. Die kunnen dus niet worden toegepast voor onderzoeken die niet onder de Tijdelijke wet vallen.

Daarnaast bevat de Tijdelijke wet in hoofdstuk 3 een tweetal specifieke voorzieningen die voor alle inlichtingenonderzoeken van de diensten gelden, ongeacht of het gaat om een onderzoek naar landen met een offensief cyberprogramma. Het betreft een regeling voor het vaststellen van een (nieuwe) eindtermijn voor het gebruik van bulkdatasets en de invoering van de TIB-toets op verleende toestemmingen voor de real time verzameling van verkeers- en locatiegegevens (stomme tap).

De fractieleden van GroenLinks-PvdA vragen de regering welke waarborgen zijn ingebouwd om gegevens verzameld onder de tijdelijke wet, ook conform de waarborgen in de tijdelijke wet te behandelen. Wij beantwoorden deze vraag graag als volgt.

Op de (verdere) verwerking van gegevens die worden verzameld in onderzoeken waarop ook hoofdstuk 2 van de Tijdelijke wet van toepassing is, zijn de reguliere waarborgen in de Wiv 2017 gewoon van toepassing (zie ook artikel 2, tweede lid). In slechts een beperkt aantal gevallen is voorzien in een aanpassing ten opzichte van de Wiv 2017. Dat betreft geautomatiseerde data-analyse (GDA) op OOG-metadata, waarbij in plaats van een TIB-toets (ex ante) nu wordt voorzien in bindend toezicht door de afdeling toezicht van de CTVD (ex durante en ex post). Met deze verschuiving wordt beter aangesloten bij de fase van verwerking waarin ook de beperking op het recht op bescherming van de persoonlijke levenssfeer zich het meest manifesteert en kan het toezicht dus effectiever worden ingezet; dit is een sterkere waarborg. Daarnaast wordt de verstrekking van de ingevolge artikel 6 verworven gegevens aan een buitenlandse dienst aan verdergaande waarborgen onderworpen dan thans uit de Wiv 2017 voortvloeit. Waar het gaat om

de voorzieningen in hoofdstuk 3 van de Tijdelijke wet wordt waar het gaat om de verdere verwerking van door de diensten met bijzondere bevoegdheden verworven bulkdatasets niet alleen voorzien in de mogelijkheid tot het stellen van (nieuwe) eindtermijnen voor het gebruik daarvan, maar ook in een aanvullende waarborg in de vorm van bindend toezicht door de afdeling toezicht van de CTIVD ter zake waarbij naar aanleiding van het amendement Hammelburg de afdeling toezicht in elk geval de rechtmatigheid onderzoekt van het derde opeenvolgende besluit tot het vaststellen van een nieuwe eindtermijn[8].

De leden van de GroenLinks-PvdA-fractie vragen welke maatregelen er zijn om te voorkomen dat de tijdelijke wet wordt ingezet om gegevens te verzamelen die vervolgens later ook voor andere doeleinden kunnen worden gebruikt. Wij beantwoorden deze vraag als volgt.

Voor de inzet van een bijzondere bevoegdheid onder de Tijdelijke wet moet in de toestemmingsaanvraag worden gemotiveerd waarom de Tijdelijke wet van toepassing is. De toestemming van de minister voor de inzet van deze bevoegdheid wordt vervolgens voorgelegd aan de TIB voor een rechtmatigheidstoets waarbij de TIB tevens toetst of de Tijdelijke wet terecht van toepassing is verklaard. Op deze manier wordt op verschillende momenten getoetst of de inzet van de bevoegdheid onder de Tijdelijke wet rechtmatig is. De met de inzet verkregen gegevens zullen primair van belang zijn voor een onderzoek dat binnen de reikwijdte van de Tijdelijke wet valt. Dit laat onverlet dat dergelijke gegevens voor enig ander lopend onderzoek van de diensten van belang (kunnen) zijn. In dat geval mogen de gegevens ook voor die onderzoeken gebruikt worden. Aan dit uitgangspunt is uitwerking gegeven in artikel 27, eerste lid, Wiv 2017 waarin is bepaald dat de toets op relevantie zich ook uitstrekt tot enig ander lopend inlichtingenonderzoek van de dienst dan waarvoor de gegevens initieel zijn verworven. Een vergelijkbare regeling is opgenomen in artikel 48 Wiv 2017.

De leden van de CDA-factie constateren dat de Algemene Rekenkamer in haar onderzoek uit 2021 concludeert dat de nieuwe waarborgen uit de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017) de inzet van bepaalde bijzondere bevoegdheden beperken.[9] Het is deze leden duidelijk dat het niet de bedoeling van dit wetsvoorstel is om alle onnodige beperkingen weg te nemen, en zij vragen de regering uiteen te zetten wat de mate is waarmee dat met dit voorstel wordt bereikt. Wij antwoorden de leden graag als volgt.

De Algemene Rekenkamer heeft in haar rapport over de operationele slagkracht van de diensten geconcludeerd dat de effectiviteit van de diensten onder druk staat. Dit wetsvoorstel beoogt, vooruitlopend op de brede herziening van de Wiv 2017, een deel van de geconstateerde knelpunten reeds nu te adresseren zodat de AIVD en MIVD in staat zijn effectiever onderzoek te doen naar landen met een offensief cyberprogramma, gelet op de toegenomen dreiging. Juist in het cyberdomein zijn snelheid en wendbaarheid de norm en cruciaal.

De Tijdelijke wet beoogt oplossingen te bieden om snelheid en wendbaarheid in de dagelijkse praktijk van de diensten mogelijk te maken zodat de wijze waarop de diensten onderzoek doen, beter past bij de dreiging van landen met een offensief cyberprogramma en de dynamiek van het cyberdomein. Dat gebeurt door op voor het onderzoek als hier bedoeld essentiële bijzondere bevoegdheden (met name hacken en de interceptiebevoegdheden) te voorzien in aanvullingen dan wel afwijkingen van het bepaalde in de Wiv 2017, waarbij tegelijkertijd voorzien is in daarop toegesneden waarborgen (deels anders dan in de Wiv 2017, deels in aanvulling daarop). Zo wordt in een aantal gevallen voorzien in een gedeeltelijke verschuiving van de statische TIB-toets vooraf naar bindend toezicht tijdens en na afloop van de inzet van een bijzondere bevoegdheid door de afdeling toezicht van de CTIVD, bijvoorbeeld bij GDA op OOG-metadata en bij de bevoegdheid tot het binnendringen in en het verkennen van geautomatiseerde werken. Met betrekking tot Onderzoeksopdracht Gerichte (OOG) interceptie op de kabel moet de Tijdelijke wet ervoor zorgen dat deze bevoegdheid ingezet kan gaan worden zoals dit destijds door de wetgever is bedoeld, namelijk als een bulkinterceptiemiddel onder meer bedoeld voor onderzoek naar verborgen dreigingen. Daarom is nu duidelijker toegelicht in de voorliggende wet dat er bij bulkinterceptie

[8] *Kamerstukken II 2022/23, 36 26, nr. 31.*
[9] *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt* (onderzoeksrapport Algemene Rekenkamer), Den Haag: 2021, p. 6.

sprake is van een andere mate van gerichtheid dan bij de inzet van andere bijzondere bevoegdheden. Tot slot kunnen de diensten, mits de minister daarvoor toestemming heeft verleend door een nieuwe eindtermijn vast te stellen, bulkdatasets in het geval van dringende redenen in het kader van de nationale veiligheid, langer gebruiken voor hun lopende onderzoeken.

Daarnaast geeft de Tijdelijke wet de mogelijkheid om in daarbij aangegeven gevallen een beroepsprocedure bij de Afdeling bestuursrechtspraak van de Raad van State te voeren. Daarmee wordt – zoals de ECW in haar evaluatierapport aangeeft – een weeffout in het bestaande stelsel van toetsing en toezicht hersteld. Dit biedt de mogelijkheid om bij een verschil van mening tussen de voor de dienst verantwoordelijke minister en de TIB of de afdeling toezicht van de CTIVD over de uitleg van de wet bij de Afdeling bestuursrechtspraak een eenduidige en gezaghebbende rechterlijke uitspraak te verkrijgen.

De CDA-fractieleden wijzen erop dat de CTIVD in verband tot voornoemd onderzoek van de Algemene Rekenkamer ook nadrukkelijk heeft gewezen op onderwerpen die buiten de reikwijdte van het voorstel vallen, zoals een verschuiving van statische naar dynamische regulering. Zij benadrukt in dit verband de noodzaak van de beoogde algehele herziening van de Wiv 2017. De leden vragen wat de observaties van de regering zijn als het gaat om de voortvarendheid daarmee. Ons antwoord op deze vragen luidt als volgt.

Wij onderschrijven de opmerkingen van de afdeling toezicht van de CTIVD inzake de noodzaak van een spoedige algehele herziening van de Wiv 2017. Ook deze omvangrijke herziening moet op een zorgvuldige wijze plaatsvinden. Op 1 september 2023 is de 'Hoofdlijnennotitie Wijziging Wiv 2017' naar de Tweede Kamer gestuurd.[10] In deze notitie worden de hoofdlijnen geschetst van een herziening van de Wiv 2017, mede aan de hand van de aanbevelingen van de ECW. Om de inhoudelijke richting voor de herziening van Wiv 2017 nader aan te scherpen, is de volgende stap het bespreken van de Hoofdlijnennotitie met de Tweede Kamer. Dit zal naar verwachting plaatsvinden in de loop van 2024. Gelet op het tijdelijke karakter (vier jaar) van de nu voorliggende Tijdelijke wet is steeds beoogd de herziening van de Wiv 2017 binnen vier jaar na inwerkingtreding van de Tijdelijke wet te realiseren.

De CDA-fractieleden hebben kennisgenomen van het tijdelijke karakter van het nu voorliggende wetsvoorstel. In het licht van de bedoeling om de Wiv 2017 meer omvattend te herzien, achten zij dat ook niet onlogisch. Toch lijkt de urgentie van de nu beoogde bepalingen aannemelijk te zijn en dient zich daarom toch de vraag aan waarom niet voor permanente voorzieningen is gekozen, vooruitlopend op de algehele herziening. Deze leden vragen de regering haar andersluidende keuze nader toe te lichten.

Van meet af aan is ingezet op een afzonderlijk en tijdelijk wetsvoorstel. Het gaat er immers om op relatief korte termijn te komen tot een op maat gesneden regeling om de door de diensten ondervonden urgente operationele problemen bij de toepassing van de Wiv 2017 in het cyberdomein te ondervangen. Een wijziging van de Wiv 2017 of een anderszins permanente voorziening zou onherroepelijk (bredere) discussies oproepen over de reikwijdte en werking van de regeling. Dat zijn legitieme vraagstukken, echter die moeten in het kader van de herziening van de Wiv 2017 aan de hand van onder andere de aanbevelingen van de ECW en na een fundamentele discussie met alle betrokkenen worden beantwoord. Van belang hierbij is dat de brede herziening een integrale herziening van de Wiv 2017 behelst en niet alleen ziet op het cyberdomein. Het is nadrukkelijk niet de bedoeling dat met de Tijdelijke wet inhoudelijk vooruitgelopen wordt op de herziening van de Wiv 2017, zij het dat niet is uitgesloten dat onderdelen daarvan wel een plek kunnen krijgen bij de herziening. Dat geldt onder meer voor de in de Tijdelijke wet geïntroduceerde beroepsmogelijkheid bij de Afdeling bestuursrechtspraak van de Raad van State. De ervaringen met de Tijdelijke wet zullen betrokken worden bij herziening van de Wiv 2017.

De fractieleden van D66 wijzen erop dat wat betreft de reikwijdte van de tijdelijke wet de wetstekst en de memorie van toelichting aangeven dat de reikwijdte is beperkt tot onderzoeken van de diensten naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen en dat het onderwerp van onderzoek bepaalt of de inzet van een bevoegdheid kan plaatsvinden

[10] *Kamerstukken II 2022/23, 34 588, nr. 92.*

onder deze wet. Het is volgens de memorie van toelichting aan de diensten om uit te zoeken of landen een dergelijk programma uitvoeren.[11] In het geval dat de aandacht naar bepaalde targets vanuit de diensten gebaseerd is op verschillende lopende onderzoeken, kan de tijdelijke wet alleen worden ingezet wanneer het zwaartepunt van het onderzoek onder deze wet valt. De TIB kan dit toetsen volgens het voorgestelde artikel 3, eerste lid. De TIB geeft zelf echter aan in haar brief van 7 december 2023 dat zij bang is dat er 'geshopt' zou kunnen worden naar de laagste vorm van toezicht.[12] Deze leden vragen of deze stelling van TIB, dat 'geshopt' kan worden, klopt. Wij antwoorden deze leden graag als volgt.

Wij delen de stelling van de TIB dat er 'geshopt' zou kunnen worden naar de laagste vorm van toezicht niet. Er is geen sprake van een laagste of een hoogste vorm van toezicht. Wel is er sprake van een (deels) andere vorm van toezicht, te weten een aanpassing van de vorm van toezicht toegesneden op de aard van de bevoegdheid (van statisch naar dynamisch) en in een aantal gevallen een toezicht bestaande uit extra waarborgen (bindend toezicht door de afdeling toezicht van de CTIVD) waar dat gelet op de voorgestelde aanpassingen vanuit oogpunt van de daarmee gepaard gaande beperking op het recht van bescherming van de persoonlijke levenssfeer aangewezen wordt geacht. De gevolgen van het toezicht vloeien van rechtswege voort uit de wel of niet toepasselijkheid van de Tijdelijke wet. Er kan dus niet daarin 'geshopt' worden. Artikel 2 bepaalt wanneer de Tijdelijke wet van toepassing is. De TIB kan dit aspect betrekken in haar rechtmatigheidsoordeel op een aan haar voorgelegde door de minister verleende toestemming tot inzet van een bijzondere bevoegdheid. De Tijdelijke wet is van toepassing op onderzoeken van de AIVD en MIVD naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen en dus niet enkel naar de offensieve cyberprogramma's *van landen* (artikel 2, eerste lid). Ingevolge artikel 2, tweede lid, is op de uitvoering van die taak de Wiv 2017 van toepassing *met inachtneming van het bepaalde in hoofdstuk 2*. Artikel 2, derde lid, bepaalt vervolgens dat bij een verzoek om toestemming als bedoeld in dit artikellid aangegeven dient te worden of uitvoering wordt gegeven aan het bepaalde in hoofdstuk 2. Dat is dus een constitutief vereiste. Indien daarvan wordt afgezien is de Tijdelijke wet niet van toepassing. Dat kan dus betekenen dat er wel sprake is van een onderzoek naar een land met een offensief cyberprogramma, maar dat afgezien wordt van toepassing verklaring van de Tijdelijke wet omdat de Tijdelijke wet ter zake van de desbetreffende bijzondere bevoegdheid geen aanvulling geeft ten opzichte van hetgeen in de Wiv 2017 wordt bepaald. Al eerder is in antwoord op vragen van de leden van de GroenLinks-PvdA-fractie over de door de TIB voorziene onduidelijkheden uiteengezet hoe bepaald wordt of er sprake is van een onderzoek naar een land met een offensief cyberprogramma.

De hiervoor gegeven uitleg is onderdeel van de parlementaire geschiedenis en beoogt duidelijkheid te verschaffen over de uitleg van de Tijdelijke wet zodat een beroepsprocedure bij de Afdeling bestuursrechtspraak op dit punt voorkomen kan worden.

De leden van de PVV-fractie constateren dat in de memorie van toelichting in het kader van landen met een offensief cyberprogramma wordt gesproken over 'beïnvloeden van beeldvorming' en 'digitale beïnvloedingscampagnes'.[13] Deze leden vragen of de regering kan aangeven in hoeverre deze vormen van beeldvorming en beïnvloeding in het kader van dit wetsvoorstel betrekking hebben op cyberprogramma's of cyberaanvallen, aangezien dergelijke campagnes evengoed via reguliere communicatie/mediakanalen kunnen verlopen. Wij beantwoorden deze vraag graag als volgt.

Dit wetsvoorstel ziet op landen met een offensief cyberprogramma. Een land met een dergelijk cyberprogramma kan zijn doelen en intenties daarmee op verschillende manier bereiken. Het verspreiden van bepaald soort nieuws ter beïnvloeding kan via verschillende manieren lopen. Zo kan een heel onlinenetwerk opgezet worden om bepaalde berichten de digitale (cyber)wereld in te brengen, die vervolgens overgenomen worden in reguliere communicatie- en mediakanalen. De AIVD en MIVD proberen door middel van inlichtingenonderzoeken te achterhalen welke heimelijke doelen en intenties een land met een offensief cyberprogramma heeft en kijken niet enkel naar een bepaalde aanval die reeds heeft plaatsgevonden. De taak van de AIVD en MIVD is juist het

[11] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 6.*
[12] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 9.
[13] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 3.*

voorkomen of direct duiden van dergelijke aanvallen zodat betrokken personen of instanties tijdig geïnformeerd kunnen worden.

De leden van de PVV-fractie vragen vervolgens of de regering daarbij tevens een afbakening kan geven van zulke campagnes: hoe en door wie wordt bepaald of een bepaalde boodschap als desinformatie wordt gezien, hoe dit zich verhoudt tot de vrijheid van meningsuiting en in hoeverre daarmee voldoende grond bestaat om bevoegdheden uit het wetsvoorstel hiervoor in te zetten.

De inlichtingen- en veiligheidsdiensten verrichten onderzoek naar personen, organisaties en landen waarvan een (mogelijke) dreiging uitgaat richting de nationale veiligheid. In een onderzoek van de diensten kan blijken dat bepaalde personen, organisaties of landen desinformatie verspreiden, eventueel in de vorm van complottheorieën. Deze onderzoeken vinden plaats binnen de kaders van Wiv 2017 en op basis van de GA. Vanuit die kaders hebben de diensten aandacht voor desinformatie.

De leden van de PVV-fractie wijzen erop dat het uitgangspunt van dit wetsvoorstel 'onderzoek naar landen met een offensief programma tegen Nederland of Nederlandse belangen' is. Deze leden vragen of de regering nader kan duiden hoe en door wie bepaald wordt welke landen dit zijn en onder welke voorwaarden, en welke criteria worden toegepast om vast te stellen dat sprake is van een offensief programma en wat de afbakening is van Nederlandse belangen. Zij vragen in het bijzonder of tot Nederlandse belangen bijvoorbeeld ook de belangen van NAVO-partners of de Europese Unie in bredere zin gerekend worden. Zij vragen of de regering tevens nader kan duiden wanneer dit criterium wel of niet een grondslag zal zijn voor inzet van bevoegdheden. Wij beantwoorden deze vragen graag als volgt.

De wettelijke taken van de diensten worden aan de hand van de inventarisatie van de behoeften bij belanghebbende ministeries uitgewerkt in onderzoeksthema's in de Geïntegreerde Aanwijzing (GA). De onderzoeken die de diensten dienen te verrichten, worden op grond van artikel 6 Wiv 2017 in de GA geformuleerd en dat geldt niet anders voor onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. In de memorie van toelichting bij het voorstel van de Tijdelijke wet worden twee voorbeelden genoemd: China en Rusland. In het jaarverslag 2022 van de AIVD worden ook Iran en Noord-Korea genoemd. Landen vallen onder deze kwalificatie als zij genoemd zijn in de GA als landen met een offensief cyberprogramma waarmee zij een risico vormen voor Nederland en/of Nederlandse belangen. De Nederlandse belangen waarnaar het wetsvoorstel verwijst, zijn de belangen zoals beschreven in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden.[14] Deze nationale veiligheidsbelangen vormen de kern van wat Nederlandse inlichtingen- en veiligheidsdiensten moeten beschermen. Er zijn verschillende dreigingen voor de nationale veiligheid. Als een dreiging één of meer veiligheidsbelangen ernstig aantast, kan dat maatschappelijke ontwrichting veroorzaken en daarmee de nationale veiligheid schaden. Tegelijkertijd zijn deze dreigingen met elkaar verweven. De ene dreiging heeft invloed op de andere dreiging, waardoor ze elkaar kunnen versterken. De Veiligheidsstrategie legt de nadruk op deze verwevenheid en beschrijft de veiligheidsbelangen als volgt:

- Territoriale veiligheid: het ongestoord functioneren van het Koninkrijk der Nederlanden en haar EU en NAVO bondgenoten als onafhankelijke staten in brede zin, – dan wel de territoriale veiligheid in enge zin.
- Fysieke veiligheid: het ongestoord functioneren van de mens in het Koninkrijk der Nederlanden en zijn omgeving.
- Economische veiligheid: het ongestoord functioneren van het Koninkrijk der Nederlanden als een effectieve en efficiënte economie.
- Ecologische veiligheid: het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij het Koninkrijk der Nederlanden.
- Sociale en politieke stabiliteit: het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen ongestoord kunnen functioneren en groepen mensen – goed met elkaar kunnen samenleven binnen de verworvenheden van de democratische rechtstaat van het Koninkrijk der Nederlanden en de daarin gedeelde waarden.

[14] https://www.rijksoverheid.nl/onderwerpen/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden

- Internationale rechtsorde en stabiliteit: het goed functioneren van het internationale stelsel van normen en afspraken, gericht op het bevorderen van de internationale vrede en veiligheid, inclusief mensenrechten, en effectieve multilaterale instituties en regimes, alsmede het goed functioneren van staten grenzend aan het Koninkrijk der Nederlanden en in de directe omgeving van de Europese Unie.

Voorts vragen leden van de PVV-fractie de regering aan te geven in hoeverre in het kader van dit wetsvoorstel ook onderzoek naar jihadisme onderdeel kan zijn van de inzet van bevoegdheden, en specifiek vragen zij de regering daarbij ook nader te duiden hoe daarbij wordt omgegaan met niet-statelijke actoren. Onze reactie hierop luidt als volgt.

De reikwijdte van de Tijdelijke wet is gericht op landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Wanneer deze landen gebruik maken van bedrijven of groeperingen, vormen deze bedrijven en groeperingen daarmee een dreiging voor de nationale veiligheid en kan onderzoek daarnaar ook plaatsvinden binnen de reikwijdte van deze wet. Ze worden namelijk ingezet door de desbetreffende statelijke actor en hun activiteiten zijn aan die statelijke actor toe te rekenen. Het maakt daarbij geen verschil of het gaat om (bijvoorbeeld) criminelen of andersoortige groeperingen (zoals jihadistische groeperingen). Doorslaggevend is dat het land is genoemd in de GA als land met een offensief cyberprogramma gericht op Nederland of Nederlandse belangen en er sprake is van handelen door de betreffende statelijke actor. Indien dat niet zo is, of indien dit vermoeden tijdens het onderzoek wordt ontkracht, valt het onderzoek niet meer onder de reikwijdte van de Tijdelijke wet. In dat geval kunnen de diensten het onderzoek eventueel vervolgen onder het regime van de Wiv 2017. Daarnaast kan het voorkomen dat een target van de dienst, bijvoorbeeld een (vermeend) jihadist, in verschillende onderzoeken van de dienst is betrokken, waaronder een onderzoek naar landen met een offensief cyberprogramma. Indien vanuit die verschillende onderzoeken de inzet van een bijzondere bevoegdheid jegens dat target wordt overwogen, zal een ad hoc afweging dienen plaats te vinden voor welk onderzoek de inzet van die bijzondere bevoegdheid en de daarmee te verkrijgen gegevens het grootste belang heeft oftewel waar het zwaartepunt van het onderzoek naar het target ligt. Als dat zwaartepunt bij het onderzoek naar landen met een offensief cyberprogramma ligt, dan kan de toepasselijkheid van de Tijdelijke wet worden ingeroepen. In algemene zin kan echter worden gesteld dat onderzoek naar jihadisme (contra-terrorisme) niet onder de reikwijdte dit wetsvoorstel valt, maar onder de Wiv 2017 zal blijven plaatsvinden.

De fractieleden van de PVV vragen of de regering kan aangeven hoe bij de toepassing van dit wetsvoorstel zal worden omgegaan met metadata en wat daarbij de uitgangspunten en beperkingen zijn.

Dit wetsvoorstel regelt twee aspecten voor wat betreft de omgang met metadata. Het gaat hier om het toepassen van geautomatiseerde data-analyse (GDA, artikel 60 Wiv 2017) op metadata verkregen uit OOG interceptie met als doel het identificeren van personen en organisaties. Het wetsvoorstel verschuift de thans in de Wiv 2017 voorziene statische toets vooraf door de TIB naar bindend toezicht door de afdeling toezicht van de CTIVD tijdens de uitvoering van deze bevoegdheid. Op deze manier kan beter aangesloten worden bij het iteratieve en dynamische karakter van geautomatiseerde data-analyse waarbij resultaten van analyses eventuele vervolgstappen beïnvloeden. Het is op voorhand immers niet te voorspellen welke vorm van GDA op welk moment met welke gegevens gebruikt gaan worden bij de onderzoeken van de diensten. Bij het verrichten van data-analyses kunnen bij elke handeling nieuwe inzichten worden verkregen en moeten nieuwe hypotheses worden getoetst. Dit alles gebeurt in een omgeving waarbij de beschikbare en bruikbare gegevens zeer veranderlijk zijn. De afdeling toezicht heeft inzicht in de systemen van de diensten en kan meekijken met de wijze waarop GDA op OOG-metadata tijdens onderzoeken wordt toegepast en is daarom de aangewezen instantie om effectief toezicht te houden. In de Tijdelijke wet krijgt de afdeling toezicht de bevoegdheid om bindend te oordelen over de wijze waarop de diensten GDA op metadata uit kabel- of etherinterceptie toepassen (artikel 12, eerste lid, onder d).

De gegevens die bij GDA op OOG-metadata worden betrokken, zijn allereerst de metadata verkregen via een rechtmatig bevonden OOG-interceptie ex artikel 48 Wiv 2017 en voorts de gegevens die door toepassing van andere aan de dienst toekomende bevoegdheden (algemeen en

bijzonder, dan wel via verkrijging van een buitenlandse dienst) zijn verworven. Het bindend toezicht heeft geen betrekking op de verwerving van die gegevens. Het bindend toezicht heeft uitsluitend betrekking op de toegepaste methodiek van GDA. Is die methodiek (bevoegdheid) onrechtmatig bevonden en heeft de afdeling toezicht daaraan het gevolg verbonden dat die bevoegdheid dient te worden beëindigd, dan kan het daaraan te koppelen gevolg – namelijk de verwijdering en vernietiging van bij de uitvoering verwerkte gegevens – alleen betrekking hebben op de gegevens die door toepassing van de betreffende GDA zijn gegenereerd; dus niet op de daarbij gebruikte gegevens. Artikel 50, vierde lid, Wiv 2017 waarop het bindend toezicht binnen de reikwijdte van het wetsvoorstel betrekking heeft ziet immers uitsluitend op het verkrijgen van toestemming van de minister voor de toepassing van een nader aan te duiden vorm van GDA met een aanduiding van de daarbij te betrekken gegevensbestanden. Het bindend toezicht komt hier in de plaats van de ex ante bindende toets door de TIB, welke zich bij haar toetsing ook tot het object van toestemming – namelijk het mogen toepassen van GDA – dient te beperken. Daarnaast gelden in algemene zin de algemene bepalingen van gegevensverwerking uit de Wiv 2017 (artikelen 17 tot en met 24). Ook wordt in artikel 14e voorzien in een TIB-toets op verleende toestemmingen voor de real time verzameling van verkeers- en locatiegegevens (stomme tap). Dit is een procedurele wijziging; de uitoefening van de bevoegdheid wijzigt niet.

De leden van de ChristenUnie-fractie observeren dat het voorliggend wetsvoorstel uitdrukkelijk een tijdelijk karakter heeft. Het vervalt op grond van artikel 17 vier jaar na het moment van inwerkingtreding. Het wetsvoorstel geeft geen ruimte voor verlenging van deze termijn. Deze tijdelijkheid hangt samen met de integrale herijking van de huidige Wiv 2017. Deze leden vragen de regering inzichtelijk te maken wat de stand van zaken met betrekking tot die herijking op dit moment is en wat het huidige tijdpad is.

Zoals hiervoor op een vraag van de leden van de CDA-fractie is geantwoord, is op 1 september 2023 de 'Hoofdlijnennotitie Wijziging Wiv 2017' naar de Tweede Kamer gestuurd die naar verwachting in de loop van 2024 zal worden besproken met de Tweede Kamer. Gelet op het tijdelijke karakter (vier jaar) van het nu voorliggende wetsvoorstel is steeds beoogd de herziening van de Wiv 2017 binnen vier jaar na inwerkingtreding van de Tijdelijke wet te realiseren.

Het wetsvoorstel is bedoeld om de inlichtingen- en veiligheidsdiensten beter in staat te stellen onderzoek te doen naar landen met een offensief cyberprogramma. Het voorgestelde artikel 2, eerste lid benoemt dit met zoveel woorden als een taak van de diensten. Het valt de leden van de ChristenUnie-fractie echter op dat het wetsvoorstel niet afbakent of zelfs maar indiceert wanneer sprake is van een land met een offensief cyberprogramma. Op welke wijze en door wie wordt dit bepaald, zo vragen zij de regering.

Zoals hiervoor is aangegeven in antwoord op vragen van de leden van de PVV-fractie over de voorwaarden en criteria om vast te stellen wanneer sprake is van een land met een offensief cyberprogramma, worden de wettelijke onderzoekstaken van de diensten aan de hand van de inventarisatie van de behoeften bij belanghebbende ministeries uitgewerkt in de GA (op grond van artikel 6 Wiv 2017). Voor de aanwijzing van landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen in de GA geldt het volgende. Landen komen in aanmerking voor deze kwalificatie als de diensten en de belanghebbende ministeries aanwijzingen hebben dat deze landen actief een offensief cyberprogramma ontplooien waarmee zij een risico vormen voor Nederland of Nederlandse belangen. Deze onderbouwing is gebaseerd op de onderzoeken die de diensten doen en het dreigingsbeeld dat daaruit voortkomt alsmede andere overwegingen bij de betrokken departementen bij het voorbereiden van de GA. Eind 2022 is de GA voor de periode 2023-2026 door het kabinet vastgesteld[15] en wordt waar nodig gedurende deze periode jaarlijks geüpdatet. Deze GA beschrijft de meerjarige inlichtingenbehoefte vanuit verschillende behoeftestellers en vormt daarmee de inhoudelijke basis voor het geheime jaarplan van de AIVD en de MIVD. De GA wordt gezamenlijk vastgesteld door de minister-president en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie, na overleg met de minister van Justitie en Veiligheid en Buitenlandse Zaken. De GA wordt op hoofdlijnen gepubliceerd in de Staatscourant. In de GA is ook het onderzoek naar cyberaanvallen van statelijke actoren opgenomen; de gerichte taakopdracht van de AIVD en MIVD is staatsgeheim gerubriceerd. Deze

[15] Stcrt. 2022, 33 858.

wordt met de Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer gedeeld. De Tijdelijke wet is dus van toepassing op elk onderzoek van de diensten naar landen met een offensief cyberprogramma die worden genoemd in de GA met een dergelijke doelstelling, gericht op Nederland of Nederlandse belangen.

In het verlengde daarvan vragen de ChristenUnie-fractieleden naar de beoogde toepassing van het voorgestelde artikel 2, derde lid. Daarin wordt – beknopt weergegeven – bepaald dat in een verzoek om toestemming of verlenging van toestemming voor de uitoefening van een bijzondere bevoegdheid vermeld wordt of daarbij toepassing wordt gegeven aan het bepaalde in dit wetsvoorstel. Deze leden vragen of zij het goed begrijpen dat de keuze voor ofwel het stelsel van de tijdelijke wet ofwel voor het stelsel van de huidige Wiv 2017 hiermee geheel aan de diensten wordt gelaten en zo ja, of de regering dit nader kan toelichten en aangeven of de diensten hierin bepaalde kaders meekrijgen.

Zoals hiervoor al is aangegeven, zijn alle onderzoeken die de diensten verrichten op grond van artikel 6 Wiv 2017 in de GA opgenomen, ook onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Daarmee is nog niet gezegd dat de Tijdelijke wet altijd van toepassing is op dergelijke onderzoeken. De Tijdelijke wet is van toepassing indien dit in het verzoek om toestemming voor de inzet van een bijzondere bevoegdheid wordt aangegeven. De keuze om de Tijdelijke wet wel of niet van toepassing te verklaren is primair aan de diensten. Zij kunnen immers het best beoordelen of sprake is van een situatie waarvoor de Tijdelijke wet van toepassing dient te zijn. De keuze om de Tijdelijke wet van toepassing te verklaren wordt gemotiveerd in het toestemmingsverzoek voor de inzet van een bijzondere bevoegdheid dat aan de minister wordt voorgelegd. Als de minister dit verzoek goedkeurt wordt dit, voor zover het een TIB-plichtige bijzondere bevoegdheid betreft, getoetst door de TIB op rechtmatigheid. Indien de TIB van oordeel is dat met betrekking tot de aan haar voorgelegde toestemming ten onrechte is bepaald dat daarmee tevens toepassing wordt gegeven aan de Tijdelijke wet, deelt zij dit terstond mede aan de minister. De TIB toetst vervolgens de toestemming zonder toepassing van het bepaalde in de Tijdelijke wet uitsluitend op grond van de Wiv 2017. Tegen het oordeel van de TIB dat in casu de Tijdelijke wet niet van toepassing is staat voor de minister beroep open bij de Afdeling bestuursrechtspraak. Ingeval de TIB een onder toepassing van de Tijdelijke wet verleende toestemming goedkeurt, deelt zij dit terstond mede aan de afdeling toezicht van de CTIVD. Indien de TIB onder toepassing van de Tijdelijke wet de goedkeuring weigert, vervalt de toestemming van rechtswege. Ook tegen dit oordeel van de TIB staat voor de minister beroep open bij de Afdeling bestuursrechtspraak.

De fractieleden van de PvdD constateren dat blijkens het tweede lid van artikel 2 van het wetsvoorstel, de Wiv 2017 "[o]p de uitvoering van de in het eerste lid bedoelde taak" van toepassing is "met inachtneming van het bepaalde in dit hoofdstuk". Deze leden vragen of zij het goed zien dat ingevolge het tweede lid van artikel 2 hoofdstuk 2 van het ontwerp van rechtswege van toepassing is op "het verrichten van onderzoek naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen". Wij beantwoorden de leden graag als volgt.

Bepalend voor de vraag of hoofdstuk 2 van de Tijdelijke wet van toepassing is op de inzet van een bijzondere bevoegdheid is of de Tijdelijke wet in de toestemmingsaanvraag van toepassing is verklaard. Dit volgt uit artikel 2, derde lid, van het wetsvoorstel. Zoals hiervoor gesteld in reactie op vragen van de D66-fractie kan het voor komen dat sprake is van een onderzoek naar een land met een offensief cyberprogramma, maar dat afgezien wordt van toepassing verklaring van de Tijdelijke wet omdat de Tijdelijke wet ter zake van de desbetreffende bijzondere bevoegdheid geen aanvulling geeft ten opzichte van hetgeen in de Wiv 2017 wordt bepaald. Hoofdstuk 2 is dus niet van rechtswege van toepassing op grond van artikel 2, tweede lid, van het wetsvoorstel.

De leden van de PvdD-fractie vragen vervolgens wie vaststelt en bij welk besluit dat een land "een offensief cyberprogramma tegen Nederland of Nederlandse belangen" uitvoert, en waar dat wettelijk geregeld is.

Voor de beantwoording van deze vragen kan verwezen worden naar het antwoord op soortgelijke vragen van de leden van de fractie van de ChristenUnie over de afbakening of indicatie wanneer

sprake is van een land met een offensief cyberprogramma en de PVV-fractie over de voorwaarden en criteria om vast te stellen wanneer sprake is van een land met een offensief cyberprogramma.

De fractieleden van de PvdD vragen ook of de diensten bevoegd zijn om het voorgestelde artikel 6 toe te passen zonder dat is vastgesteld dat de verkenning betrekking heeft op een land met een offensief cyberprogramma tegen Nederland of Nederlandse belangen.

Dat is niet het geval. Hoofdstuk 2 van het wetsvoorstel is uitsluitend van toepassing op onderzoek naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Alleen in het kader van een dergelijk onderzoek kan artikel 6 van het wetsvoorstel worden toegepast met dien verstande dat ook indien een digitale aanval nog niet (direct) te attribueren is aan een land, maar er wel een vermoeden is dat deze te attribueren is aan een statelijke actor, de Tijdelijke wet, en dus ook artikel 6, ook kan worden toegepast.

De leden van de PvdD-fractie vragen vervolgens waarop een vermoeden kan worden gebaseerd dat een land een offensief cyberprogramma hanteert in een bepaald digitaal verkeer of bij bepaalde telecommunicatie alsnog geen verkenning als bedoeld in artikel 6 heeft plaatsgevonden.

Aanwijzingen van de diensten over offensieve cyberprogramma's van landen zijn op het moment van inwerkingtreding van het wetsvoorstel niet gebaseerd op de toepassing van de verkennende bevoegdheid ex artikel 6. De diensten verzamelen nu al met andere bevoegdheden dan de verkennende bevoegdheid voor OOG-interceptie, gegevens die inzicht geven in de activiteiten van andere landen en al dan niet aanwijzingen geven of deze landen een offensief cyberprogramma hanteren.

De leden van de Volt-fractie merken op dat dit wetsvoorstel de Wiv 2017 gedeeltelijk lijkt te herzien zonder dat het daadwerkelijk een herziening is. Zij wijzen erop dat de regering heeft aangegeven dat een herziening bij een volgend kabinet ligt en vragen tot op welke hoogte deze tijdelijke wet voorziet in de lacunes die momenteel door de Militaire Inlichtingen- en Veiligheidsdienst en de Algemene Inlichtingen- en Veiligheidsdienst in hun werk ervaren worden. Ook vragen zij of de Kamer op korte termijn nogmaals een voorstel voor een tijdelijke wet kan verwachten of dat zij eerder een herziening van de Wiv 2017 kan behandelen. Wij beantwoorden de vragen van deze leden graag als volgt.

Het onderhavige wetsvoorstel is geen wijziging of herziening van de Wiv 2017. De Wiv 2017 blijft van toepassing, ook in gevallen waarop de Tijdelijke wet van toepassing is, met dien verstande dat de Tijdelijke wet op enkele onderdelen een aanvulling of afwijking bevat op hetgeen in de Wiv 2017 is geregeld.

De Tijdelijke wet is tot stand gekomen omdat de huidige wet en de uitleg daarvan in de toepassingspraktijk onvoldoende aansluit op de huidige dreiging en de operationele werkelijkheid in het cyberdomein. Daar is snelheid en wendbaarheid vereist en de Wiv 2017 geeft die onvoldoende. Dit leidt tot urgente operationele knelpunten. Bestaande bevoegdheden kunnen niet of niet voldoende effectief worden ingezet en hierdoor is het zicht op de dreiging van landen met een offensief cyberprogramma de afgelopen jaren afgenomen. Met de Tijdelijke wet moeten de AIVD en MIVD beter in staat worden gesteld hun bevoegdheden in te zetten en snel en effectief te acteren. Dit alles laat onverlet dat de brede herziening van de Wiv 2017 onverminderd urgent is. Zoals hiervoor aangegeven in reactie op een vraag van de leden van de CDA-fractie, is op 1 september 2023 de 'Hoofdlijnennotitie Wijziging Wiv 2017' naar de Tweede Kamer gestuurd die naar verwachting in de loop van 2024 met de Tweede Kamer zal worden besproken. Gelet op het tijdelijke karakter (vier jaar) van het nu voorliggende wetsvoorstel is steeds beoogd de herziening van de Wiv 2017 binnen vier jaar na inwerkingtreding van de Tijdelijke wet te realiseren.

3. De maatregelen nader beschouwd

In de wetsteksten, wetsbehandeling en memorie van toelichting worden verschillende begrippen gebruikt. Daarom hebben de fractieleden van GroenLinks-PvdA enkele verduidelijkende vragen.
In het inlichtingenproces met betrekking tot ongerichte kabelinterceptie zijn er naar het begrip van voornoemde fractieleden drie stappen:
1. Het opslaan van internetverkeer van veel nietsvermoedende en grotendeels onschuldige mensen.

2. Het door middel van *artificial intelligence* (hierna: AI) hierin speuren naar zaken die 'mogelijk interessant' zijn.
3. Het door analisten van inlichtingendiensten nader bekijken van de informatie.

De fractieleden van GroenLinks-PvdA vragen of het klopt dat wat de regering 'verkennen' noemt, bovenstaande stappen 1 en 2 behelst, en of de regering kan betogen waarom het *chilling effect* van aftappen niet zou plaatsvinden bij dergelijk 'verkennen'. Zij vragen daarbij of de regering het standpunt deelt dat stap 2 in feite het beoordelen van mensen op basis van hun gedrag en uitingen behelst dan wel impliceert. Maakt het voor een mens effectief uit of de beoordeling die aan hem of haar wordt toegeschreven door AI of door een mens komt, als hier gevolgen aan verbonden kunnen zijn? Ook stellen deze fractieleden dat meer fundamenteel gesteld kan worden dat AI inmiddels in staat is om binnen datasets verbanden te leggen die zonder de toepassing daarvan niet zichtbaar zouden worden en dat dit op gespannen voet staat met de uiteindelijke, hiervoor genoemde stap 3. Deze leden vragen de regering op deze stelling te reflecteren. Deze leden vragen vervolgens wat het materiële verschil tussen stap 2 en 3 is voor de betrokkenen.

Op de door de leden van de fractie van GroenLinks-PvdA gestelde vragen willen wij graag als volgt reageren, waarbij we allereerst willen opmerken dat de door deze leden geschetste drie stappen voor ongerichte kabelinterceptie afwijken van de wijze waarop de keten van OOG-interceptie bij de diensten is ingericht. Alvorens in te gaan op de gestelde vragen, zal die keten – en de onderlinge samenhang tussen de onderscheiden ketens – hieronder kort worden toegelicht.

OOG-interceptie is een complexe en strategische bevoegdheid die, anders dan gerichte interceptie, een ketenbevoegdheid is die bestaat uit meerdere fases. Bij het uitvoeren van OOG-interceptie is er sprake van meerdere handelingen per fase, ieder met bijbehorende waarborgen, waaronder een TIB-toets, ook in de fase van verkennen ten behoeve van OOG-interceptie. Dit zorgt voor een gebalanceerd stelsel waarbinnen de diensten op een proportionele wijze onderzoek kunnen verrichten naar de hedendaagse dreiging om met name ongekende dreigingen te kunnen identificeren en onderzoeken.

OOG-interceptie vindt plaats door interceptie van communicatie (inhoud en metadata) van kabelverkeer of door interceptie van satellietverkeer. OOG-interceptie (ongeacht of het voor verkenning is of ten behoeve van het uiteindelijke inlichtingenonderzoek) begint bij de keuze van de locatie waarop de gegevensstromen geïntercepteerd moeten worden. De diensten mogen namelijk niet zomaar elke kabel of satelliet verkennen of intercepteren. De diensten richten zich op gegevensstromen die hoofdzakelijk internationaal verkeer bevatten en mogelijk van waarde kunnen zijn voor de inlichtingenonderzoeken van de diensten.[16] Op deze locatie vindt, na een TIB-toets op de daartoe verleende toestemming van de minister, het verwerven van deze gegevensstromen ten behoeve van de vastgestelde onderzoeksopdrachten plaats. Daarbij is het goed om te vermelden dat een kabel bestaat uit glasvezels of fibers. Binnen de fibers kunnen weer 'tientallen' kanalen te onderscheiden zijn. De diensten kunnen door middel van vooronderzoek op een hoog abstractieniveau fibers en kanalen duiden waarvan een verwachting bestaat dat er sprake is van hoofdzakelijk internationaal verkeer dat mogelijk relevant kan zijn voor de inlichtingenonderzoeken van de diensten. In het kader van het vooronderzoek kunnen de diensten informatie opvragen bij een aanbieder, zoals een (markt)partij waar de accesslocatie gerealiseerd zou kunnen worden. Ook kunnen de diensten de bevoegdheid tot verkennen ten behoeve van OOG-interceptie toepassen om vast te stellen welke fibers en kanalen relevant zijn. Dit moet eraan bijdragen dat de diensten alleen die gegevensstromen intercepteren en verder verwerken die van belang zijn voor hun onderzoeken.

De verschillende fasen die de diensten bij OOG-interceptie op de kabel hanteren zijn de volgende:

<u>1. Verkennen (artikel 6 Tijdelijke wet)</u>
In deze fase wordt inzichtelijk gemaakt welke kabels een bijdrage kunnen leveren aan inlichtingenonderzoeken van de diensten. De diensten richten zich hierbij op hoofdzakelijk internationaal verkeer. De voor de dienst verantwoordelijke minister geeft toestemming voor de verkenning en deze toestemming wordt getoetst door de TIB. De eis van gerichtheid geldt hierbij

[16] Vgl. ECHR Big Brother Watch v. United Kingdom § 375-376.

niet, maar de uitoefening is wel strikt doelgebonden. Alleen daartoe aangewezen medewerkers van de diensten mogen kennisnemen van de met de verkenning verworven gegevens en de bewaartermijn voor deze gegevens is maximaal zes maanden. Ook mogen deze gegevens uitsluitend gebruikt worden om de aanvraag voor de verwerving ten behoeve van het inlichtingenproces (fase 2) beter te onderbouwen. De afdeling toezicht van de CTIVD houdt regulier toezicht op de uitvoering.

De fasen die hierop volgen betreffen de uitvoering van OOG-interceptie ten behoeve van de teams in het inlichtingenproces. Binnen de keten van OOG-interceptie speelt het gerichtheidscriterium een grote rol. De wijze waarop dit criterium wordt ingevuld, is afhankelijk van de fase waarin het onderzoek zich bevindt en de technische en operationele omstandigheden van de casus.

2. Verwerving voor het inlichtingenproces (artikel 48 en 49, eerste lid, Wiv 2017 en artikel 7 Tijdelijke wet)
Indien uit de verkenning blijkt dat de onderzochte kabels relevante gegevens bevatten die uiteindelijk door de teams in het inlichtingenproces gebruikt mogen worden voor het beantwoorden van hun onderzoeksvragen (fase 4), kan overgegaan worden tot de bevoegdheid tot kabelinterceptie ter verwerving van gegevens die gebruikt mogen worden in het inlichtingenproces. Ook hierbij richten de diensten zich op hoofdzakelijk internationaal verkeer. De minister verleent hiervoor toestemming en ook deze toestemming wordt getoetst door de TIB. In deze fase vindt ook (de eerste) filtering plaats waarbij een groot deel van de gegevens vernietigd wordt omdat deze niet relevant zijn gebleken voor de onderzoeken van de diensten. De gegevens die wel relevant zijn, worden opgeslagen zodat deze gegevens op een later moment bevraagd kunnen worden. De afdeling toezicht van de CTIVD houdt regulier toezicht op de uitvoering.

3. Identificatie (artikel 49, tweede lid, Wiv 2017)
In het identificatieonderzoek worden de verworven gegevens door daartoe aangewezen medewerkers van de diensten doorzoekbaar gemaakt en doorzocht op kenmerken die horen bij gekende en ongekende dreigingen ten behoeve van de teams in het inlichtingenproces. Deze medewerkers doen dit op basis van selectoren en complexe zoekvragen. Als uitkomst hiervan kunnen nieuwe dreigingen worden geïdentificeerd en bestaande dreigingen worden bevestigd. De aangewezen medewerkers bepalen of gegevens toebehoren aan een gekend target of dat er sprake is van een ongekende dreiging. De selectoren en complexe zoekvragen worden uitsluitend gebruikt voor onderzoeksgebieden uit de GA en waarvoor toestemming is verleend door de minister en deze toestemming wordt getoetst door de TIB. De afdeling toezicht van de CTIVD houdt regulier toezicht op de uitvoering.

4. Selectie (artikel 50 Wiv 2017)
Uiteindelijk worden de gegevens geselecteerd die de teams in het inlichtingenproces kunnen gebruiken voor hun inlichtingenonderzoek. De teams in het inlichtingenproces krijgen uitsluitend toegang tot de geselecteerde gegevens die op basis van een selectiekenmerk (gericht op een onderwerp, persoon of organisatie) zijn gekoppeld aan een target of onderzoeksopdracht en waarvoor de minister toestemming heeft verleend die door de TIB rechtmatig is geoordeeld. De geselecteerde gegevens kunnen vervolgens in combinatie met andere gegevens gebruikt worden door de teams in het inlichtingenproces wat kan leiden tot het uitbrengen van mededelingen aan belangendragers. De overige gegevens worden niet ter beschikking gesteld aan de teams in het inlichtingenproces. Ook GDA op metadata valt onder deze bevoegdheid. Op grond van de Tijdelijke wet geldt hiervoor in afwijking van de Wiv 2017 geen TIB-toets, maar houdt de afdeling toezicht van de CTIVD bindend toezicht op de uitvoering. Voor het overige houdt de afdeling toezicht regulier toezicht op de uitvoering.

Naast de bindende TIB toetsen per fase op de benodigde ministeriële toestemmingen voor de daarbij uit te oefenen bijzondere bevoegdheden, kennen de diensten toenemende waarborgen per fase (waaronder de beschikbaarheid van gegevens die door filtering en reductie van gegevens kan afnemen). De eerste drie fases kunnen uitsluitend worden uitgevoerd door medewerkers die specifiek zijn aangewezen (functiescheiding). Dit betekent dat alleen deze medewerkers, bij uitsluiting van anderen, de mogelijkheid hebben om kennis te nemen van deze gegevens.

Het wettelijk kader en de hiervoor geschetste fases die daaruit volgen voldoen naar ons oordeel aan de eisen en voorwaarden die voortvloeien uit het EVRM (artikel 8) en de jurisprudentie van het EHRM ter zake. Daarbij is uitwerking gegeven aan de door het EHRM in onder meer de zaak Big Brother Watch e.a. tegen het Verenigd Koninkrijk neergelegde lijn waarbij het EHRM bulkinterceptie ziet als een gradueel proces waarbij de mate van inmenging met de in artikel 8 EVRM vastgelegde rechten van een persoon toeneemt naargelang het proces zich verder ontwikkelt. Daar dienen dan ook steeds verdergaande waarborgen tegenover te staan. De inbreuk die door de handeling op het door artikel 8 EVRM beschermde recht wordt gemaakt, bepaalt de stringentheid van de toe te passen waarborg. In het wettelijk stelsel voor de Nederlandse inlichtingen- en veiligheidsdiensten is dat met name vertaald in een bindende rechtmatigheidstoets door de TIB en een systeem van functiescheiding. De diensten motiveren in de toestemmingsaanvragen de proportionaliteit ook nadrukkelijk aan de hand van de door het EHRM geschetste graduele proces.

We zullen thans ingaan op de door de leden van de GroenLinks-PvdA-fractie gestelde vragen.

Ten aanzien van de vraag of de bevoegdheid tot verkennen overeenkomt met de door deze leden geschetste stappen 1 en 2, wordt opgemerkt dat dit niet het geval is. Zoals in de inleidende opmerkingen reeds is gesteld, wijken de door deze leden geschetste drie stappen voor ongerichte kabelinterceptie af van de wijze waarop de keten van OOG-interceptie bij de diensten is ingericht.

De vraag met betrekking tot het chilling effect wordt als volgt beantwoord. Voor zover met chilling effect wordt bedoeld dat Nederlandse burgers hun gedrag en uitingen zouden aanpassen bij het gebruik van digitale middelen uit vrees voor “aftappen bij verkennen” omdat hun gegevens mogelijk in onderzoek worden genomen, kunnen wij aangeven dat OOG-interceptie wordt ingezet op landen met een offensief cyberprogramma en zich dus richt op internationale gegevensstromen, niet op nationale gegevensstromen. Door de werking van het internet kan het zich toch voordoen dat gegevens van Nederlandse burgers worden geïntercepteerd. Echter, zoals hiervoor toegelicht bij de vier verschillende fases van OOG-interceptie, kunnen uitsluitend gegevens betrokken worden in een inlichtingenonderzoek die gekoppeld zijn aan onderzoeken naar landen met een offensief cyberprogramma. De diensten richten zich dus op internationale gegevensstromen en hanteren een systeem waarbinnen er robuuste waarborgen gelden voordat gegevens betrokken kunnen worden in een inlichtingenonderzoek waarbij in elk geval de TIB in elke fase in de keten van OOG-interceptie toetst.

Op de vragen die zijn gesteld met betrekking tot het gebruik van AI reageren we als volgt. De Wiv 2017 spreekt over geautomatiseerde data-analyse (GDA) in plaats van AI. AI is onderdeel van het begrip GDA, dat een ruimere reikwijdte heeft omdat er ook andere algoritmische toepassingen onder vallen. GDA is een algemene bevoegdheid (art. 60, Wiv 2017) en kan in verschillende fasen van de OOG-keten worden toegepast. De toepassing van GDA in de OOG-keten gebeurt in de hierboven genoemde fasen twee en drie door daartoe aangewezen functionarissen en met een specifiek doel. Omdat GDA een vorm is van gegevensverwerking, moet ook worden voldaan aan de eisen van noodzaak, proportionaliteit en subsidiariteit. Pas in de vierde fase komen pas gegevens ter beschikking van het inlichtingenteam. Voordat die gegevens in het inlichtingenproces komen is er toestemming nodig voor search gericht op selectie en selectie (art. 49, lid 2 en art. 50, lid 1, onder a, Wiv 2017). Deze toestemming wordt getoetst door de TIB. De selectoren en zoekvragen zien ook enkel op onderzoeksgebieden uit de GA waar toestemming voor is gekregen.

Daarnaast hebben de diensten op grond van artikel 50 lid 1 sub b Wiv 2017 de bevoegdheid om GDA op OOG-metadata toe te passen ter identificatie van personen en organisaties, om de resultaten daarvan te betrekken in het inlichtingenonderzoek. De bevoegdheid kan ingezet worden na toestemming van de minister en de CTIVD krijgt, binnen het kader van de Tijdelijke wet, de bevoegdheid om bindend toezicht te houden. Het doorzoekbaar maken en doorzoeken van OOG-metadata met GDA is in de vierde fase van OOG-interceptie onmisbaar om relevante verbanden tussen gegevens over dreigingen van bijvoorbeeld personen en organisaties te kunnen onderkennen. Indien GDA of AI wordt toegepast is er altijd sprake van een menselijke weging die de verificatie doet op de resultaten. In de Wiv 2017 staat ook dat geautomatiseerde besluitvorming verboden is. De diensten mogen geen maatregelen jegens een persoon treffen die uitsluitend gebaseerd is op de resultaten van een GDA. Er moet altijd sprake zijn van menselijke validatie, weging en tussenkomst.

Met betrekking tot het nut van het verzamelen van bulkdata wijzen de fractieleden van GroenLinks-PvdA op het volgende. Tijdens de technische briefing in de Eerste Kamer op 14 november 2023 is een voorbeeld gegeven van waarom bulkdata soms noodzakelijk zijn. Het hoofd van de MIVD gaf aan dat dankzij bulkinterceptie kon worden vastgesteld dat het Assad-regime achter het gebruik van gifgas zat in Syrië. Op basis van de uitleg leek het alsof metadata (wie communiceert met wie en wanneer) voldoende was om deze conclusie te staven. Volgens deze leden lijkt dit voorbeeld, bedoeld als reden/illustratie voor bulkinterceptie, daarmee niet te voldoen aan subsidiariteit (het minst ingrijpende middel gebruiken waar mogelijk). De leden vragen de regering uit te leggen hoe in dit voorbeeld, dat illustratief is bedoeld, er sprake is van subsidiariteit, en zij vragen de regering eventueel andere voorbeelden te geven. Wij beantwoorden deze vraag graag als volgt.

Het voorbeeld dat de directeur van de MIVD tijdens de technische briefing in de Eerste Kamer heeft gebruikt, ziet op het gebruik van een reeds rechtmatig verworven bulkdataset (geen OOG-data) in combinatie met andere reeds bij de diensten aanwezige gegevens en was het bedoeld om het belang en de langdurige operationele waarde van bulkdatasets (niet zijnde OOG-data) toe te lichten. In dit geval betrof het een bulkdataset met locatie-metadata-gegevens waarmee, door het combineren van informatie uit openbare bronnen en uit andere inlichtingenmiddelen, de verantwoordelijke voor de gifgasaanval kon worden vastgesteld. Het gebruik van de bij de diensten aanwezige bukdataset was hierbij van doorslaggevend belang. De bulkdataset is in dit voorbeeld een noodzakelijke schakel geweest om gegevens die de diensten al hadden met elkaar te verbinden en te verrijken. Reeds aanwezige gegevens krijgen hierdoor meerwaarde. Bulkdatasets dienen veelal als naslagwerk, waarbij kenmerkend is dat niet op voorhand te bepalen is welke gegevens uit die bulkdatasets relevant zijn. De waarde zit juist in de gehele bulkdataset. Voorbeelden van een bulkdataset verkregen met bijzondere bevoegdheden zijn: een telefoonboek of kamer van koophandel gegevens uit Rusland of een set met technische gegevens zoals communicatie en locatiegegevens uit Syrië.

Voor de duidelijkheid moeten de begrippen bulkinterceptie (ether- en kabelinterceptie) en bulkverwerving (een bevoegdheid waarbij bulkdatasets worden verworven) van elkaar worden onderscheiden. Elke verwervende bevoegdheid – dus ook bulkinterceptie - moet voldoen aan de eisen van subsidiariteit, noodzaak, proportionaliteit, gerichtheid (met uitzondering van de verkennende bevoegdheid ten behoeve van OOG-interceptie in de Tijdelijke wet).

De fractieleden van GroenLinks-PvdA stellen dat de tijdelijke wet een expliciete wettelijke grondslag voor het ongericht verkennen ten behoeve van bulkinterceptie creëert, en dat het betreffende artikel ook een grondslag introduceert voor het onder bepaalde voorwaarden delen van (ongeëvalueerde) bulkdata met buitenlandse partnerdiensten. De leden stellen vervolgens dat de Wiv 2017 op dit moment geen specifieke bepaling bevat die dat mogelijk maakt. De leden stellen tot slot dat de Raad van State adviseert de mogelijkheid tot het delen van ongeëvalueerde gegevens afkomstig uit de bevoegdheid tot verkennen, uit het wetsvoorstel te schrappen, en dat dit advies niet is overgenomen.

De regering wenst op dit punt te verhelderen dat het onjuist is dat de Wiv 2017 geen specifieke bepaling zou bevatten die het delen van (ongeëvalueerde) bulkdata met buitenlandse diensten mogelijk maakt, en dat in de Tijdelijke wet hiervoor een grondslag zou worden geïntroduceerd. De artikelen 62, 64 en 89 van de Wiv 2017 bevatten een grondslag voor de diensten om gegevens te delen met buitenlandse diensten, ook ongeëvalueerde gegevens. Ook bij toepassing van de Tijdelijke wet zijn dit de grondslagen voor het delen van gegevens met buitenlandse diensten.

Aansluitend gaan de fractieleden van GroenLinks-PvdA erop in dat middels de tijdelijke wet deze bulkdata gedeeld mogen worden met buitenlandse diensten voor ‘technische ondersteuning’. De leden vragen of met het delen van data het geven van de mogelijkheid tot inzage wordt bedoeld of dat data (in bulk) overgedragen worden. Zij vragen de regering om aan te geven wat de voor- en nadelen van beide varianten zijn en waarom hiervoor gekozen wordt. Wij antwoorden de leden graag als volgt.

Een verstrekking van gegevens verkregen met de verkennende bevoegdheid als bedoeld in artikel 6 van de Tijdelijke wet heeft tot doel om met de ontvangen resultaten (beter) te kunnen vaststellen op welke gegevensstromen een verzoek om toestemming voor OOG-interceptie ex artikel 48 Wiv

2017 betrekking dient te hebben. Het doel van de verstrekking, de gevraagde ondersteuning en de wegingsnotitie over de betreffende buitenlandse dienst zijn bepalend voor de vorm waarin de verstrekking plaatsvindt. Het ter inzage aanbieden op een systeem van de dienst is één van de mogelijkheden, net als het verstrekken door het toesturen van gegevens (al dan niet in bulk). Als het verzoek ziet op bijvoorbeeld het ontsleutelen van bepaalde gegevens, zal de buitenlandse dienst doorgaans de eigen systemen nodig hebben om dat te realiseren, ook omdat een buitenlandse dienst meestal niet bereid is dergelijke technieken te delen met een andere dienst. In dit voorbeeld ligt een verstrekking van gegevens aan die buitenlandse dienst meer voor de hand.

De fractieleden van GroenLinks-PvdA vragen of bij het delen van bulkdata met buitenlandse diensten dit enkel achteraf, na 'beoordeling' van de data, zal kunnen plaatsvinden of dat er ook sprake kan zijn van het bijna live (*real time*) delen van bulkdata met buitenlandse diensten. Voornoemde fractieleden vragen de regering om een verduidelijking. Hiernaast vragen zij of het voor buitenlandse diensten technisch mogelijk is om verkeer van Nederlandse kabels gescheiden te houden. Wij beantwoorden deze vragen graag als volgt.

In de toelichting op artikel 6 is geëxpliciteerd dat de diensten de gegevens kunnen delen die zijn verkregen uit de bevoegdheid tot verkennen met het oog op toepassing van artikel 48 Wiv 2017 met buitenlandse diensten om ondersteuning te krijgen bij het technisch onderzoek van die gegevens. Een verstrekking kan – indien noodzakelijk – spoedig na verwerving plaatsvinden of op een later moment binnen de bewaartermijn van zes maanden. Het kan daarbij zowel gaan om gegevens die reeds beoordeeld zijn door de diensten als om gegevens die de diensten nog niet hebben beoordeeld. Om de gegevens te kunnen beoordelen is juist ook het technisch onderzoek van buitenlandse diensten nodig.

In het kabellandschap bestaan geen Nederlandse kabels of Nederlands verkeer. Internetverkeer gaat immers over verschillende kabels. Als de diensten een bulkdataset delen met een buitenlandse dienst, kunnen zij dat wel scheiden van andere datasets die zij hebben.

De fractieleden van GroenLinks-PvdA wijzen erop dat het wetsvoorstel een tijdelijke wet betreft. Zij stellen dat daarom niet uit te sluiten is dat op enig moment in de toekomst deze informatiestroom stopt en dat het stoppen zou kunnen worden geduid als een beschadiging door Nederland van de goede betrekkingen met de buitenlandse bevriende dienst. Zij vragen de regering welke maatregelen zijn voorzien om dit scenario te voorkomen, en of de regering ervoor kan instaan dat dergelijke argumentatie niet op een later moment richting de wetgever wordt ingezet om te betogen dat er niet gestopt kan worden met het opslaan of delen van deze informatie. Wij reageren hierop als volgt.

Zoals eerder in deze nota naar aanleiding van het verslag is gesteld biedt de Wiv 2017 reeds de mogelijkheid om gegevens – geëvalueerd en ongeëvalueerd, al dan niet in de vorm van bulkdata – te verstrekken aan buitenlandse diensten. In de Tijdelijke wet is dit waar het gaat om de gegevens die zijn verworven onder toepassing van de bevoegdheid ex artikel 6 beperkt en aan extra waarborgen onderworpen. Bij de herziening van de Wiv 2017 kan deze verstrekkingsregeling opnieuw aan de orde komen.

De leden van de GroenLinks-PvdA-fractie vragen of het klopt dat de finale keuze voor doorgifte van bulkdata bij de minister ligt en dat de toezichthouder middels de tijdelijke wet hierbij een adviserende rol heeft. Aansluitend vragen zij of de toezichthouder ook wordt geïnformeerd over de keuze van de minister in situaties waarover geadviseerd is, of de minister kan afwijken van de verzoeken van de diensten en zo ja, op basis waarvan dat mogelijk is. Ook vragen de leden of er sprake is van een discretionaire bevoegdheid en of er in dat kader waarborgen nodig zijn mocht er ooit sprake zijn van een minister met bijvoorbeeld pro-Russische sympathieën. Wij beantwoorden deze vragen graag als volgt.

Allereerst dient te worden opgemerkt dat de diensten opereren binnen de wettelijke kaders van de Wiv 2017 en de Tijdelijke wet met de daarbij behorende waarborgen. Zo is in artikel 6, zevende lid, van de Tijdelijke wet bepaald dat artikel 89, tweede lid, van de Wiv 2017 van overeenkomstige toepassing is, met dien verstande dat de verstrekking, behoudens een dringende en gewichtige reden, niet eerder plaatsvindt dan vijf dagen nadat de afdeling toezicht omtrent de verleende

toestemming is geïnformeerd. Dit betekent dat voor alle verstrekkingen als hier bedoeld de minister toestemming dient te verlenen; mandaat is niet mogelijk. Van belang is dat er altijd een verzoek van de dienst tot het delen van informatie aan ten grondslag ligt. Het betreft een discretionaire bevoegdheid van de minister, die een verzoek van de dienst om bulkdata te verstrekken aan een buitenlandse dienst dus kan afwijzen. Daartoe kunnen verschillende redenen bestaan, bijvoorbeeld dat de minister niet overtuigd is van de noodzaak maar ook omdat bijvoorbeeld de vertrekking vanwege (geo)politieke overwegingen niet opportuun wordt geacht. Behoudens de situatie van dringende en gewichtige redenen, een uitzonderingssituatie, geldt dat de verstrekking niet eerder plaatsvindt dan vijf dagen nadat de afdeling toezicht van de CTIVD wordt geïnformeerd omtrent de beslissing van de minister. Daarmee wordt aan de afdeling toezicht de gelegenheid geboden om in het kader van de reguliere toezichtstaak aan de verantwoordelijke minister kenbaar te maken dat zij bedenkingen (hetgeen geen advies is) heeft bij de voorgenomen verstrekking. Die bedenkingen hebben geen bindend karakter en derhalve is er geen sprake van bindend toezicht. De minister kan de verleende toestemming vervolgens heroverwegen. Hoewel niet expliciet geregeld, ligt het voor de hand dat de afdeling toezicht omtrent de uitkomst van de heroverweging wordt geïnformeerd. De afdeling toezicht is overigens niet verplicht om bedenkingen te uiten. Blijft de vijf dagentermijn onbenut dan kan de verstrekking gewoon doorgang vinden. Zoals hiervoor aangegeven vindt de toets door de afdeling toezicht plaats in het kader van haar reguliere toezichtstaak, hetgeen betekent dat men daarbij hetzelfde toetsingskader hanteert als bij de uitoefening van die reguliere toezichtstaak, namelijk op de rechtmatigheid van de uitvoering van hetgeen bij of krachtens de Wiv 2027 en de Tijdelijke wet is gesteld (zie artikel 97, derde lid, Wiv 2017 en artikel 2, tweede lid, Tijdelijke wet).

De fractieleden van GroenLinks-PvdA vragen ook of de stelling klopt dat het met de tijdelijke wet mogelijk wordt zo'n jaar lang een verkende kabel in z'n geheel te delen voor 'technische assistentie'. Ook vragen zij wat er eigenlijk bedoeld wordt met 'technische ondersteuning' en zij vragen de regering dit met enkele voorbeelden toe te lichten. Ons antwoord op deze vragen luidt als volgt.

De stelling dat het met de Tijdelijke wet mogelijk wordt zo'n jaar lang een verkende kabel in z'n geheel te delen voor 'technische assistentie is om meerdere redenen onjuist. Allereerst introduceert de Tijdelijke wet geen nieuwe grondslag voor het verstrekken van gegevens. De bevoegdheid tot het verstrekken van gegevens aan buitenlandse diensten, ook waar het gaat om bulkdata, is een bevoegdheid die al bestaat en is opgenomen in de Wiv 2017, te weten in de artikelen 62, 64 en 89, Wiv 2017. De Wiv 2017 bevat een aantal criteria aan de hand waarvan wordt bepaald of met een inlichtingen- en veiligheidsdienst kan worden samengewerkt en zo ja, wat de aard en intensiteit van die samenwerking kan zijn. Dit regime geldt ook voor het delen van gegevens uit de bevoegdheid tot verkennen, met dien verstande dat de Tijdelijke wet daaraan enkele beperkingen stelt, zoals doelbinding en een bewaartermijn van maximaal zes maanden waardoor het verstrekken van gegevens ouder dan zes maanden niet mogelijk is.

Belangrijker nog is het feit dat een verstrekking van gegevens moet passen bij het doel van de verkennende bevoegdheid voor OOG-interceptie – vaststellen in hoeverre een gegevensstroom kan bijdragen aan een verzoek om toestemming als bedoeld in artikel 48 Wiv 2017 – moet voldoen aan de eisen van noodzaak, behoorlijkheid en zorgvuldigheid en moet passen binnen de randvoorwaarden die aan de hand van een wegingsnotitie aan de samenwerking met een buitenlandse dienst door de minister zijn vastgesteld. Als het gaat om de verstrekking van ongeëvalueerde gegevens is ook eerst altijd toestemming nodig van de voor de dienst verantwoordelijke minister en wordt de afdeling toezicht van de CTIVD van een verleende toestemming terstond op de hoogte gesteld. Als gevolg van het door de Tweede Kamer aangenomen amendement Hammelburg (nr. 23) vindt een verstrekking pas plaats nadat vijf dagen zijn verstreken vanaf de mededeling aan de afdeling toezicht van de CTIVD. Artikel 90 van de Wiv 2017 biedt de wettelijke grondslag voor de AIVD en de MIVD om in het kader van een goede taakuitvoering een verzoek te doen aan een buitenlandse dienst tot het verlenen van technische of andere vormen van ondersteuning. De gevraagde technische ondersteuning kan zich onder andere richten op het onderzoeken van de gebruikte technische protocollen en de toegepaste versleuteling. Zo kan de desbetreffende buitenlandse dienst technische informatie geven over hoe deze gegevens het beste verwerkt kunnen worden. Dit kan bijdragen aan een gerichtere formulering van het

verzoek om toestemming voor OOG-interceptie ten behoeve van inlichtingenonderzoek ex artikel 48 Wiv 2017.

De fractieleden van GroenLinks-PvdA vragen of er een indicatie is te geven van het aantal keren dat het vragen om 'technische ondersteuning' van buitenlandse diensten aan de orde is geweest, en hoe is geborgd dat deze ongeëvalueerde bulkdata door buitenlandse diensten ook echt alleen voor 'technische ondersteuning' worden gebruikt. Deze leden vragen of er waarborgen zijn, zo ja, hoe die eruitzien en zo nee, wat dit betekent voor de vanuit de Grondwet en de internationale verdragen noodzakelijke waarborgen bij het delen van informatie. Wij beantwoorden deze vragen graag als volgt.

Het samenwerken met buitenlandse diensten is een dagelijkse praktijk. Technische samenwerking vindt al langdurig plaats in het domein van niet-kabelgebonden interceptie. Dit kan zowel incidentele samenwerking zijn als samenwerking in een meer structurele vorm. Een indicatie van het aantal verzoeken om ondersteuning zegt niets over de aard en omvang van de verzochte ondersteuning. Daarover kunnen geen mededelingen worden gedaan vanwege het staatsgeheime karakter van de verzoeken. Een enkel ondersteuningsverzoek kan een verzoek tot doorlopende ondersteuning zijn waarbij meerdere keren ondersteuning wordt verleend. Als waarborg geldt, op grond van artikel 65, tweede lid, Wiv 2017, dat de diensten verplicht zijn om in alle gevallen waarbij sprake is van verstrekking van gegevens aan inlichtingen- en veiligheidsdiensten van andere landen, de voorwaarde te stellen dat degene aan wie de gegevens worden verstrekt, deze gegevens niet aan anderen mag verstrekken (de zogeheten derde partijregel). Uitsluitend de voor de dienst verantwoordelijke minister, of namens deze het hoofd van de dienst, kan aan de ontvangende dienst alsnog toestemming verlenen om de gegevens aan andere personen of instanties te verstrekken, waaraan voorwaarden kunnen worden verbonden (artikel 65, derde lid, Wiv 2017). Het is ook gangbaar dat verstrekkingen plaatsvinden binnen een kader van gemaakte afspraken, dit kunnen internationale richtlijnen zijn van bijvoorbeeld de NAVO of bi- dan wel multilaterale afspraken tussen de AIVD, MIVD en buitenlandse diensten. Indien geconstateerd wordt dat een dienst van een ander land zich niet aan de afspraken houdt, zal de samenwerkingsrelatie met die dienst opnieuw worden gewogen. Afhankelijk van de uitkomst wordt besloten of de samenwerkingsrelatie moet worden voortgezet en, zo ja, wat dan de aard en de intensiteit van die relatie – mede in het licht van de geconstateerde vertrouwensbreuk – moet zijn. Dat kan betekenen dat met de desbetreffende buitenlandse dienst geen gegevens meer mogen worden gedeeld. Schending van het wederzijdse vertrouwen is namelijk een doodzonde in de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten.

Ten aan zien van de bescherming van persoonsgegevens en de constitutionele en internationale verplichting daartoe is ten eerste van belang dat, zoals hierboven uiteengezet, de regering gedegen reden heeft om erop te vertrouwen dat wanneer gegevens onder voorwaarden worden gedeeld, deze voorwaarden ook worden nageleefd. Dit betekent dat de gegevens in kwestie niet gebruikt worden voor het inlichtingenproces van de partnerdienst. Daardoor is de impact van de gegevensdeling op de persoonlijke levenssfeer minimaal. Ten tweede moet worden vastgesteld dat zowel de Grondwet als internationale verdragen impliciet dan wel expliciet ruimte laten voor verwerking van persoonsgegevens ten behoeve van de nationale veiligheid. Zo staat de Grondwet toe dat bij wet beperkingen worden gesteld aan de eerbiediging van de persoonlijke levenssfeer[17], laat het EVRM beperkingen toe die bij wet zijn voorzien en noodzakelijk zijn in een democratische samenleving (waarbij bescherming van nationale veiligheid nadrukkelijk genoemd wordt als zijnde in het belang van de democratische samenleving)[18] en zijn activiteiten ten behoeve van de nationale veiligheid uitgezonderd van toepassing van de Algemene Verordening Gegevensbescherming[19]. Ten derde wordt benadrukt dat sinds de inwerkingtreding van de Wiv 2017 aan de gegevensdeling een wegingsnotitie vooraf dient te gaan, waarbij onder andere wordt gekeken naar de mensenrechtensituatie in het land van de partnerdienst en het door de partnerdienst geboden niveau van gegevensbescherming.

[17] Artikel 10 Grondwet.
[18] Artikel 8, tweede lid, EVRM.
[19] Overweging 16 en artikel 23, eerste lid, onder a) van de AVG.

Tot slot wordt opgemerkt dat verstrekking van gegevens aan diensten waarmee geen samenwerkingsrelatie bestaat weliswaar in artikel 64 Wiv 2017 is toegestaan, maar die mogelijkheid is bedoeld voor situaties waarin een dringende en gewichtige reden daartoe noodzaakt.

De fractieleden van GroenLinks-PvdA vragen of het klopt dat op het delen van gegevens met buitenlandse collegadiensten in de tijdelijke wet geen bindend toezicht is door de CTIVD, dus dat de CTIVD alleen kan adviseren. Ook vragen deze leden wat de grondslag is voor de inhoudelijke toetsing door de CTIVD op het delen van bulkinfo met buitenlandse diensten voor 'technische ondersteuning'. Voornoemde fractieleden wensen hierbij een verwijzing naar de betreffende artikelen te ontvangen. Wij reageren hierop als volgt.

Voor de beantwoording van deze vragen wordt verwezen naar de hiervoor gegeven antwoorden op soortgelijke vragen van de fractie van GroenLinks-PvdA over de finale keuze voor doorgifte van bulkdata die bij de minister ligt en adviserende rol hierin van de toezichthouder.

De fractieleden van GroenLinks-PvdA wijzen erop dat ten behoeve van het wel/niet delen van informatie met buitenlandse diensten wegingsnotities worden opgesteld. In deze notities komen onderstaande wegingsaspecten (een vijftal plus twee aanvullende) aan de orde:
1. De democratische inbedding van een dienst: wat is zijn wettelijke basis en hoe is de (parlementaire) controle in het land geregeld?
2. De mensenrechtensituatie in een land: zijn er internationale mensenrechtenverdragen getekend en houdt het land – bijvoorbeeld op het gebied van persvrijheid – zich hieraan?
3. Professionaliteit en betrouwbaarheid: kan erop vertrouwd worden dat een dienst professioneel omgaat met informatie? Deze afweging wordt gemaakt op basis van eerdere ervaringen van de Nederlandse diensten en die van andere diensten.
4. Wettelijke bevoegdheden en mogelijkheden: wat kan en mag de dienst van een land doen in vergelijking met de AIVD?
5. Niveau van gegevensbescherming: hoe gaat de dienst om met het opslaan en vernietigen van verzamelde gegevens?

Daarnaast wordt gesteld door de AIVD: "wij [wegen] ook mee of de samenwerking een toegevoegde waarde voor ons heeft of dat die wenslijk is in verband met internationale verplichtingen. Ook is voor ons het quid pro quo-principe (voor wat hoort wat) van belang".[20]

In algemene zin merken wij over internationale samenwerking graag het volgende op. De AIVD en de MIVD werken sinds jaar en dag samen met buitenlandse diensten. Deze samenwerking heeft door de internationale ontwikkelingen op veiligheidsgebied alleen maar aan belang en intensiteit gewonnen. Samenwerking met buitenlandse diensten is ook van belang, omdat op deze wijze voor de nationale veiligheid van Nederland belangrijke informatie kan worden verkregen. De regering benadrukt dat intensieve internationale samenwerking, en daarmee ook de uitwisseling van ongeëvalueerde gegevens, onmisbaar is. Of het nu gaat om het uitwisselen van persoonsgegevens van terroristen die Europa inreizen, het uitwisselen van identificeerbare kenmerken van cyberaanvallen gericht op het hoogwaardig Europees bedrijfsleven of het met bondgenoten uitvoeren van militaire operaties in brandhaarden over de wereld: de razendsnelle uitwisseling van gegevens blijft doorslaggevend voor het nemen van adequate tegenmaatregelen en het verkrijgen van een adequaat dreigingsbeeld. Door binnen de internationale inlichtingen- en veiligheidswereld intensief met elkaar samen te werken, vallen afzonderlijke puzzelstukjes in elkaar, zodat het werkelijke gezicht van de dreiging zich laat zien.

In de praktijk van samenwerking van inlichtingen-, veiligheids- en SIGINT-diensten is bij de uitwisseling van informatie het beginsel van "quid pro quo" (voor wat hoort wat) een belangrijk element. Het is van belang te beseffen dat bij internationale samenwerking binnen de inlichtingenwereld een tweezijdige relatie wordt aangegaan. Overigens is ook de *need to share* een belangrijk beginsel. Bijvoorbeeld binnen het verband van de Counter Terrorism Group (CTG) speelt «quid pro quo» een beperktere rol omdat in de samenwerking tussen de Europese diensten informatie, die betrekking heeft op terrorisme dreigingen jegens een van de aangesloten landen,

[20] https://www.aivd.nl/onderwerpen/samenwerking-met-buitenlandse-diensten.

verwacht wordt te worden verstrekt zonder dat er iets voor wordt terugverwacht. Ook bij militaire operaties is het delen van informatie cruciaal. Aldus kan gefragmenteerde informatie worden gecompleteerd. Zonder de uitwisseling van gegevens zal mogelijk geen van de partijen ooit het benodigde inzicht verkrijgen. Bij het uitwisselen van gegevens, maar ook bij het gezamenlijk uitvoeren van operaties, is naast het "quid pro quo-beginsel" ook altijd sprake van een gedeeld belang en mag het belang van een buitenlandse dienst niet onverenigbaar zijn met de belangen die de diensten te behartigen hebben.

De intensieve internationale samenwerking betekent niet dat de regering zonder voorafgaande afweging informatie deelt. Integendeel: voor de internationale uitwisseling van ongeëvalueerde gegevens is er één deur en die is voorzien van vier sloten. Allereerst kan alleen met andere diensten worden gedeeld wat rechtmatig door onze diensten is vergaard (eerste slot). Ook werken de diensten bij de uitwisseling van ongeëvalueerde gegevens slechts met een zeer beperkt aantal landen samen (tweede slot). Eerbied voor de mensenrechten en democratische inbedding worden gewogen, voordat er wordt samengewerkt (derde slot). Ook houdt de afdeling toezicht van de CTIVD toezicht op deze praktijk (vierde slot).

In internationale samenwerking zijn de wegingsnotities leidend. Het wettelijk kader van de betreffende buitenlandse dienst en in welke mate gegevensbescherming plaatsvindt is één van de aspecten die wordt meegewogen bij de beslissing om (ook in een specifiek geval) samen te werken met een buitenlandse dienst. Een dergelijke samenwerking is dus aan beide kanten voorzien met waarborgen. In het kader van een technisch ondersteuningsverzoek aan een buitenlandse dienst, kan er ook geen sprake zijn van verzoeken waarbij een buitenlandse dienst een bevoegdheid uitoefent die de AIVD en MIVD niet hebben. Dit is verboden op grond van artikel 90, vijfde lid, van de Wiv 2017.

De fractieleden van GroenLinks-PvdA hebben enkele vragen over de wegingsnotities en over de (onderlinge) weging van de verschillende factoren. Zo vragen zij waar de werkwijze rondom wegingsnotities is geregeld en zij verzoeken daarbij concrete verwijzingen naar wet- en regelgeving te ontvangen. Wij beantwoorden deze vragen als volgt.

De werkwijze met betrekking tot wegingsnotities is geregeld in artikel 88 van de Wiv 2017. Voorafgaand aan het aangaan van een samenwerkingsverband met een buitenlandse dienst wordt een wegingsnotitie opgesteld (artikel 88, tweede lid, Wiv 2017). Daarbij worden in ieder geval de criteria worden betrokken die zijn genoemd in artikel 88, derde lid. Aan de hand van die weging wordt bepaald of kan worden overgegaan tot een samenwerkingsrelatie en, zo ja, wat de aard en de intensiteit van de beoogde samenwerking kan zijn. De afdeling toezicht van de CTIVD houdt toezicht op internationale samenwerking door de diensten en kan daarin ook de wegingsnotities betrekken.

De fractieleden van GroenLinks-PvdA vragen aansluitend of er een, al dan niet fictief, voorbeeld kan worden gegeven waaruit blijkt wat er bedoeld wordt met de wegingsfactor ‘samenhangend met internationale verplichtingen’. Ons antwoord hierop luidt dat hierbij gedacht kan worden aan verplichtingen of afspraken die voortvloeien uit deelname aan samenwerkingsrelaties in Europa of samenwerkingsverbanden binnen de NAVO.

De fractieleden van GroenLinks-PvdA fractieleden hebben begrepen dat de wegingsnotities één keer per vier jaar gemaakt worden en aan de hand van actualiteiten kunnen worden aangepast en zij vragen of dit klopt. Wij reageren hierop als volgt.

De wegingsnotities worden conform het interne beleid van de diensten inderdaad één keer per vier jaar volledig herzien. Daarnaast moet een wegingsnotitie op grond van artikel 88, vijfde lid, van de Wiv 2017 aangepast worden indien er omstandigheden zijn die daartoe aanleiding geven. De samenwerking met buitenlandse diensten en de aard en intensiteit van die samenwerking kunnen in de loop der tijd aan verandering onderhevig zijn.

De fractieleden van GroenLinks-PvdA vragen vervolgens of deze wegingsnotities per land worden gemaakt, en van hoeveel landen er op dit moment een actuele wegingsnotitie is. Wij antwoorden de leden graag als volgt.

Wegingsnotities worden niet per land gemaakt, maar per samenwerkingsrelatie. Een land kan meerdere inlichtingen- en/of veiligheidsdiensten hebben waarmee wordt samengewerkt. Er kunnen dus per land meerdere wegingsnotities zijn. Over het precieze aantal wegingsnotities kunnen geen uitspraken worden gedaan omdat het staatsgeheim is, maar wel kan verwezen worden naar rapport 60 van de afdeling toezicht van de CTIVD waarin het volgende wordt gezegd over het onderzoek dat de afdeling toezicht van de CTIVD heeft gedaan naar de wegingsnotities van de AIVD en MIVD: "Het is niet mogelijk het precieze aantal te noemen, omdat het aantal sigint-samenwerkingspartners staatsgeheim is. "Meer dan veertig" betreft de 29 CTG-partnerdiensten en een aantal sigint-samenwerkingspartners."[21]

De fractieleden van GroenLinks-PvdA vragen voorts of alle hiervoor genoemde wegingsaspecten in alle notities worden beschreven, dus ook de laatste twee aanvullende wegingsfactoren, en op welke wijze de laatste twee factoren ('internationale verplichtingen' en 'voor wat hoort wat') meewegen. De leden vragen of deze twee wegingsfactoren gelijkwaardig zijn aan de eerste vijf wegingsfactoren. De laatste twee wegingsfactoren zijn volgens deze fractieleden van een andere orde en zij vragen de regering in algemene zin iets te zeggen over het onderlinge gewicht van de verschillende wegingsfactoren. Wij reageren hierop graag als volgt.

Alle in artikel 88, derde lid, Wiv 2017 genoemde criteria worden betrokken en gewogen in de weging. Het zijn criteria die conform deze bepaling in ieder geval bij de weging moeten worden betrokken; ook andere (niet wettelijke) criteria, zoals de twee criteria waaraan in de vraagstelling wordt gerefereerd, worden bij de weging betrokken. Met de vijf wettelijke criteria worden de risico's van een eventuele samenwerkingsrelatie met de betreffende dienst inzichtelijk gemaakt. De weging is afhankelijk van de mate waarin informatie beschikbaar is over een bepaald criterium en de factoren aan de hand waarvan dat criterium wordt ingevuld; onvoldoende duidelijkheid of beschikbaarheid van informatie betekent dat er geen goed oordeel kan worden gegeven op welke wijze of in welke mate wordt voldaan aan het betreffende criterium en zal uit voorzorg leiden tot de vaststelling dat sprake is van een verhoogd risico in de weging van dat criterium. Naast het vaststellen van de eventuele risico's op basis van in ieder geval de vijf wettelijke criteria betrekken de AIVD en MIVD aanvullend in de weging wat de belangen zijn bij de totstandkoming van een samenwerkingsrelatie met de betreffende dienst. Dit zijn geen wettelijke criteria en de weging staat los van risico's of voorwaarden. In die zin zijn deze twee wegingsfactoren inderdaad van een andere orde. Bij deze twee factoren wordt namelijk meegenomen of de samenwerking bevorderlijk is voor een adequate taakuitvoering of wenselijk is in verband met internationale verplichtingen of afspraken.

Het quid-pro-quo-principe is internationaal een bekend uitgangspunt dat doorgaans wordt nageleefd bij internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Uiteindelijk wordt in samenhang bezien of en onder welke voorwaarden en binnen welke bandbreedte kan worden samengewerkt waarbij vervolgens per concrete samenwerkingsactiviteit moet worden vastgesteld door toetsing aan de wegingsnotitie of deze hierbinnen valt.

De fractieleden van GroenLinks-PvdA vragen of het kan voorkomen dat vanwege het meewegen van een van beide laatste (of beide) wegingsfactoren informatie gedeeld wordt met landen die geen voldoende scoren op alle vijf de andere wegingsfactoren. Wij beantwoorden deze vraag als volgt.

De genoemde situatie kan zich inderdaad voordoen. Voor het aangaan van een samenwerking en het daarbij delen van informatie is het niet verplicht op alle wegingsfactoren een voldoende te scoren. Het delen van informatie met een (dienst van een) ander land is altijd een afweging van de belangen die worden gediend bij verstrekking, de mogelijke risico's die zich voor kunnen doen en in hoeverre deze risico's op voorhand kunnen worden gemitigeerd door het stellen van bepaalde voorwaarden. Het uiteindelijke resultaat van de weging moet antwoord geven op de vraag of en, zo ja, kan worden overgegaan tot het aangaan van een samenwerkingsrelatie. Die weging – of althans het resultaat daarvan – zal in de praktijk van dienst tot dienst variëren. Het is bovendien ook geen

[21] CTIVD rapport 60 over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners (2018), p. 5.

mathematische aangelegenheid. Naast de wettelijk vastgelegde criteria zullen ook concrete operationele belangen in relatie tot het door de diensten te beschermen belang van de nationale veiligheid een belangrijke rol kunnen spelen. Zoals de afdeling toezicht van de CTIVD heeft opgemerkt in de rapporten 22a en 22b dienen de diensten de grootst mogelijke terughoudendheid te betrachten in de samenwerking met diensten van landen waar nauwelijks tot geen democratische traditie bestaat en waar (structureel) mensenrechten worden geschonden, maar dat het op voorhand uitsluiten van samenwerking in de praktijk zou kunnen leiden tot onwenselijke of zelfs rampzalige situaties, bijvoorbeeld bij een dreigende terroristische aanslag

In de weging wordt derhalve uiteindelijk bepaald waarom samenwerking met een buitenlandse dienst – ook indien niet aan alle eisen wordt voldaan – noodzakelijk is, op welke wijze die samenwerking wordt ingevuld en welke randvoorwaarden daarbij gelden. In het kader van de weging zullen ook de risico's die aan een eventuele samenwerking verbonden zijn in kaart te worden gebracht. Dat bepaalt onder meer waaruit die samenwerking dan kan bestaan (en waaruit niet). Daarbij moet onder meer worden gedacht aan zaken als ten aanzien van welke onderwerpen onder welke omstandigheden gegevensuitwisseling kan plaatsvinden en aan welke andere voorwaarden moet worden voldaan. Het uitwisselen van persoonsgegevens verdient hierbij uitdrukkelijk de aandacht. Bij diensten waarvan is gebleken dat risico's aan de samenwerking zijn verbonden wordt van oudsher terughoudendheid betracht bij het uitwisselen van persoonsgegevens. Uitgangspunt blijft dat op voorhand geen enkele samenwerking kan worden uitgesloten.

De fractieleden van GroenLinks-PvdA wensen een toelichting te ontvangen op de wijze waarop in een wegingsnotitie 'de weging' wordt gemaakt. Zij vragen of een wegingsnotitie een weging per wegingsaspect bevat en/of is er sprake van een weging als geheel van alle wegingsfactoren. Ook vragen zij onder wiens ambtelijke en bestuurlijke verantwoordelijkheid, en met wiens deskundigheid, deze wegingsnotities tot stand komen. Deze leden willen in dit kader weten of bijvoorbeeld de beschrijving van 'de mensenrechtensituatie in een land' door het ministerie van Buitenlandse Zaken wordt geleverd, en door wie de weging op dit onderdeel wordt gemaakt. Wij beantwoorden deze vragen graag als volgt.

Elk wegingsaspect speelt een rol en wordt apart van elkaar gewogen. Uiteindelijk wordt de weging per aspect samengenomen en wordt er één concluderende weging voor samenwerking gemaakt. Indien op één aspect een risico bestaat in de samenwerking, is reeds sprake van een risicodienst. De weging is afhankelijk van de mate waarin informatie beschikbaar is over een bepaald criterium en de factoren aan de hand waarvan dat criterium wordt ingevuld; onvoldoende duidelijkheid of beschikbaarheid van informatie is een sterke contra-indicatie voor de beoordeling van het betreffende criterium en zal uit voorzorg leiden tot de vaststelling dat sprake is van een verhoogd risico in de weging van dat criterium. Er wordt daarin geen onderscheid gemaakt tussen de verschillende wegingsaspecten.

Het vaststellen van de wegingsnotities vindt plaats onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie. De weging op alle criteria, dus ook die van de mensenrechtensituatie in een land, wordt gedaan door de AIVD en MIVD. Bij het opstellen van de wegingsnotities maken de diensten gebruik van verschillende gesloten en openbare bronnen, waaronder intern beschikbare informatie, landeninformatie van het Ministerie van Buitenlandse Zaken en rapporten van NGO's. Dit gebeurt op gestandaardiseerde wijze met een uitgebreide lijst van relevante openbare bronnen. Ook de betrouwbaarheid van internetbronnen wordt hierin meegenomen. Of een dienst in voldoende mate democratisch is ingebed hangt af van een aantal factoren. Zo wordt onder meer gekeken naar het algehele politieke bestel van het land in kwestie en de positie die de betreffende dienst daarin inneemt, de wettelijke bevoegdheden van de dienst, de democratische controle en het (onafhankelijke) toezicht op de dienst en mate waarin een land een scheiding der machten inclusief onafhankelijke rechtspraak kent. Met betrekking tot de eerbiediging van de mensenrechten wordt bezien of het desbetreffende land mensenrechtenverdragen heeft geratificeerd en of deze mensenrechtenverdragen in de praktijk worden nageleefd. De mate waarin een buitenlandse dienst als professioneel en als betrouwbaar kan worden beschouwd is grotendeels afhankelijk van de ervaringen van de AIVD en MIVD die zijn opgedaan in de samenwerkingsrelatie met de betrokken dienst. Voor de wettelijke bevoegdheden en mogelijkheden van een dienst wordt onder andere gekeken naar de wettelijke

kaders en de bevoegdheden die de betreffende dienst heeft. Het door de dienst geboden niveau van gegevensbescherming wordt beoordeeld aan de hand van waarborgen op het gebied van onder andere doelbinding, dataminimalisatie, bewaartermijnen en toezicht op gegevensbescherming.

De leden van de GroenLinks-PvdA-fractie verwijzen naar de antwoorden van de diensthoofden tijdens de technische briefing op 14 november 2023 op vragen van Eerste Kamerleden over wat voor criteria er zijn voor het delen van bulkdata met buitenlandse diensten. Daarbij werd als voorbeeld gegeven dat er niet met Saudi-Arabië gedeeld wordt, gezien de algemene mensenrechtensituatie aldaar. Dat antwoord ligt volgens deze leden in de lijn der verwachting, maar zij vragen hoe het zit met landen buiten de EU die als bondgenoten worden beschouwd, in het bijzonder de Verenigde Staten en het Verenigd Koninkrijk. Wij reageren hierop graag als volgt.

Het wettelijk kader maakt geen onderscheid tussen diensten of tussen landen. Diensten uit landen buiten de EU, ook die van bondgenoten zoals de VS en het VK, worden gewogen aan de hand van dezelfde criteria en dezelfde methodiek als diensten van andere landen.

De leden van de GroenLinks-PvdA-fractie constateren vervolgens dat de tijdelijke wet regelt dat in afwijking van de Wiv 2017 de beoordelingstermijn van bulkdatasets die verworven zijn met de uitoefening van een bijzondere bevoegdheid, steeds met een jaar kan worden verlengd. Op het proces van de verlenging van de termijn houdt de CTIVD volgens het wetsvoorstel bindend toezicht. De regeling is niet van toepassing op bulkdatasets die met behulp van onderzoeksopdrachtgerichte interceptie (hierna: OOG-interceptie) zijn verworven, omdat deze bulkdata een eigen regeling kennen in de Wiv 2017.

De Evaluatiecommissie Wiv stelt voor een geheel nieuw bulkdataregime in te voeren en doet een groot aantal aanbevelingen hiervoor.[22] Deze aanbevelingen worden meegenomen bij de brede herziening van de Wiv 2017. De Raad van State stelt hierover:

"*De vraag rijst in dit verband of alleen het verlengen van de beoordelingstermijn voor bulkdatasets recht doet aan het bredere vraagstuk omtrent bulkdatasets. Verlenging van de beoordelingstermijn is onlosmakelijk verbonden met de andere aanbevelingen die de Evaluatiecommissie heeft gedaan. Dat betreft met name de regeling van belangrijke waarborgen. Zo raakt de voorgestelde bepaling onder meer aan de vraag of niet alle bulkdatasets onder deze regeling moeten vallen, of er niet een maximum termijn moet komen voor het beoordelen op relevantie, en of een onderscheid tussen soorten bulkdatasets (zoals het onderscheid tussen registerbulkdata en gedragsbulkdata) niet noodzakelijk is.*"[23]

De regering deelt de mening van de Raad van State, dat verlenging van de bewaartermijn onlosmakelijk met de andere aanbevelingen is verbonden, en stelt het volgende:
"*De uitwerking van al deze aanbevelingen in samenhang bezien in een concreet (onderdeel van een) wetsvoorstel is echter een complexe (wetgevings)operatie. Dat vergt de nodige tijd. Deze brede problematiek zal dan ook meegenomen worden bij de voorgenomen herziening van de Wiv 2017.*"[24]

De fractieleden van GroenLinks-PvdA hebben enkele vragen over bulkdatasets, mede naar aanleiding van de advisering daaromtrent door de Evaluatiecommissie Wiv en de Raad van State. De leden stellen dat de verlenging volgens de regering onlosmakelijk verbonden is met het regelen van belangrijke waarborgen. De leden vragen waarom de regering ervoor kiest om nu al wel de bewaartermijn te verlengen en nog niet de daarmee samenhangende waarborgen te bepalen. De leden vragen of de regering deze analyse van voornoemde fractieleden deelt en zo nee, waarom niet en zo ja, wat hiervoor de motivering is. Wij beantwoorden deze vragen als volgt.

Bulkdatasets die met bijzondere bevoegdheden zijn verworven en nog essentieel zijn voor lopende onderzoeken van de diensten moeten op grond van de Wiv 2017 na anderhalf jaar vernietigd

[22] *Kamerstukken II 2020/21, 34 588, nr. 88, bijlage Evaluatie 2020. Wet op de inlichtingen- en veiligheidsdiensten 2017, p. 4-5.*
[23] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 26-27.*
[24] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 27.*

worden. Dit heeft grote impact op met name lopende buitenlandonderzoeken van de diensten. Door het vernietigen van bulkdatasets is de informatiepositie van de diensten verslechterd en zijn waardevolle gegevens verloren gegaan.

Naast de ECW geeft ook de afdeling toezicht van de CTIVD aan dat het wettelijk kader voor bulkdatasets aangepast moet worden, omdat de CTIVD, zowel de afdeling toezicht als de afdeling klachtbehandeling, van mening is dat bulkdatasets een langdurige operationele waarde kunnen hebben. Dit houdt in dat een set na bijvoorbeeld 10 jaar nog steeds relevante informatie kan opleveren voor lopende onderzoeken van de diensten. Zo lang er geen aanpassing van het wettelijk kader heeft plaatsgevonden, dienen bulkdatasets na anderhalf jaar vernietigd te worden, ook als zij nog operationele waarde hebben. Met de brede herziening van de Wiv 2017 zal in lijn met de ECW-aanbevelingen een geheel nieuw bulkstelsel opgenomen worden. Aangezien de brede herziening van de Wiv 2017 nog ter hand moet worden genomen, is de regering van oordeel dat niet op deze brede herziening kan worden gewacht, omdat de diensten steeds meer bulkdatasets dienen te vernietigen en dit een acuut probleem voor lopende onderzoeken oplevert. Om die reden wordt dit onderwerp geregeld in de Tijdelijke wet, mét belangrijke waarborgen. De afdeling toezicht van de CTIVD onderschrijft dit. In het wetsvoorstel wordt voorzien in een eindtermijn van anderhalf jaar, met de mogelijkheid om na deze eerste termijn een nieuwe eindtermijn vast te stellen indien er sprake is van dringende redenen met het oog op de nationale veiligheid. Hierbij moet gemotiveerd worden aangegeven op basis van de in de wet vastgestelde criteria waarom dit noodzakelijk is. Deze beoordeling zorgt ervoor dat bulkdatasets niet langer bewaard zullen worden dan strikt noodzakelijk. Het zorgt er juist voor dat op de juiste, meeste proportionele wijze, per bulkdataset wordt gedifferentieerd in de gebruikstermijn van de bulkdatasets. Als extra waarborg voor het vaststellen van een nieuwe eindtermijn, geldt dat de afdeling toezicht van de CTIVD op het besluit tot vaststelling van een nieuwe eindtermijn bindend toezicht kan houden waarbij de afdeling toezicht in elk geval de rechtmatigheid onderzoekt van het derde opeenvolgende besluit tot het vaststellen van een nieuwe eindtermijn.

Bulkdatasets die met algemene bevoegdheden zijn verworven, zijn op een andere wijze ontsloten op de systemen van de diensten dan de bulkdatasets die met bijzondere bevoegdheden zijn verkregen. Dit gelijkschakelen zou betekenen dat bulkdatasets die met algemene bevoegdheden zijn verworven in hetzelfde systeem opgenomen moet worden als bulkdatasets die met bijzondere bevoegdheden zijn verworven. Eén bulkregime, waarbij de sets dus in de interne systemen van de diensten gelijk worden ontsloten, betreft een zeer omvangrijke IT-operatie en kan niet op korte termijn plaatsvinden. Het zou het implementatietraject van de Tijdelijke wet doorkruisen en de inwerkingtreding van dit onderdeel aanzienlijk vertragen hetgeen, gelet op de urgentie van het Tijdelijke wet, niet zonder risico's voor de nationale veiligheid is. Een dergelijke ingrijpende operatie is niet passend voor een Tijdelijke wet die urgente problematiek adresseert en is dus niet uitvoerbaar op dit moment. Met de herziening van de Wiv 2017 zal in lijn met de ECW-aanbevelingen een geheel nieuw bulkstelsel opgenomen worden.

De regering hecht eraan te benadrukken dat een groot deel, meer dan 80%, van de bulkdatasets waarover de diensten op dit moment beschikken, zien op gegevens uit het buitenland. De reden hiervoor is dat de diensten in het buitenland doorgaans veel minder mogelijkheden hebben voor een gerichtere inzet van bevoegdheden. Gegevens over personen in Nederland zouden op verschillende andere manieren, met inzet van andere gerichte bevoegdheden verkregen kunnen worden.

Tot slot kan worden gewezen op de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017[25] die ook van toepassing zal zijn op de bulkdatasets die binnen het bereik van dit wetsvoorstel vallen. Deze regeling bepaalt dat na één, twee of drie jaar getoetst moet worden of de bulkdataset langer gebruikt mag worden en dat een verwerkingsregime van toepassing is met passende waarborgen, afhankelijk van de beperking die het gebruik van deze bulkdataset kan hebben op het recht op de eerbiediging van de persoonlijke levenssfeer. De waarborgen zien bijvoorbeeld op functiescheiding (enkel specifiek aangewezen personen mogen de bulkdataset bevragen) en de wijze van bevraging van een bulkdataset (zogenaamde *hit - no hit*).

[25] Stcrt. 2020, 56482.

De fractieleden van GroenLinks-PvdA vragen hoe volgens de regering de door de Raad van State gestelde noodzakelijke zorgvuldige afweging is geborgd in de tijdelijke wet en waarom er niet is gekozen voor een wettelijke eindtermijn in de tijdelijke wet. De leden achten dat logisch in afwachting van een gehele herziening van de Wiv 2017. Wij reageren hierop graag als volgt.

De Tijdelijke wet voorziet in een eindtermijn van anderhalf jaar voor het gebruik van bulkdatasets die met bijzondere bevoegdheden (met uitzondering van OOG-interceptie) zijn verworven. De Raad van State heeft ook aangegeven dat er een uitzonderingsmogelijkheid overwogen kan worden om bulkdatasets langer te kunnen gebruiken indien het noodzakelijk is voor de nationale veiligheid. Met de Tijdelijke wet wordt het mogelijk om, voor bulkdatasets waarvan de eindtermijn verloopt, onder voorwaarden een nieuwe eindtermijn van ten hoogste een jaar te stellen voor het gebruik van een bulkdataset in het geval van dringende redenen met het oog op de nationale veiligheid. Om hieraan te kunnen voldoen, is er een aantal criteria opgenomen in artikel 14ba, tweede lid. Op grond van de uitwerking van de wettelijke criteria in het toestemmingsverzoek beoordeelt de verantwoordelijke minister of alles afwegende, inderdaad sprake is van dringende redenen met het oog op de nationale veiligheid. Indien wordt voldaan aan de in de voorliggende wet vastgelegde criteria, is daarmee voldaan aan de maatstaf van dringende redenen van nationale veiligheid die het noodzakelijk maken dat een nieuwe eindtermijn wordt vastgesteld. Zo moet onder andere de noodzaak, proportionaliteit en subsidiariteit gemotiveerd worden alsmede aangegeven worden hoelang de bulkdataset reeds wordt bewaard en wat de verwachte potentiële bijdrage is aan enig lopend onderzoek. Als extra waarborg hiervoor, kan de afdeling toezicht van de CTIVD bindend toezicht houden op het besluit tot het vaststellen van een nieuwe eindtermijn waarbij de afdeling toezicht in elk geval de rechtmatigheid onderzoekt van het derde opeenvolgende besluit tot het vaststellen van een nieuwe eindtermijn. Met bovengenoemde criteria is sprake van voldoende waarborgen. De CTIVD onderschrijft dit ook.

Daarnaast is de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 ook van toepassing op de bulkdatasets die binnen het bereik van dit wetsvoorstel vallen. Deze regeling is toegelicht in het antwoord op de voorgaande vraag.

De leden van de D66-fractie wijzen erop dat in het wetsvoorstel wordt bepaald dat informatie die verkregen is door middel van OOG-interceptie, uitsluitend met buitenlandse diensten gedeeld mag worden vijf dagen nadat de door de Minister verleende toestemming is gedeeld met de afdeling toezicht van de CTIVD. De D66-fractieleden vragen of de regering kan aangeven in hoeverre dit consequenties kan hebben voor de internationale samenwerking tussen diensten. Zou deze bepaling de samenwerking kunnen doorkruisen in het geval de CTIVD voor het delen van deze informatie gaat liggen? En zou het delen van informatie met buitenlandse diensten niet louter onder de ministeriële verantwoordelijkheid van de desbetreffende minister moeten vallen? Hoe verhoudt zich dit tot het rechtmatigheidsoordeel van de CTIVD? Wij reageren hierop graag als volgt.

De verstrekking van ongeëvalueerde gegevens is een verantwoordelijkheid van de desbetreffende minister. Ook het amendement van het lid Hammelburg (nr. 23) verandert dit niet. De termijn biedt de afdeling toezicht van de CTIVD de gelegenheid om in het kader van haar reguliere toezichtstaak aan de verantwoordelijke minister kenbaar te maken dat zij bedenkingen heeft bij de voorgenomen verstrekking. De minister kan de verleende toestemming vervolgens heroverwegen. De impact van de termijn van vijf dagen op de operationele taakuitvoering van de diensten, voorafgaand aan een verstrekking van gegevens verkregen met de verkennende bevoegdheid ex artikel 6 Tijdelijke wet is werkbaar. De impact kan groter zijn in geval van spoed; dan kan een operatie immers niet voortgezet worden. Voor dergelijke gevallen is voorzien in een uitzondering.

De afdeling toezicht van de CTIVD kan op elk moment de rechtmatigheid beoordelen van een toestemming voor het delen van ongeëvalueerde gegevens en van de feitelijke verstrekking.

De fractieleden van de ChristenUnie wijzen erop dat een belangrijk vereiste bij het toepassen van bijzondere bevoegdheden dat van gerichtheid is. Artikel 26, vijfde lid, van de Wiv 2017 bepaalt in dat verband: “De uitoefening van een bevoegdheid dient zo gericht mogelijk te zijn.” De fractieleden stellen dat in het voorgestelde artikel 6, vierde lid die gerichtheidsbepaling in situaties waarop het wetsvoorstel ziet met zoveel woorden buiten toepassing wordt verklaard. De

fractieleden vragen of zij het goed zien dat dit de eerste wettelijke uitzondering is op de gerichtheidsregel en zij vragen of de regering de noodzaak van deze uitzondering concreet en met voorbeelden kan onderbouwen. Wij beantwoorden de vragen van deze leden graag als volgt.

Het is juist dat dit de eerste (en enige) uitzondering op het in de Wiv 2017 vastgelegde gerichtheidsvereiste is. De Tijdelijke wet maakt namelijk een uitzondering op de toepassing van het gerichtheidsvereiste ex artikel 26, vijfde lid, Wiv 2017 bij de uitvoering van de bevoegdheid tot OOG-interceptie ten behoeve van verkennen. Bij deze bevoegdheid, die juist dient om vast te stellen waarop de toepassing van artikel 48 Wiv 2017 (OOG-interceptie), waarbij sprake is van verwerving van gegevens ten behoeve van het inlichtingenproces, zich dient te richten, is de eis van gerichtheid bij de uitoefening van de verkenningsbevoegdheid naar zijn aard niet toepasbaar. Dit wordt tevens door de afdeling toezicht van de CTIVD in rapport 75 naar inzet van kabelinterceptie onderschreven.[26] Het is daarbij van belang te benadrukken dat deze bevoegdheid dient als opstap naar het indienen van een verzoek tot OOG-interceptie ten behoeve van het inlichtingenproces. Deze gegevens mogen dan ook alleen gebruikt worden ten behoeve van het indienen van dat verzoek. Voor de interceptie ten behoeve van het inlichtingenproces geldt de eis van gerichtheid onverkort.

De fractieleden van de ChristenUnie stellen dat het wetsvoorstel de mogelijkheid opent om onder bepaalde voorwaarden bulkdata te delen met diensten uit andere landen. Zij wijzen erop dat in de advisering door de Raad van State hierover kritische opmerkingen zijn gemaakt.[27] Deze leden vragen hoe de regering de verhouding beschouwt tussen deze nieuwe bevoegdheid en de waarborgen die passen bij een inbreuk op het recht op bescherming van de persoonlijke levenssfeer, zoals dat onder meer is vervat in artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Ook willen de leden weten hoe aan de door de Raad van State geopperde bezwaren is tegemoetgekomen. Wij reageren hierop graag als volgt.

De bevoegdheid tot het verstrekken van gegevens aan buitenlandse diensten, ook waar het gaat om bulkdata, is een bevoegdheid die al bestaat en is opgenomen in de Wiv 2017, te weten in de artikelen 62, 64 en 89, Wiv 2017. Wel is het zo dat de Wiv 2017 een aantal criteria bevat aan de hand waarvan wordt bepaald of met een inlichtingen- en veiligheidsdienst kan worden samengewerkt en zo ja, wat de aard en intensiteit van die samenwerking kan zijn. Dat kan ook betrekking hebben op de verstrekking van gegevens al dan niet in de vorm van bulkdata en over de voorwaarden die daaraan, los van de wettelijk voorgeschreven derde-partijregel, gesteld moeten worden. Daarnaast is in artikel 89, tweede lid, van de Wiv 2017 vastgelegd dat voor de verstrekking van ongeëvalueerde gegevens altijd de toestemming van de voor de dienst verantwoordelijke minister is vereist. Waar het gaat om de verstrekking van gegevens die zijn verworven in het kader van de bevoegdheid als bedoeld in artikel 6 van de Tijdelijke wet, geldt dat in het zevende lid, daarvan – naast doelbinding van de verstrekking – artikel 89, tweede lid, Wiv 2017 daarop van overeenkomstige toepassing is verklaard. Op de verstrekking zijn de algemene bepalingen, zoals neergelegd in paragraaf 3.1 van de Wiv 2017, van toepassing. Dat houdt onder meer in dat een verstrekking als hier bedoeld slechts plaats mag vinden voor een bepaald doel, noodzakelijk moet zijn voor een goede uitvoering van de wet, in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze plaats dient te vinden. Voor zover het gaat om de verwerking van persoonsgegevens zal daarbij voldaan dienen te worden aan de eisen die artikel 8 EVRM stelt en de jurisprudentie die in dat kader door het EHRM is ontwikkeld. In hoofdstuk 9 van de memorie van toelichting op het wetsvoorstel dat tot de Wiv 2017 heeft geleid is uitvoerig ingegaan op de betekenis van het EVRM en de jurisprudentie van het EHRM voor het wettelijk kader voor inlichtingen- en veiligheidsdiensten en de wijze waarop die eisen in de Wiv 2010 zijn uitgewerkt. Ook in de memorie van toelichting op onderhavig wetsvoorstel en in het kader van de behandeling van het wetsvoorstel in de Tweede Kamer is daar – meer toegespitst op hetgeen in de Tijdelijke wet wordt geregeld – in aanvullende zin daarop ingegaan. Kortheidshalve wordt daarnaar verwezen.[28] Waar het gaat om de bezwaren van de Afdeling advisering van de Raad van State, die van oordeel was dat verstrekking van ingevolge artikel 6 van de Tijdelijke wet verworven gegevens aan een buitenlandse dienst niet zou mogen plaatsvinden, is in reactie daarop in het nader rapport

[26] Toezichtsrapport 75 over de inzet van kabelinterceptie door de AIVD en de MIVD - De snapshotfase (2022), p. 55.
[27] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 22-23.*
[28] *Kamerstukken II 2022/2023, 36 263, nr. 3, p. 39 e.v.*

uiteengezet waarom de mogelijkheid om een dergelijke verstrekking wel dient te bestaan.[29] Allereerst geldt dat de verstrekking, evenals de eigen verwerking door AIVD of MIVD van de desbetreffende gegevens, strikt doelgebonden is: namelijk om vast te stellen op welke gegevensstromen een verzoek om toestemming als bedoeld in artikel 48, tweede lid, Wiv 2017 betrekking dient te hebben. Dit vaststellen bestaat uit technisch onderzoek van de verworven bulkdata. In de meeste gevallen zullen de Nederlandse diensten dit onderzoek prima zelf kunnen doen, maar er zijn situaties denkbaar waarin een buitenlandse dienst beschikt over kennis of technische mogelijkheden waar Nederland (nog) niet over beschikt. Hierbij worden de voor dat technisch onderzoek benodigde gegevens aan de desbetreffende buitenlandse dienst verstrekt. Uitsluitend voor dat – bij de verstrekking als voorwaarde te stellen – doel worden de gegevens aan de buitenlandse dienst worden verstrekt en voorts wordt daarbij het expliciete verbod gesteld om deze gegevens te gebruiken voor inlichtingendoeleinden. Via het bij amendement ingevoegde artikel 6, zevende lid, wordt de doelbinding voor de verstrekking aan een buitenlandse dienst ook wettelijk verankerd.

De leden van de ChristenUnie-fractie stellen dat zowel de commissie Jones-Bos[30] als de Raad van State hebben aanbevolen of geadviseerd om een bewaartermijn in de wet op te nemen, en dat de Raad van State zelfs adviseerde om een fatale termijn op te nemen.[31] Deze leden zien een dergelijke termijn echter in het wetsvoorstel niet terug, anders dan de in het voorgestelde artikel 14b en de verder opgenomen 'eindtermijn' die bij herhaling te verlengen is. De leden vragen hoe dit zich verhoudt tot de genoemde adviezen, die mede lijken te zijn ingegeven door staande jurisprudentie van het Europees Hof voor de Rechten van de Mens. Wij antwoorden de leden graag als volgt

De Raad van State adviseerde te voorzien in een wettelijke eindtermijn met daarbij tevens een nauwkeurig begrensde mogelijkheid om daarvan bij wijze van uitzondering af te kunnen wijken indien dringende redenen met het oog op de nationale veiligheid dat strikt noodzakelijk maken. Daaraan is gevolg gegeven door in artikel 14b een eindtermijn op te nemen waarmee in afwijking van het bepaalde in artikel 27, eerste en derde lid, Wiv 2017 een door de diensten verworven bulkdataset die is verworven met een bijzondere bevoegdheid, niet zijnde de bevoegdheid ex artikel 48 Wiv 2017, anderhalf jaar kan worden gebruikt. Tevens is in navolging van het advies van de Raad van State voorzien in een mogelijkheid om hiervan af te wijken wanneer sprake is van dringende redenen met het oog op de nationale veiligheid. Hiermee is aangesloten bij het door de Afdeling geformuleerde criterium voor de door haar mogelijk geachte uitzondering op een eindtermijn en wordt recht gedaan aan de aard van iedere afzonderlijke bulkdataset en het gebruik daarvan in de inlichtingenpraktijk. Voor wat betreft de jurisprudentie van het EHRM wordt opgemerkt dat het Hof in een concrete zaak het stelsel als geheel in aanmerking neemt en daarbij beziet of het stelsel voldoende waarborgen bevat die in hun onderlinge samenhang adequate en effectieve garanties bieden tegen willekeur en het risico van misbruik. Hoewel het Hof belang hecht aan een zo kort mogelijke bewaartermijn, stelt het Hof niet de eis dat altijd sprake moet zijn van een vaste of fatale termijn. De regering is van oordeel dat de voorgestelde regeling voldoet aan de vereisten van de jurisprudentie van het EHRM.

De fractieleden van de PvdD wijzen erop dat de Afdeling advisering van de Raad van State stelt dat bulkdata die worden verkregen door middel van de verkennende bevoegdheid, zich niet lenen voor uitwisseling met buitenlandse diensten. "Het betreft immers gegevens die ook de Nederlandse inlichtingendiensten binnen de eigen rechtsorde niet verder mogen verwerken"[32], aldus de Afdeling advisering. De fractieleden vragen of die laatste opmerking klopt. Wij reageren hierop graag als volgt.

De opmerking van de Afdeling advisering van de Raad van State betreft artikel 6, zesde lid, van het wetsvoorstel, waarin staat dat de gegevens die middels verkenning ten behoeve van OOG-interceptie zijn verkregen niet worden verwerkt voor andere doeleinden dan om vast te stellen op welke gegevensstromen een verzoek om toestemming als bedoeld in artikel 48, tweede lid, van de

[29] *Kamerstukken II 2022/2023, 36 263, nr. 4, p. 23.*
[30] *Kamerstukken II 2020/21, 34 588, nr. 88, bijlage Evaluatie 2020. Wet op de inlichtingen- en veiligheidsdiensten 2017.*
[31] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 27-28.*
[32] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 22.*

Wiv 2017 betrekking dient te hebben. Voor zover de Afdeling met de woorden "verder verwerken" heeft bedoeld de verdere verwerking voor een ander doel dan dat gesteld in artikel 6, eerste lid, van het wetsvoorstel, dan klopt haar opmerking ter zake. Nu de eventuele verstrekking aan een buitenlandse dienst eenzelfde beperking kent en als voorwaarde bij de verstrekking zal worden gesteld, zien wij geen reden waarom een dergelijke verstrekking niet mogelijk zou zijn.

De leden van de PvdD-fractie hebben ervan kennisgenomen dat de regering stelt dat met betrekking tot de verstrekking aan buitenlandse diensten: "Deze verstrekking vindt plaats met het expliciete verbod deze gegevens te gebruiken voor inlichtingendoeleinden."[33] Deze fractieleden vragen uit welke voorschriften volgt dat het bedoelde 'verbod' juridische verplichtingen in het leven roept voor die buitenlandse dienst en hoe dat 'verbod' wordt gehandhaafd. Wij beantwoorden deze vragen graag als volgt.

De wijze waarop een ander land omgaat met de ontvangen gegevens valt onder de rechtsmacht van het betreffende land, waarvoor de eigen toezichthouder bevoegd is. De naleving van de voorwaarde zoals genoemd in deze vraag maar ook het verbod op delen met andere partijen (de derde partij regel), berust op de (ongeschreven) vertrouwensregel die in de samenwerking tussen inlichtingen- en veiligheidsdiensten geldt. Indien geconstateerd wordt dat een dienst van een ander land zich niet aan de gestelde voorwaarde(n) houdt, zal de samenwerkingsrelatie met die dienst opnieuw worden gewogen. Afhankelijk van de uitkomst wordt besloten of de samenwerkingsrelatie wordt voortgezet en, zo ja, wat dan de aard en de intensiteit van die relatie – mede in het licht van de geconstateerde vertrouwensbreuk – moet zijn.

De fractieleden van de PvdD vragen welke persoonsgegevens de gegevensstroom die bij toepassing van het voorgestelde artikel 6 onder het bereik van de dienst komt, kan omvatten. Specifiek vragen zij of dat alle 'verkeer' is dat onderschept is en of dat e-mails, inloghandelingen, gegevens over betalingen en bankoverschrijvingen kunnen zijn. Wij beantwoorden deze vragen als volgt.

De persoonsgegevens die in de gegevensstromen kunnen zitten zijn divers en kunnen e-mails, inloghandelingen en betalingsverkeer bevatten. Belangrijk is dat de gegevensstromen verworven met OOG-interceptie geen volledig beeld geven van de digitale activiteiten van een persoon of organisatie; dat geldt dus ook voor de interceptie in het kader van de verkenningsbevoegdheid. De gegevensstromen verworven met OOG-interceptie bevatten – door de werking van het internet - slechts gedeelten (fragmenten) van de communicatie van personen en organisaties in het digitale domein. Gegevens verkregen uit de bevoegdheid tot verkenning op de kabel zijn overigens uitgesloten van gebruik voor het inlichtingenproces.

De fractieleden van de PvdD wijzen op de constatering van de Afdeling advisering van de Raad van State dat de gegevensstromen "verschillende typen diensten inhouden, zoals video-on-demand-platformen (zoals Netflix), videoplatformdiensten (zoals Youtube), en sociale media (zoals Facebook)."[34] De fractieleden hebben kennis genomen van de stelling van de regering dat het niet mogelijk is om op voorhand en categorisch gegevensstromen uit te sluiten, omdat "is gebleken dat actoren gebruik maken van veel verschillende protocollen en technieken om hun offensieve cyberprogramma uit te voeren en hun activiteiten te verhullen."[35] De leden vragen hoe aannemelijk het is dat actoren video-on-demand-platformen (zoals Netflix) of videoplatformdiensten (zoals YouTube) kunnen gebruiken om een offensief cyberprogramma tegen Nederland of Nederlandse belangen in te zetten. De leden vragen de regering dat met praktijkvoorbeelden toe te lichten. Wij reageren hierop graag als volgt.

De Afdeling merkt inderdaad terecht op dat de gegevensstromen verschillende typen diensten inhouden, waaronder video-on-demand-platformen. De Afdeling schrijft ook het begrijpelijk te vinden dat het niet altijd mogelijk zal zijn categorisch gegevensstromen uit te sluiten. De Afdeling vraagt zich af of het niet mogelijk is te differentiëren tussen de verschillende type diensten, door een afweging tussen het recht op de bescherming van de persoonlijke levenssfeer en operationele belangen. De regering heeft daarop gereageerd met de constatering dat gegevensstromen

[33] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 23.*
[34] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 24.*
[35] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 25.*

dynamisch zijn en filters die gericht zijn op het filteren van gegevens daarop moeten worden aangepast. Deze dynamiek van gegevensstromen is inherent aan technologische ontwikkelingen. In de toelichting op de Tijdelijke wet staat dat om het middel effectief ten behoeve van een onderzoek in te zetten, het dus niet mogelijk is om gegevensstromen enkel op basis van technische eigenschappen, zoals de oorsprong of bestemming van communicatie of de soort (streaming)dienst die wordt aangeboden, uit te sluiten.[36] Het is van belang dat de diensten per geval een afweging kunnen maken welke gegevens gefilterd moeten worden en welke gegevens doorgelaten kunnen worden. Deze verduidelijking in de Tijdelijke wet wordt nodig geacht om duidelijkheid te scheppen over de vernietiging van niet-relevante gegevens. Reeds bij het wetgevingsproces van de Wiv 2017 was beoogd duidelijk te maken dat niet-relevante gegevens niet verder worden verwerkt, dit in het belang van de bescherming van de persoonlijke levenssfeer. Dit betekent echter niet dat indien de diensten niet in staat zijn om dit soort gegevensweg te filteren de diensten helemaal niet over mogen gaan tot de uitvoering van OOG-interceptie. Dit betekent wel dat de diensten op het eerst mogelijke moment evident niet-relevante gegevens dienen te vernietigen. Beoogd was ook om aan te geven dat verkeer waarvan aan de buitenkant op het eerste gezicht van de gegevens de evidente niet-relevantie is vast te stellen niet wordt geïntercepteerd, zoals verkeer van populaire streamings- en downloaddiensten als Netflix, Spotify en BitTorrent. In de wetsgeschiedenis is ook benadrukt dat datareductie plaatsvindt binnen het gehele proces van OOG-interceptie.[37] Omdat de diensten nu (beperkte) praktijkervaring hebben opgedaan met OOG-interceptie en in het belang van voorzienbaarheid wordt opgemerkt dat het op voorhand categorisch uitsluiten van bepaalde gegevensstromen de effectiviteit van OOG-interceptie kan beperken. Vanzelfsprekend zijn ook de technische beperkingen relevant bij de inspanningsverplichting voor het vernietigen van evident niet-relevante gegevens. Niet-relevante gegevens worden zo veel mogelijk vernietigd door een dynamische toepassing van filtering. In de praktijk zal dit betekenen dat in het belang van volumereductie streamings- en downloadverkeer wordt vernietigd, maar waar noodzakelijk voor het beantwoorden van onderzoeksvragen er opslag van verkeer kan plaatsvinden. De afdeling toezicht van de CTIVD houdt toezicht op de gehele uitvoering van OOG-interceptie, waaronder de toegepaste filtering. Het belang van dynamische filters wordt verder onderbouwd met het feit dat statelijke actoren die een offensief cyberprogramma uitvoeren het grootste belang hebben om hun activiteiten te verhullen. Het is aannemelijk dat statelijke actoren hun cyberaanvallen verhullen als legitiem netwerkverkeer, zoals binnenlands verkeer of als verkeer van streamings- en downloaddiensten dan wel sociale media. Daarnaast onderzoeken de diensten niet alleen de cyberaanvallen van statelijke actoren met een offensief cyberprogramma, maar ook de activiteiten van personen en organisaties die uitvoering geven aan de geopolitieke strategie van een land, waaronder een offensief cyberprogramma. Hiervoor kunnen die statelijke actoren ook legitieme platforms gebruiken. Juist als categorisch gegevensstromen van interceptie of verdere verwerking worden uitgesloten, kan dit voor statelijke actoren aanleiding geven hun verkeer juist via - of vergelijkbaar met - een legitiem platform uit te wisselen. In de memorie van toelichting op het wetsvoorstel wordt als voorbeeld genoemd dat de Russische militaire inlichtingendienst op online mediaplatforms desinformatie heeft verspreid over het neerhalen van vlucht MH17 en hiermee het beeld hebben proberen te kleuren dat mensen hebben van het neerhalen van vlucht MH17 boven Oekraïne in 2014.

De leden van de PvdD-fractie verwijzen naar de brief van de TIB van 7 december 2023, waarin de TIB stelt dat er door de minister is toegezegd dat er geen interceptie zal plaatsvinden in het zogeheten Nederland-Nederland-verkeer, tenzij voor *cyber defence*.[38] De leden vragen of die stelling juist is, of dit ook geldt voor het gebruik van bevoegdheden waarop het onderhavige wetsvoorstel betrekking heeft en zo nee, of dat dan in strijd is met de toezegging. Wij beantwoorden deze vragen als volgt.

De bedoelde stelling is onjuist. In de kamerbrief van april 2018[39] is door de ministers aangegeven dat het vrijwel uitgesloten is dat OOG-interceptie op de kabel de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek in het kader van cyber defence, omdat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en OOG-interceptie op de kabel noodzakelijk kan zijn om dit

[36] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 24.*
[37] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 24.*
[38] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 2.
[39] *Kamerstukken II 2017/18, 34 588, nr. 70, p. 3*.

te ontdekken). De CTIVD geeft in haar rapport aan dat de precieze strekking van de gedane toezegging niet eenduidig is, maar dat geconcludeerd kan worden dat het zwaartepunt van de toezegging gericht is op onderzoek naar gegevens met oorsprong en bestemming Nederland en niet op de interceptie van gegevens met oorsprong en bestemming Nederland.[40] Interceptie van gegevens met oorsprong en bestemming Nederland is door de werking van het internet op voorhand niet uit te sluiten. De waarborg die voortvloeit uit de gedane toezegging door de ministers dient op een manier gelezen te worden dat het vrijwel uitgesloten is dat de diensten OOG-interceptie zullen inzetten voor inlichtingenonderzoeken naar gegevens met oorsprong en bestemming Nederland met uitzondering van de onderzoeken in het kader van cyber defence.

De fractieleden van de PvdD verwijzen nogmaals naar de brief van de TIB van 7 december 2023, waarin de TIB op bladzijde 6 bovenaan stelt: "De Tijdelijke wet bevat echter geen fatale bewaartermijn."[41] De fractieleden vragen of die constatering juist is, zo nee, uit welk voorschrift die fatale bewaartermijn blijkt, en zo ja, of het aannemelijk is dat het Europees Hof voor de Rechten van de Mens het ontbreken van een fatale bewaartermijn onrechtmatig zal achten en als de regering dat laatste niet aannemelijk acht, op grond van welke rechtspraak de regering dan tot dat oordeel komt. Wij reageren hierop graag als volgt.

De Tijdelijke wet bevat geen fatale bewaartermijn in de zin dat voor alle bulkdatasets een vooraf vastgesteld moment is waarop deze vernietigd moeten worden. Zoals hiervoor aangegeven in reactie op vragen van de leden van de fractie van de ChristenUnie, voorziet het wetsvoorstel in een eindtermijn met de mogelijkheid voor de verantwoordelijke minister om een nieuwe eindtermijn vast te stellen wanneer sprake is van dringende redenen met het oog op de nationale veiligheid. Hiermee wordt enerzijds tot uitdrukking gebracht dat in beginsel dient te worden uitgegaan van een maximale termijn van anderhalf jaar voor het gebruik van een bulkdataset en anderzijds wordt aangesloten bij de door de Raad van State mogelijk geachte uitzondering. Hierbij geldt tevens dat, indien de minister tot het oordeel komt dat er (inderdaad) dringende redenen met het oog op de nationale veiligheid aanwezig zijn die het noodzakelijk maken om een nieuwe eindtermijn te geven voor het gebruik van een bulkdataset en hij een nieuwe eindtermijn vaststelt, de afdeling toezicht van de CTIVD hierop bindend toezicht kan uitoefenen. De vraag in hoeverre het aannemelijk is dat het EHRM het ontbreken van een fatale bewaartermijn onrechtmatig zal achten, kan niet met zekerheid worden beantwoord. Het EHRM doet immers uitspraak in een concreet aan het Hof voorgelegde casus waarbij het Hof kijkt naar het hele systeem van waarborgen en de effectiviteit van die waarborgen in onderlinge samenhang. Hoewel het Hof belang hecht aan een zo kort mogelijke bewaartermijn, stelt het Hof overigens niet de eis dat altijd sprake moet zijn van een vaste of fatale termijn.

De fractieleden van Volt stellen dat de MIVD en de AIVD vaak gegevens delen met buitenlandse geheime diensten, zoals de Duitse, Britse en de Amerikaanse. Deze leden stellen dat de Nederlandse diensten na overdracht van de data geen zicht meer hebben op wat er met de data gebeurt en hoe deze bewaard worden. De leden vragen in hoeverre de regering kan garanderen dat verzamelde data in Nederland wel wordt getoetst en eventueel vernietigd wanneer deze aan buitenlandse diensten zijn overgedragen en hun bewaartermijn hebben bereikt. Ook vragen deze leden in hoeverre er verschillen zijn in het toezicht dat Nederland kan houden op uitgewisselde bulkdata met andere diensten binnen en buiten Europa. Wij beantwoorden deze vragen als volgt.

De AIVD en MIVD moeten op grond van artikel 88 Wiv 2017 wegingsnotities opstellen voor samenwerkingsrelaties. In een wegingsnotitie wordt een weging gemaakt van onder andere de eerbiediging van de mensenrechten en democratische inbedding. In een wegingsnotitie kunnen aanvullende waarborgen opgenomen worden als er verhoogde risico's bestaan in de samenwerking, bijvoorbeeld indien het land niet als een democratische rechtsstaat functioneert, er geen toezicht is op een dienst of dat het land bekend staat om de schending van mensenrechten. Een aanvullende waarborg kan dan zijn dat geen ongeëvalueerde gegevens bepaalde andere gegevens worden gedeeld. Daarbij mogen buitenlandse diensten de door de AIVD en MIVD verstrekte gegevens niet gebruiken ten behoeve van handelingen die in strijd zijn met internationaal recht, ze mogen deze

[40] Toezichtsrapport 75 over de inzet van kabelinterceptie door de AIVD en de MIVD – De Snaphotfase (2022), p. 41.
[41] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 6.

gegevens niet aan derden verstrekken (derde partij-regel) en er wordt met betrekking tot data die met het verkennend onderzoek voor OOG wordt verkregen een verbod op gebruik voor inlichtingendoeleinden gesteld.

Verder wordt opgemerkt dat buitenlandse diensten, net als de AIVD en MIVD, een eigen wettelijk kader en een eigen toezichtstelsel hebben. Het eventueel ontbreken daarvan wordt betrokken bij het opstellen van een wegingsnotitie. De wegingsnotitie vormt de basis voor de eventuele samenwerking en het uitwisselen van gegevens.

Indien gegevens onder bepaalde beperkingen of voorwaarden aan een buitenlandse dienst worden verstrekt, dan dient de buitenlandse dienst zich daaraan in deze concrete samenwerking te houden. De naleving van deze voorwaarden berust op de (ongeschreven) vertrouwensregel die in de samenwerking tussen inlichtingen- en veiligheidsdiensten geldt. Indien geconstateerd wordt dat een dienst van een ander land zich niet aan de gestelde voorwaarden houdt, zal de samenwerkingsrelatie met die dienst opnieuw worden gewogen. Afhankelijk van de uitkomst wordt besloten of de samenwerkingsrelatie moet worden voortgezet en, zo ja, wat dan de aard en de intensiteit van die relatie – mede in het licht van de geconstateerde vertrouwensbreuk – moet zijn.

Dat geldt evenzeer voor de omgekeerde situatie: ingeval gegevens worden verstrekt aan de AIVD of MIVD door een buitenlandse dienst zal de toezichthouder uit dat andere land evenmin in staat zijn om het gebruik van de gegevens door de AIVD en MIVD toezicht te houden. Er ontbreekt immers rechtsmacht.

4. Toets en toezicht en de mogelijkheid van beroep op de Afdeling bestuursrechtspraak van de Raad van State

Met de tijdelijke wet wordt met het voorgestelde artikel 6 'zo gericht als mogelijk' buiten werking gesteld bij het verkennen van de kabels, zo merken de fractieleden van GroenLinks-PvdA op. Dit gaat om het verkennen van kabels om te kijken of er interessante dingen op zitten om eventueel op een later moment 'af te luisteren' op grond van artikel 48 van de Wiv 2017. Om dit verkennen uit te voeren, wordt er een 'snapshot' van de hele kabel gemaakt en opgeslagen ('kabelinterceptie'). Door de manier waarop artikel 6 is geschreven, is het voor de fractieleden van GroenLinks-PvdA moeilijk voorstelbaar dat de TIB een verzoek ooit af kan wijzen. Er staat namelijk:

"*De diensten zijn bevoegd met het oog op toepassing van de bevoegdheid, bedoeld in artikel 48, eerste lid, van de Wiv 2017, tot het met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk ongeacht waar een en ander zich bevindt, met het uitsluitende doel vast te stellen op welke gegevensstromen een verzoek om toestemming als bedoeld in artikel 48, tweede lid, van die wet, betrekking dient te hebben.*"
Voornoemde leden wijzen hierbij met nadruk op de woorden "*met het uitsluitende doel*". En in het vierde lid van het voorgestelde artikel 6 staat: "*Artikel 26, vijfde lid, van de Wiv 2017 blijft buiten toepassing.*"

De fractieleden van GroenLinks-PvdA vragen of zij het goed begrijpen dat 'verkennen' enkel en alleen gerechtvaardigd wordt door de behoefte om later misschien artikel 48 van de Wiv 2017 in te zetten. Deze fractieleden vragen of de TIB dus vooraf alleen kan toetsen op de aan- of afwezigheid van de melding van de diensten dat ze artikel 48 van de Wiv 2017 op enig moment in willen zetten, De fractieleden vragen een toelichting van de regering. Zij menen dat hiermee feitelijk elk verkenningsverzoek rechtmatig is en vragen de regering voorbeelden te noemen waarbij onder de tijdelijke wet de TIB een niet-rechtmatigheidsoordeel zou kunnen geven. Wij beantwoorden deze vragen als volgt.

Het is juist dat de verkenningsbevoegdheid van artikel 6 uitsluitend ten dienste staat voor het eventueel kunnen toepassen van de bevoegdheid tot OOG-interceptie ex artikel 48 Wiv 2017. Elke vorm van gegevensverwerking moet voldoen aan de eisen van noodzaak, proportionaliteit en subsidiariteit. Die eisen gelden dus ook bij de toepassing van de bijzondere bevoegdheid in artikel 6 van het wetsvoorstel. Voor de toepassing van deze bevoegdheid is toestemming van de minister

vereist, die vervolgens onderworpen is aan de voorafgaande bindende toets door de TIB. Het verzoek om toestemming moet voorts voldoen aan de eisen van artikel 29, tweede lid, Wiv 2017, waarbij dus ook het doel en de reikwijdte van de bevoegdheidsuitoefening moeten worden gemotiveerd. Dat betekent dat ingeval van toepassing van artikel 6 de toestemming per definitie beperkt is tot het in artikel 6 geformuleerde doel. De TIB kan die toestemming op reguliere wijze aan de genoemde eisen die zijn gesteld aan gegevensverwerking toetsen. Het is niet zo dat elke door de minister aan de diensten verleende toestemming tot toepassing van artikel 6 op voorhand tot een rechtmatigheidsoordeel zou leiden bij de TIB.

De fractieleden van GroenLinks-PvdA hebben ook vragen over het toezicht tijdens en achteraf door de CTIVD. De fractieleden menen dat de CTIVD kan toetsen op de aan- of afwezigheid van de melding van de diensten dat ze artikel 48 van de Wiv 2017 op enig moment in willen zetten, en dat indien dit zo is, dat dan het verzoek rechtmatig is. Zij menen dat hiermee feitelijk elke verkenning rechtmatig is. De fractieleden vragen of deze lezing correct is, en zo niet, dan ontvangen voornoemde fractieleden graag een toelichting. Wij reageren hierop graag als volgt.

De melding van de TIB aan de afdeling toezicht van de CTIVD dat de TIB een verleende toestemming voor toepassing van artikel 6 rechtmatig heeft verklaard, strekt ertoe om de afdeling toezicht in staat te stellen om daarop vervolgens adequaat toezicht te houden. De CTIVD toetst echter niet of een verleende toestemming voor de inzet van de verkennende bevoegdheid voor OOG-interceptie rechtmatig is, immers deze toets (ex ante) is door de wetgever aan de TIB opgedragen. Wel ziet de afdeling toezicht van de CTIVD toe op de rechtmatige uitvoering van de bevoegdheid.

De fractieleden van GroenLinks-PvdA vragen of de CTIVD dan alleen in zou kunnen grijpen als blijkt dat men de data direct inzet voor inlichtingendoeleinden zonder de daadwerkelijke toestemming (artikel 48 van de Wiv 2017) daarvoor aan te vragen. De leden vragen of deze stelling correct is, of dat er andere voorbeelden te noemen zijn waarbij ingrijpen mogelijk is. De fractieleden vragen de regering meerdere voorbeelden te noemen en hierbij duidelijk aan te geven hoe dat ingrijpen eruit kan zien. Wij beantwoorden deze vragen als volgt.

De CTIVD houdt regulier toezicht op de uitvoering van de bevoegdheid als bedoeld in artikel 6 en heeft hier geen bindende bevoegdheden. Het gebruiken van met deze bevoegdheid verworven gegevens voor inlichtingendoeleinden is in strijd met het in artikel 6 bepaalde doel en dus onrechtmatig. Tijdens de uitvoering van de verkennende bevoegdheid voor OOG-interceptie kan de afdeling toezicht van de CTIVD niet alleen toezien of het gebruik van de gegevens in overeenstemming is met het doel, maar ook bijvoorbeeld of de gegevens binnen de wettelijk bepaalde bewaartermijn zijn vernietigd. Daarnaast kan de CTIVD toezicht houden op het voldoen aan de eisen van noodzaak, proportionaliteit en subsidiariteit tijdens de uitoefening van de verkennende bevoegdheid.

De fractieleden van GroenLinks-PvdA verwijzen naar het voorgestelde artikel 7, dat twee aspecten noemt die betrokken moeten worden bij de proportionaliteitstoets van de TIB. In de Tweede Kamer is een amendement[42] aangenomen waardoor de woorden "met name" in dit artikel zijn komen te vervallen. De TIB leest het amendement zo dat "betoogd [is] om te verduidelijken dat deze twee elementen betrokken moeten worden bij de proportionaliteitstoets, *naast andere* elementen die hierin moeten worden betrokken, waaronder de feitelijke inbreuk die het voorgestelde middel heeft op de grondrechten van burgers."[43] Deze leden vragen of de regering de interpretatie van het amendement van de TIB deelt, of dit amendement volgens de regering te zien is als een beperktere vorm van de proportionaliteitstoets, zo nee, waarom niet en zo ja, hoe zich dit verhoudt tot Europese wet- en regelgeving en jurisprudentie. Ons antwoord hierop luidt als volgt.

[42] *Kamerstukken II 2023/24, 36 263, nr. 27.*
[43] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 8; het cursiveren is gedaan door de fractieleden van GroenLinks-PvdA.

Zoals aangegeven in de brief aan de voorzitter van de Tweede Kamer van 24 oktober 2023, waarin ingegaan wordt op de appreciatie van het desbetreffende amendement door de regering[44], geeft artikel 7 van het wetsvoorstel, ook na aanname van het amendement van de leden Bisschop (SGP) en Van der Graaf (ChristenUnie), richting aan de proportionaliteits- en gerichtheidstoets binnen de uitvoering van OOG-interceptie in de gehele keten. Door de woorden 'met name' te laten vervallen wordt naar ons oordeel sterker tot uitdrukking gebracht dat specifiek deze twee aspecten, namelijk een omschrijving van de gegevensstromen en een omschrijving van de reductie van gegevens, in die toets betrokken worden. Er is voor deze criteria gekozen aangezien hiermee inzage kan worden gegeven in de mate van gerichtheid van de verwerving en de (direct daaropvolgende) verwerking (en dus reductie) van de gegevens, en daarmee ook de proportionaliteit van de inzet zorgvuldig kan worden getoetst. Een omschrijving van de gegevensstromen geeft immers een zekere mate van inzicht in de gegevens die verworven wordt, bijvoorbeeld door aan te geven op welke klantkanalen geïntercepteerd zal worden. De wijze waarop de reductie van gegevens plaatsvindt geeft daarnaast inzicht in welke gegevens door middel van filtering wel en niet verder worden verwerkt en in het inlichtingenproces terecht kunnen komen. Daarbij dient het gehele systeem van handelingen, van interceptie van gegevens tot aan verdere verwerking van gegevens in inlichtingenproducten, en waarborgen, van functiescheidingen tot de aanwezigheid van een efficiënte klachtprocedure, betrokken te worden in de toetsing van OOG-interceptie. In dit verband kan ook verwezen worden naar de hiervoor gemaakte opmerkingen over de graduele benadering bij OOG-interceptie in reactie op de door de fractie van GroenLinks-PvdA geschetste stappen voor kabelinterceptie. Naar ons oordeel zijn dit de meest fundamentele aspecten voor de proportionaliteitstoets bij de inzet van OOG-interceptie. Deze aspecten bieden, binnen de kaders van wat voorafgaand aan daadwerkelijke inzet bekend is, het meest concrete inzicht in de mate en de omvang van de inbreuk op de persoonlijke levenssfeer, afgezet tegen de belangen van de nationale veiligheid.

Wellicht ten overvloede wordt opgemerkt dat de proportionaliteitstoets op een middel als OOG-interceptie niet te vergelijken is met een proportionaliteitstoets bij een middel voor gerichte interceptie. Dit komt omdat OOG-interceptie een ander doel dient, namelijk het onderkennen van ongekende dreiging en het vergroten van kennis over reeds gekende dreiging. OOG-interceptie richt zich, anders dan gerichte interceptie, op brede gegevensstromen die een veelheid van gebruikers betreft en daarmee gegevens in bulk verwerft. Bij OOG-interceptie wordt het overgrote deel van de geïntercepteerde gegevens niet verder verwerkt en zullen de diensten ook geen analyse uitvoeren op een zeer groot gedeelte van de geïntercepteerde gegevensstromen. Bij gerichte interceptie – gerelateerd aan een specifiek persoon, organisatie of technisch kenmerk – zullen over het algemeen alle op deze wijze verworven gegevens verder worden verwerkt.

Dat laat onverlet dat voldaan dient te worden aan de uit het EVRM en de uit jurisprudentie daarop voortvloeiende eisen, zoals de toets op subsidiariteit. De TIB kan daaraan toetsen. Volgens de regering is het amendement dan ook niet te zien als een beperking van de proportionaliteitstoets maar juist een aansluiting bij de uitkomst van de laatste Europese rechtspraak op dit vlak.

De fractieleden van GroenLinks-PvdA stellen dat het aannemelijk is dat bij kabelinterceptie ook persoonsgegevens zoals iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven, worden 'verkend'. De leden wijzen erop dat de TIB stelt dat zij, conform Europese jurisprudentie, een volledige rechtmatigheidstoets moet uitvoeren. Daarbij hoort "een volle toetsing op de gronden van noodzaak, proportionaliteit en subsidiariteit."[45] Een proportionaliteitstoets kenmerkt zich daarbij tussen een afweging van de noodzaak van het voorgestelde middel en de inbreuk op grondrechten die het middel met zich brengt. De in het wetsvoorstel voorgestelde twee elementen bevatten nu alleen een omschrijving van de gegevensstroom die geïntercepteerd moet worden, en de voorgestelde latere reductie van gegevensstromen. De fractieleden vragen of de regering de bovengenoemde stelling van de TIB deelt. Deze vraag komt naar ons oordeel materieel overeen met de vorige vraag van deze leden, zodat we graag naar ons antwoord daarop verwijzen.

De leden van de GroenLinks-PvdA-fractie vragen hoe deze ongerichte dataverzameling zich verhoudt tot specifiek het medisch beroepsgeheim. Wij beantwoorden deze vraag graag als volgt.

---

[44] *Kamerstukken II 2023/24, 36 263, nr. 33.*

[45] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 8.

De regering acht het van belang om ter voorkoming van misverstanden duidelijk onderscheid te maken tussen enerzijds het medisch beroepsgeheim en anderzijds de bescherming van bijzondere persoonsgegevens. Het medisch beroepsgeheim is een zwijgplicht voor medisch hulpverleners om gegevens over hun patiënten niet zonder toestemming van hun patiënt te delen met anderen. Alleen medisch personeel dat vanuit hun beroep over deze gegevens beschikt, is gebonden aan het medisch beroepsgeheim.

Bij de ongerichte verzameling van gegevens, dat bij verkenning ten behoeve van OOG-interceptie aan de orde is, is het niet uitgesloten dat daarin ook gegevens voor kunnen komen die betrekking hebben op iemands gezondheidssituatie. Dat is echter op voorhand niet bekend. Deze en andere gegevens mogen echter niet voor inlichtingendoeleinden worden gebruikt. Dat zou immers in strijd zijn met de wet en derhalve onrechtmatig (artikel 19, derde lid, van de Wiv 2017 bepaalt dat de verwerking van gegevens wegens iemands gezondheid niet is toegestaan). Dergelijke gegevens mogen slechts worden verwerkt in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is (artikel 19, vierde lid). Van een dergelijke situatie zal gelet op het doel van de verkenning en het toegestane gebruik van de gegevens geen sprake kunnen zijn.

De fractieleden van GroenLinks-PvdA melden dat de Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst stelt dat de diensten nooit willekeurig medische gegevens zullen verzamelen.[46] Deze fractieleden menen echter dat verkenning/kabelinterceptie juist volstrekt willekeurig is. Graag ontvangen de fractieleden van GroenLinks-PvdA een reactie van de regering. Ook vragen de leden wat de handelwijze is als de diensten vaststellen dat er medische gegevens voorkomen in de verzamelde data. Specifiek willen de fractieleden weten wat er dan wel/niet met deze data gebeurt en of de betreffende patiënt/hulpverlener hierover wordt geïnformeerd en zo nee, waarom niet. Wij reageren hierop graag als volgt.

Zoals hiervoor in antwoord op de vraag van deze leden is aangegeven is in artikel 19, derde lid, van de Wiv 2017 bepaald dat de verwerking van gegevens wegens iemands gezondheid niet is toegestaan tenzij deze gegevens in aanvulling op andere gegevens worden verwerkt en deze verwerking onvermijdelijk is. Uitsluitend in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is kunnen dergelijke gegevens door de diensten worden verwerkt (artikel 19, vierde lid). Indien bij de verwerking van de gegevens wordt vastgesteld dat van dergelijke gegevens sprake is, dan zullen die overeenkomstig deze bepaling moeten worden verwerkt, hetgeen – behoudens de het bepaalde in het vierde lid – dienen te worden vernietigd.[47] Op de toepassing van deze regeling ziet de afdeling toezicht van de CTIVD toe. De betreffende patiënt/hulpverlener wordt hierover niet geïnformeerd. Dit is veelal onmogelijk omdat aanvullende gegevens zouden moeten worden verkregen om een persoon te identificeren.

Overigens wordt opgemerkt dat voor de inwerkingtreding van de Wiv 2017 door de AIVD met vertegenwoordigers van de KNMG is gesproken over de waarborgen die in de Wiv 2017 zijn opgenomen inzake het medisch beroepsgeheim. Naar aanleiding daarvan zijn artikelen gepubliceerd op de websites van zowel de AIVD als de KNMG.

De fractieleden van GroenLinks-PvdA vragen hoe de ongerichte dataverzameling zich verhoudt tot specifiek de bronbescherming van journalisten, wat de handelwijze is als de diensten vaststellen dat een journalist voorkomt in de verzamelde data, wat er dan wel/niet met deze data gebeurt, of de betreffende journalist hierover wordt geïnformeerd, en zo nee, waarom niet. Wij reageren hierop graag als volgt.

---

[46] https://www.knmg.nl/actueel/nieuws/nieuwsbericht/aivd-verzekert-waarborgen-medische-gegevens-in-de-wiv.

[47] In artikel 6 van de Beleidsregels Wiv 2017 staat ook dat indien de diensten bij de verwerking van gegevens stuiten op gegevens betreffende de gezondheid van een persoon en de verwerking niet voldoet aan de in artikel 19, vierde lid, van de wet neergelegde eis, deze terstond worden vernietigd.

Met betrekking tot de interceptie van communicatie (gericht als in bulk), de selectie van bulkdata verkregen via interceptie als bij de inzet van bevoegdheden jegens journalisten in relatie tot bronbescherming, voldoet de Wiv 2017 alsmede de in onderhavig wetsvoorstel opgenomen voorstellen aan de eisen die ingevolge artikel 10 EVRM en de jurisprudentie van het EHRM worden gesteld aan journalistieke bronbescherming. Bij de inzet van bijzondere bevoegdheden jegens journalisten gericht op het achterhalen van hun bronnen is de toestemming vereist van de rechtbank Den Haag. Gelet op de aard van de bevoegdheid van OOG-interceptie – te weten interceptie in bulk - zal inzet daarvan *gericht* op het achterhalen van een bron van journalist niet aan de orde kunnen zijn.

De fractieleden van GroenLinks-PvdA stellen dat onder de huidige wet het gebruik van AI alleen mag met expliciete toestemming vooraf. Onder de tijdelijke wet onderscheiden deze leden twee soorten bulkafluisteren: 'verkennen' (voorgestelde artikel 6) en 'regulier bulk afluisteren' (artikel 48 van de Wiv 2017). Bij het 'verkennen' zijn er volgens de leden geen beperkingen (geen toetsing vooraf en er is geen plan noodzakelijk), behalve met wie de opgedane kennis gedeeld mag worden. Hierop vindt geen bindend toezicht plaats. Daarnaast, als er eenmaal zo'n echte afluistervergunning is (voornoemd artikel 48), dan mag, zo stellen de leden, onder de huidige wet alleen met toetsing vooraf de data aan AI ('geautomatiseerde data-analyse') gevoerd worden. In de tijdelijke wet vervalt de noodzaak hier toestemming bij de TIB voor te vragen: "In afwijking van het bepaalde in artikel 36, eerste lid, van de Wiv 2017 wordt een door Onze betrokken minister verleende toestemming als bedoeld in *artikel 50, vierde lid*, van die wet *niet* voor toetsing voorgelegd aan de toetsingscommissie."[48] Door de nieuwe wet kan er bij de echte kabeltap (voornoemd artikel 48) ook zonder externe toestemming met AI gezocht worden, maar moet er wel een plan zijn. In dit laatste geval heeft de CTIVD bindend toezicht (AI op bulktaps: artikel 48 en artikel 50, vierde lid, van de Wiv 2017), aldus de fractieleden van GroenLinks-PvdA. Wij willen hier graag een reactie op geven.

De Wiv 2017 spreekt over geautomatiseerde data-analyse in plaats van AI. AI is onderdeel van het begrip GDA, dat een ruimere reikwijdte heeft omdat er ook andere algoritmische toepassingen onder vallen. De diensten zijn bevoegd om GDA toe te passen op alle gegevens die de diensten verwerven. Hiervoor is geen toestemming nodig, met uitzondering van de toepassing van GDA op OOG-metadata gericht op de identificatie van personen en organisaties. In het geval geautomatiseerde data-analyse toegepast gaat worden op ex artikel 48 Wiv 2017 verworven metadata, met als doel het identificeren van personen of organisaties is van tevoren toestemming vereist (art 50, eerste lid, onder b). Een toestemming van de minister voor verkennen ten behoeve van OOG-interceptie wordt getoetst door de TIB op rechtmatigheid voordat de bevoegdheid wordt toegepast.

De fractieleden van GroenLinks-PvdA zijn van mening dat toetsing (vooraf en tijdens) heel belangrijk is bij geautomatiseerde data-analyse van gegevens die 'in bulk' zijn verzameld vanwege de risico's die hiermee samenhangen. De leden stellen dat de Nederlandse overheid op verschillende terreinen het toezicht op algoritmen aan het versterken is, maar dat in de tijdelijke wet het toezicht op het algoritmegebruik door de geheime diensten juist wordt verminderd. De fractieleden vragen of de regering deze conclusie van voornoemde fractieleden deelt, zo ja, waarom hiervoor is gekozen en zo nee, waarom niet. Graag ontvangen zij een nauwgezette toelichting. Wij beantwoorden deze vragen graag als volgt.

Het toezicht op algoritmegebruik wordt in de Tijdelijke Wet dynamischer. In plaats van een eenmalige, statische toets voorafgaand aan de inzet van de bevoegdheid tot GDA op OOG-metadata door de TIB, wordt dit vervangen door een bindend toezicht door de afdeling toezicht van de CTIVD gedurende de uitvoering van die bevoegdheid en dus ook op het gebruik van algoritmen. De afdeling toezicht kan in dat kader effectief ingrijpen en dat gebruik bij geconstateerde onrechtmatigheden doen beëindigen. Daarnaast kan de afdeling toezicht van de CTIVD in het kader van haar reguliere toezichtstaak toezien op de wijze waarop aan de wettelijke zorgplicht als bedoeld in artikel 24 Wiv 2017 uitwerking wordt gegevens, waaronder de kwaliteitseisen die worden gesteld aan het ontwikkelen en uitvoeren van algoritmen (artikel 24, tweede lid, onder a, Wiv 2017).

[48] Het voorgestelde artikel 8; het cursiveren is gedaan door de fractieleden van GroenLinks-PvdA.

De fractieleden van GroenLinks-PvdA vragen of de tijdelijke wet voldoet aan alle onderdelen van de nieuwe EU-*act* ten aanzien van het gebruik van AI. Graag ontvangen deze leden een appreciatie van de regering op alle afzonderlijke onderdelen. Deze EU-*act* bevat ook afspraken over een onafhankelijke toezichthouder. De leden vragen of de tijdelijke wet voldoet aan de voorwaarden gesteld aan het toezicht, zo ja, waarop is die aanname gebaseerd, en zo nee, wat dat betekent voor deze tijdelijk wet. Wij reageren hierop graag als volgt.

Voor zover met deze vraag wordt gedoeld op de AI-verordening van de Europese Unie geldt dat deze niet van toepassing is op de ontwikkeling en het gebruik van AI-systemen voor het doel van nationale veiligheid. Nationale veiligheid blijft krachtens artikel 4, tweede lid, van het EU-Verdrag immers de uitsluitende verantwoordelijkheid van de lidstaten. De toepassing van GDA door de diensten is gereguleerd door de bepalingen inzake gegevensverwerking uit de Wiv 2017, en in het bijzonder artikel 60 van de Wiv 2017. De AI-verordening heeft dus geen gevolgen voor dit wetsvoorstel.

De staatsecretaris van Binnenlandse Zaken en Koninkrijksrelaties schrijft in de verzamelbrief over algoritmen reguleren van 7 juni 2023:

"[…] *de controle en toetsing worden bemoeilijkt, omdat gemaakte keuzes in het ontwerp en de implementatie van AI of algoritmen ondoorgrondelijk zijn. Hierdoor wordt het voeren van een maatschappelijk debat over de impact bemoeilijkt. Ook controlerende instanties zoals toezichthouders kunnen gemaakte keuzes mogelijk niet of onvoldoende toetsen, omdat niet duidelijk is welke keuzes met of door de technische oplossingen worden gemaakt."*[49]

De fractieleden van GroenLinks-PvdA vragen in hoeverre dit knelpunt in de tijdelijke wet ook aan de orde is en hoe dit wordt voorkomen. De staatsecretaris introduceert een algoritmeregister en het Implementatiekader Algoritmen. De fractieleden vragen hoe de voorliggende wetgeving en daaruit voorvloeiende werkwijze zich verhoudt tot deze nieuwe instrumenten/werkwijze. Wij reageren hierop graag als volgt.

Het ligt niet voor de hand dat wetgeving op het terrein van nationale veiligheid op enigerlei wijze onder de reikwijdte van het algoritmeregister zal worden gebracht. De in de Wiv 2017 vastgelegde beperkingen aan openbaarheid en transparantie staan hieraan logischerwijs in de weg.
Waar het gaat om het toezicht door de CTIVD op het gebruik van AI door de diensten wordt het volgende opgemerkt. De CTIVD heeft volledige toegang tot alle systemen, gegevens en medewerkers van de diensten. Hierdoor is het mogelijk om zowel bij de ontwikkeling van algoritmen toezicht te houden als bij de opleiding van medewerkers, bij het opstellen van de werkinstructies ten behoeve van de uitvoering en bij de technische systemen waarop deze uitvoering daadwerkelijk plaatsvindt. Hierdoor blijft geen enkel aspect van de hele cyclus van algoritme ontwikkeling en gebruik buiten beschouwing. De CTIVD kan ook controleren in hoeverre de diensten het stelsel voor compliance adequaat hebben ingericht, de zogenaamde zorgplicht voor gegevensverwerking (artikel 24 Wiv 2017).

De leden van de GroenLinks-PvdA-fractie vragen hoe de voorliggende wetgeving en daaruit voorvloeiende werkwijze zich verhoudt tot het normenkader dat de Auditdienst Rijk in 2022 heeft opgesteld en het toetsingskader algoritmen van de Algemene Rekenkamer. Wij beantwoorden deze vraag graag als volgt.

De voorliggende wetgeving bevat geen (aanvullende) normen voor het toepassen van algoritmen ten opzichte van de Wiv 2017. Op het toepassen van algoritmen zijn ook de algemene vereisten voor gegevensverwerking uit de Wiv 2017 van toepassing; waaronder proportionaliteit en zorgvuldigheid. Volgens de zorgplicht ex artikel 24 van de Wiv 2017 moeten de hoofden van diensten maatregelen treffen om rechtmatig gegevens te verwerken en de kwaliteit van de gegevensverwerking te bevorderen, waaronder begrepen de daarbij behorende algoritmen en modellen. Dit geldt voor alle algoritmen die worden toegepast ter uitvoering van de Wiv 2017 en de Tijdelijke wet. Net als voor andere overheidsorganisaties kunnen normenkaders van bijvoorbeeld de

[49] *Kamerstukken II 2022/23, 26 643, nr. 1056, p. 3.*

Auditdienst Rijk en de Algemene Rekenkamer voor de diensten behulpzaam zijn om uitvoering te geven aan een zorgvuldige ontwikkeling, toepassing en beheer van algoritmen. We plaatsen nog wel de kanttekening dat die kaders deels gebaseerd zijn op de Algemene verordening gegevensbescherming (AVG) en die verordening niet van toepassing is op de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten.

De fractieleden van GroenLinks-PvdA constateren dat als motivering voor het afschaffen van toezicht vooraf onvoldoende operationele snelheid en wendbaarheid wordt genoemd. Deze leden menen dat een spoedprocedure kan snelheid geven en zij vragen de regering uit te leggen waarom dit geen afdoende oplossing biedt. Ons antwoord op deze vraag luidt als volgt.

In de context van de uitvoering van de Wiv 2017 moet spoed enerzijds onderscheiden worden van snelheid en wendbaarheid anderzijds. De spoedprocedure is bedoeld voor onvoorziene en uitzonderlijke situaties waarbij niet gewacht kan worden met de inzet van middelen om een dreiging te onderzoeken, terwijl in onderzoeken naar landen met een offensief cyberprogramma operationele snelheid en wendbaarheid juist doorlopend van essentieel belang is en als uitgangspunt dient. Zo moet er bij cyberoperaties snel meebewogen kunnen worden met de aanvaller, bijvoorbeeld door kenmerken bij te schrijven op een hacklast, en is snelheid de norm. Het is daarnaast van belang gedurende een hackoperatie het binnendringen in een geautomatiseerd werk en onderzoek in dit systeem ononderbroken voort te zetten. Dit om te voorkomen dat inlichtingenposities verloren gaan, doordat operaties stil komen te liggen of operaties worden onderkend. De spoedprocedure uit de Wiv 2017 is daarom niet de geschikte procedure om snelheid en wendbaarheid in deze onderzoeken te bewerkstelligen. Dit wetsvoorstel beoogt oplossingen te bieden om die snelheid en wendbaarheid in de dagelijkse praktijk van de diensten mogelijk te maken. Dit zorgt ervoor dat de wijze waarop de diensten onderzoek doen past bij de gebruikelijke dynamiek van de dreiging. Daarom wordt in een gedeeltelijke verschuiving van de statische TIB toets vooraf naar bindend toezicht van de afdeling toezicht van de CTIVD gedurende en na afloop van de uitvoering van bepaalde bijzondere bevoegdheden voorzien, bijvoorbeeld ten aanzien van de bijschrijfmogelijkheid bij de bevoegdheid tot het binnendringen in en de bevoegdheid tot het verkennen van geautomatiseerde werken.

De fractieleden van GroenLinks-PvdA vragen hoe de algoritmen en AI die de opgeslagen data doorzoeken, worden getraind en ingesteld. Aansluitend vragen de leden hoe kan worden voorkomen dat hier bias in ontstaat. Wij beantwoorden deze vragen als volgt.

De AIVD en de MIVD zijn vanzelfsprekend vanuit hun taakuitvoering erbij gebaat dat algoritmen correct functioneren en dat ze op de hoogte zijn van alle eigenschappen van de opgeslagen en te verwerken gegevens. Ten behoeve hiervan worden medewerkers opgeleid en is er een zorgplicht voor wat betreft het gebruik van algoritmen en de omgang met gegevens. Dat betekent dat het gebruik van algoritmen en de omgang met gegevens op een verantwoorde en gedocumenteerde manier plaatsvindt. Hierdoor kan op dit hele proces de afdeling toezicht van de CTIVD inhoudelijk en technisch toezicht houden.

Met het wetsvoorstel dat voorligt, wordt voor een belangrijk deel het toezicht verschoven van ‘vooraf’ naar ‘tijdens’. Hierover hebben de fractieleden van GroenLinks-PvdA enkele vragen. Bij toezicht *vooraf* hebben de diensten en de Rijksoverheid een belang bij voldoende toegeruste toezichthouders, want zonder toestemming vooraf kan het werk niet beginnen. Er zal dus maximaal geprobeerd worden om de toezichthouders adequaat (snel en tijdig) te informeren bij vragen, zodat het werk kan aanvangen. Bij toezicht ‘tijdens’ verandert dit: wanneer de toezichthouder het niet kan bijhouden, dan gaat het werk door, maar dan (tijdelijk?) met minder toezicht.

Graag ontvangen de fractieleden van GroenLinks-PvdA een reflectie op deze redenering over de onderlinge afhankelijkheden van de diensten en de toezichthouders. Indien de regering het niet eens is met de redenering, dan ontvangen zij graag een motivering.

De Nederlandse maatschappij heeft ten behoeve van de bescherming van de nationale veiligheid belang bij goed functionerende inlichtingen- en veiligheidsdiensten en een goed functionerend stelsel van toezicht. De wetgever heeft immers aan de diensten verstrekkende bevoegdheden toegekend en de toepassing daarvan moet aan strikte rechtmatigheidseisen voldoen. Een

toereikend stelsel van *checks and balances* waarin die bevoegdheidsuitoefening is ingebed en met adequate bevoegdheden toegeruste toezichthouders zijn daarbij van essentieel belang. In dit kader is ook van belang dat de wet erin voorziet dat de toezichthouders alle medewerking en inlichtingen worden verstrekt die zij voor een goede taakuitvoering nodig hebben. Dat is ook noodzakelijk om te (blijven) voldoen aan de eisen die uit het EVRM voortvloeien, waar het gaat om de inbreuken die door de bevoegdheidsuitoefening worden gemaakt op door het EVRM gegarandeerde mensenrechten (zoals privacy, vrijheid van nieuwsgaring en dergelijke). Dat is ook van belang om het zo noodzakelijke draagvlak voor de activiteiten van de diensten in de maatschappij te behouden.

Het klopt dat de Tijdelijke wet enkele aanpassingen voorstelt binnen het stelsel van toetsing en toezicht. De reden voor deze aanpassingen is om het stelsel van toetsing en toezicht beter aan te laten sluiten bij de dynamiek van het cyberdomein en de operationele praktijk van het werk van de diensten. Er kan daardoor ook effectiever toezicht plaatsvinden. Een belangrijk uitgangspunt bij het vormgeven van dit wetsvoorstel is dat het toezicht op het werk van de diensten niet wordt afgeschaald en op z'n minst gelijk blijft, in lijn met de in de Tweede Kamer aanvaarde motie van het lid Van Baarle. Daar is met de voorgestelde wijzigingen aan voldaan.

De diensten zijn erbij gebaat dat de afdeling toezicht van de CTIVD in staat is om adequaat toezicht te houden. Als de afdeling toezicht van de CTIVD door omstandigheden niet (tijdig) toezicht kan houden en bijvoorbeeld pas na geruime tijd een onrechtmatigheid zou constateren, heeft dit verstrekkende gevolgen voor het werk van de diensten. Gegevens moeten wellicht vernietigd worden, zaken moeten worden teruggedraaid en de potentiële impact is daardoor zeer groot. Het is voor de diensten veel wenselijker om tijdig signalen van de toezichthouder te hebben om bepaalde zaken aan te scherpen. Dit zorgt ervoor dat over de volle breedte en op de langere termijn, de diensten beter en met meer vertrouwen hun werk kunnen doen in de wetenschap dat er door de toezichthouder systematisch op de rechtmatigheid van deze werkzaamheden kan worden toegezien.

Volgens de fractieleden van GroenLinks-PvdA is toetsen *achteraf* veel meer werk en complexer dan toetsen *vooraf*. Want de toezichthouder moet uitzoeken wat de bedoeling was, wat er daadwerkelijk gebeurd is, en of dat te ver ging.

Graag ontvangen voornoemde fractieleden een reflectie op deze redenering. Ook vragen zij hoe de regering deze redenering beziet in het licht van de wens om het toezicht op peil te houden/niet af te schalen. Wat zijn de afspraken als de toezichthouders van mening zijn dat zij 'verzuipen' in het werk? Wie wordt er dan geïnformeerd? Kan de regering toezeggen dat dit signaal direct ook aan de Tweede en Eerste Kamer wordt gemeld? Hoe wordt voorkomen dat er, in zo'n situatie, dingen misgaan? Wij reageren hierop graag als volgt.

Voor het antwoord op de vraag hoe de regering de redenering in het licht van de wens om het toezicht op peil te houden/niet af te schalen beziet, verwijzen we naar het hiervoor gegeven antwoord.

Voor zowel de diensten als de toezichthouders geldt dat de Tijdelijke Wet extra capaciteit zal vragen, zowel bij de implementatie ervan als bij de toepassing. In aanloop naar de inwerkingtreding is er daarom al met beide instanties gesproken over de benodigde extra capaciteit, zowel juridisch als ondersteunend van aard. Voor een uitgebreidere toelichting op de uitkomsten van de uitvoeringstoetsen en de gevolgen voor de uitvoering van de diensten van de Tijdelijke wet wordt verwezen naar het antwoord op een soortgelijke vraag van de fractieleden van GroenLinks-PvdA. Met de afdeling toezicht van de CTIVD en de TIB is afgesproken dat zij, vooruitlopend op de inwerkingtreding van de Tijdelijke wet, hun formaties uitbreiden. Zo krijgt de afdeling toezicht van de CTIVD er 10 FTE bij en de TIB 3 FTE. Hiermee verwachten de toezichthouders het werk voortvloeiend uit de Tijdelijke Wet uit te kunnen voeren. Ook na de inwerkintreding van de wet worden de gesprekken op diverse niveaus met de toezichthouders voortgezet. Een onderdeel van deze gesprekken zal de werkvoorraad zijn. Indien de werkvoorraad bij de TIB en de afdeling toezicht van de CTIVD, ondanks de capaciteitsuitbreiding, te groot blijkt te zijn, dan zal dit aanleiding zijn voor een gesprek met de ministers, om in samenspraak tot een oplossing te komen. Mocht het goede functioneren van beide instanties in het geding zijn zal het kabinet de kamer daarover informeren.

De fractieleden van GroenLinks-PvdA constateren dat in het onder de Wiv 2017 geldende stelsel van toezicht op de AIVD en de MIVD sprake is van een bindende toets vooraf door de TIB bij de inzet van de meest indringende bijzondere bevoegdheden. De leden stellen vervolgens dat in het toezichtstelsel op onderdelen het bindend toezicht wordt afgeschaft en dat er geen sprake zou zijn van een dekkend bindend toezicht (voor- dan wel achteraf). De leden vragen de regering een overzicht te geven van alle onderdelen (per wetsartikel) waarvoor het bindend toezicht verdwijnt in de tijdelijke wet en voor welke onderdelen het bindend toezicht verschuift van vooraf naar tijdens/achteraf. Wij beantwoorden dit verzoek graag als volgt.

In de Wiv 2017 wordt voor een aantal bijzondere bevoegdheden voorgeschreven dat die niet mogen worden uitgeoefend voordat de toestemming van de minister op rechtmatigheid is getoetst door de TIB. Indien de toestemming van de minister door de TIB rechtmatig wordt bevonden, houdt de afdeling toezicht van de CTIVD vervolgens niet-bindend toezicht gedurende en na afloop van de uitoefening van de bevoegdheid. De figuur van bindend toezicht door de afdeling toezicht van de CTIVD komt in de Wiv 2017 niet voor. In de Tijdelijke wet wordt voor een drietal situaties de TIB-toets vooraf geheel of gedeeltelijk vervangen door bindend toezicht door de afdeling toezicht van de CTIVD. Er zijn géén situaties waarin onder de Tijdelijke wet de TIB-toets komt te vervallen zónder dat dit wordt vervangen door bindend toezicht door de afdeling toezicht van de CTIVD. De verschuiving van een bindende TIB-toets vooraf naar bindend toezicht door de afdeling toezicht van de CTIVD vindt plaats ten aanzien van de volgende onderdelen:
- verkennen van geautomatiseerde werken (artikel 45, eerste lid, onder a van de Wiv 2017, artikel 4, eerste lid, van de Tijdelijke wet);
- de technische risico's bij het binnendringen van een geautomatiseerd werk (artikel 45, vierde lid, onder a van de Wiv, artikel 5, eerste lid, van de Tijdelijke wet) (door de TIB worden enkel op het moment van de aanvraag bekende technische risico's getoetst) en:
- het toepassen van geautomatiseerde data-analyse op de metadata van middels OOG-interceptie verkregen gegevens (artikel 50, eerste lid, onder b van de Wiv 2017, artikel 8 van de Tijdelijke wet);

Hiernaast is er ook een drietal situaties waar de Tijdelijke wet de mogelijkheid biedt om bij te schrijven in plaats van een geheel nieuwe toestemmingsprocedure voor de desbetreffende bijzondere bevoegdheid te doorlopen. In deze drie situaties wordt op de oorspronkelijke toestemming tot uitvoering van de desbetreffende bevoegdheid nog steeds een TIB-toets uitgevoerd, maar kan op die verleende toestemming worden bijgeschreven. Op deze bijschrijvingen wordt telkens bindend toezicht gehouden door de CTIVD. Dit betreft de volgende onderdelen:
- bijschrijven van geautomatiseerde werken die niet-exclusief in gebruik zijn door de persoon of organisatie waarnaar onderzoek wordt gedaan (artikel 5, tweede lid, van de Tijdelijke wet);
- bijschrijven van nummers of technische kenmerken die gebruikt worden door dezelfde persoon of organisatie waar de oorspronkelijke toestemming op ziet (artikel 9 van de Tijdelijke wet) en:
- bijschrijven van een andere aanbieder, persoon of instantie die in de plaats treedt van de aanbieder, persoon of instantie waar de oorspronkelijke toestemming op ziet (artikel 10 van de Tijdelijke wet).

De fractieleden van GroenLinks-PvdA wensen een beeld te krijgen van de impact van *niet-bindend toezicht*. Zij vragen hoe vaak er in het kader van *niet-bindend toezicht* afgelopen jaren (sinds de invoering van de Wiv 2017) door de beide toezichthouders een is brief geschreven/een verzoek gedaan om alsnog in te grijpen, hoe vaak hier door de regering positief op is gereageerd, en hoe vaak niet. Wij beantwoorden deze vraag als volgt.

De afdeling toezicht van de CTIVD is belast met het toezicht op de rechtmatigheid van de uitvoering van de Wiv (en Wet veiligheidsonderzoeken) door de diensten. De afdeling toezicht van de CTIVD voert regelmatig rechtmatigheidsonderzoeken en uit en stelt daarover toezichtsrapporten op. Dit kan ook op verzoek van één van beide kamers. De afdeling toezicht van de CTIVD zendt het rapport aan de betrokken minister. De betrokken minister zendt het rapport met zijn reactie daarop aan beide kamers van de Staten-Generaal. Het rapport en die reactie worden daarmee openbaar; uitgezonderd de staatsgeheime gegevens die uitsluitend aan de CIVD worden voorgelegd. Het toezichtsrapport bevat over het algemeen aanbevelingen met betrekking tot eventueel te treffen maatregelen. Deze aanbevelingen worden vrijwel altijd overgenomen. Slechts in één geval heeft de

regering een aanbeveling van de afdeling toezicht van de CTIVD niet opgevolgd, dit was het advies van de afdeling toezicht van de CTIVD over de bulkdatasets en het algemene relevantiebeoordelingssysteem. De Tweede Kamer is hierover geïnformeerd per brief van 22 september 2020.[50] De TIB geeft alleen bindende rechtsmatigheidsoordelen.

De TIB voert ook een volledige proportionaliteitstoets uit ten aanzien van hackoperaties door de diensten. De TIB stelt:

"*Per brief van 31 maart 2023 hebben de toenmalig minister van BZK en de minister van Defensie uiteengezet dat de Tijdelijke wet geen beperking van de proportionaliteitstoets zal betekenen. Onderdeel van deze proportionaliteitsafweging bij hackoperaties is of door de inzet van het middel inbreuken worden gemaakt op de fundamentele rechten van burger en of de inzet van het middel zwaarder weegt dan deze inbreuken. Het hacken beperkt zich overigens niet alleen tot een target, maar kan zich ook richten ook op non targets of derden. Ook hun belangen worden bij de beoordeling betrokken.*"[51]

Met de tijdelijke wet wordt in artikel 5, eerste lid de verplichting om een omschrijving van de technische risico's op te nemen in de beslissing, buiten toepassing verklaard. De TIB stelt:

"*De TIB heeft overigens goede nota genomen van de brief van de minister d.d. 31 maart 2023 waarin benadrukt wordt dat er geen enkele intentie is om de wijze waarop de TIB thans de proportionaliteitstoets uitvoert in te perken. De aanpassing in de toelichting bij de beoordeling van technische risico's is doorgevoerd met als doel te verduidelijken waar (in de nieuwe systematiek) het domein van de TIB ophoudt en het domein van de CTIVD begint, aldus de minister.*"[52]

De fractieleden van GroenLinks-PvdA vragen of de regering de interpretatie van de TIB van de uit te voeren proportionaliteitstoetsing deelt. Wij reageren hierop graag als volgt.

De regering staat achter haar standpunt als verwoord in de brief d.d. 31 maart 2023. De regering heeft niet beoogd de wijze waarop de TIB de proportionaliteitstoets uitvoert in te perken. Wel is beoogd te verduidelijken hoe de TIB op het moment van het verzoek om toestemming voor inzet van de bevoegdheid bekende risico's in haar proportionaliteitstoets kan betrekken. De minister kan de beschrijving van de bekende risico's meenemen in de beoordeling of een operatie tot binnendringen in een geautomatiseerd werk verantwoord is en dus toegestaan kan worden. De verleende toestemming wordt vervolgens door de TIB getoetst op rechtmatigheid en de TIB kan de bekende risico's, zoals hiervoor uiteengezet, in haar proportionaliteitstoets meewegen. Gezien de dynamische en onvoorzienbare aard van hackoperaties zal deze toets door de TIB op bekende risico's een hoger abstractieniveau hebben. Ook zal het vaak het geval zijn dat er vooraf geen risico's bekend zijn, omdat de diensten risico's veelal proberen te mitigeren of vermijden voordat tot handelen wordt overgegaan. Om die redenen heeft de regering ervoor gekozen om het toezicht op technische risico's bij de inzet van de hackbevoegdheid ex durante bij de afdeling toezicht van de CTIVD te beleggen.

De leden van de GroenLinks-PvdA-fractie stellen dat met de huidige wet 'bijschrijven', 'bijtappen' en 'bijhacken' van computers/telefoons van derden niet kan zonder TIB-toets. Op dit moment moet in een lopende operatie een nieuwe toestemmingsprocedure worden gestart als de diensten de inzet wil uitbreiden tot andere geautomatiseerde werken of technische kenmerken die de *cyberactor* gebruikt. In de tijdelijke wet zijn de mogelijkheden verruimd om in de bestaande toestemming voor de inzet van bepaalde bevoegdheden andere geautomatiseerde werken of kenmerken die de *cyberactor* in dat kader gebruikt, 'bij te schrijven', 'bij te tappen' en/of 'bij te hacken'. Gelet op de risico's voor derden en de inbreuk op het recht op bescherming van de persoonlijke levenssfeer die de voorgestelde verruiming met zich brengt, merkt de Raad van State op dat gebruikmaking van de spoedprocedure de voorkeur heeft. De fractieleden vragen waarom de regering niet kiest voor de spoedprocedure, en hoe zij oordeelt over de tijdswinst enerzijds en het verlies van de waarborgen anderzijds. Wij reageren hierop graag als volgt.

[50] *Kamerstukken II 2020/21, 29 924, nr. 203.*
[51] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 8.
[52] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 5.

Voor wat betreft de vraag waarom niet wordt gekozen voor de spoedprocedure, wordt verwezen naar de beantwoording van vergelijkbare vraag van de leden van de fractie van GroenLinks-PvdA. Het gaat hier niet om spoed, maar om snelheid en wendbaarheid. Van verlies van waarborgen is naar ons oordeel geen sprake. Voor de initiële inzet van de bijzondere bevoegdheden waarvoor in de Tijdelijke wet de mogelijkheid tot bijschrijving wordt geregeld, geldt dat op de daartoe verleende toestemming de TIB-toets gehandhaafd blijft en dat vervolgens bij de bijschrijving op de verleende toestemming er bindend toezicht door de afdeling toezicht wordt geïntroduceerd. De regering ziet hierin geen verlies van waarborgen, maar per saldo een versteviging van het toezicht.
De fractieleden van GroenLinks-PvdA wijzen erop dat er in de huidige wet eisen staan voor het tappen van advocaten en journalisten. Ook heeft de CTIVD concrete uitspraken gedaan wanneer dit mag gebeuren. De leden vragen of deze CTIVD-richtlijnen worden geschrapt. Wij beantwoorden deze vraag graag als volgt.

De eisen voor de inzet van bijzondere bevoegdheden jegens advocaten en/of journalisten zijn opgenomen in de Wiv 2017. Deze eisen worden niet aangepast door de Tijdelijke wet. Voor zover met de concrete uitspraken van de CTIVD verwezen wordt naar de tijdelijke regeling van de afdeling toezicht van de CTIVD bij toezichtsrapport 52 over de inzet van bijzondere bevoegdheden jegens advocaten en journalisten door de AIVD en de MIVD wordt opgemerkt dat deze tijdelijke regeling was opgesteld ten tijde van de Wiv 2002 omdat de Wiv 2002 niet voorzag in onafhankelijk toezicht door een orgaan dat de bevoegdheid heeft de inzet van een bijzondere bevoegdheid jegens advocaten of journalisten te voorkomen of te beëindigen terwijl dit wel noodzakelijk was.[53] Deze taak werd (tijdelijk) belegd bij een tijdelijke onafhankelijke toetsingscommissie bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten die voorafgaande aan onder meer de inzet van een bijzondere bevoegdheid of verstrekking aan het Openbaar Ministerie (OM) verplicht om bindend advies moest worden gevraagd.[54] Deze regeling is vervallen met inwerkingtreding van de Wiv 2017.

De leden van de GroenLinks-PvdA-fractie stellen dat de diensten bij het hacken niet meer vooraf technische risico's en onbekende kwetsbaarheden hoeven te beschrijven (en ook niet achteraf). Met de tijdelijke wet wordt in artikel 5, eerste lid de verplichting om een omschrijving van de technische risico's op te nemen in de beslissing, buiten toepassing verklaard. Zowel de Raad van State als de Evaluatiecommissie Wiv zien een belangrijke waarborg in het zoveel mogelijk vooraf omschrijven van technische risico's en het gebruik van onbekende kwetsbaarheden. Hacken is immers een bevoegdheid met mogelijk vergaande gevolgen voor derden, ook in het licht van de verruiming van de bijschrijfmogelijkheid. De Raad van State stelt dat "*het vooraf omschrijven van technische risico's, waaronder het gebruik van onbekende kwetsbaarheden, het proportionaliteitsvereiste operationaliseert; het is nodig om een heldere afweging te kunnen maken over de proportionaliteit van de inzet van de hackbevoegdheid.*"[55] De leden vragen waarom deze, zoals de Raad van State het verwoordt, operationalisatie van het proportionaliteitsvereiste niet wordt omarmd door de regering. De leden menen dat dit ook de diensten noodzakelijke waarborgen biedt. Wij reageren hierop graag als volgt.

De regering kiest ervoor om op passende wijze invulling te geven aan waarborgen, waarbij een duidelijker afbakening plaatsvindt van wie in welke fase wat toetst en waarbij de effectiviteit daarvan – strekkende tot een proportionele inzet gelet op de daarmee gepaard gaande beperking van het recht op privacy – bepalend is. Enkel op het moment van de aanvraag bekende technische risico's dienen naar ons oordeel bij de ex ante door de TIB te worden getoetst. Daarbij is van belang dat voorafgaand aan de inzet van de hackbevoegdheid het zo is dat concrete technische risico's niet bekend zijn, omdat de technische omgeving nog niet bekend is en de uit te voeren handelingen van de diensten binnen deze omgeving ook niet. Hoe concrete risico's zich tijdens de operatie daadwerkelijk manifesteren wordt immers pas tijdens de uitvoering van de operatie duidelijk. De afdeling toezicht kan tijdens een operatie mee kijken bij het uitvoeren van de hackbevoegdheid en indien aan de orde een oordeel vormen of een technisch risico dat daarbij

[53] Voorzieningenrechter rechtbank Den Haag, 1 juli 2015, ECLI:NL:RBDHA:2015:7436 en gerechtshof Den Haag, 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.
[54] Stcrt. 2015, 46477.
[55] *Kamerstukken II 2022/23, 36 263, nr. 4, p. 29.*

optreedt proportioneel is ten opzichte van de inbreuk die ermee wordt gemaakt op de rechten van derden. Indien de afdeling toezicht dit disproportioneel acht kan er bindend worden ingegrepen.

De fractieleden van GroenLinks-PvdA verwijzen naar de consultatiereactie van Bits of Freedom, die het belang van juist deze technische toets vooraf benadrukt en stelt dat de diensten de afweging over welke risico's voor de samenleving aanvaardbaar zijn, niet alleen kunnen maken: *"Zij hebben, nog meer dan wij allen door de grote belangen die met hun werk gemoeid gaan, baat bij een blik van buitenaf."*[56] De fractieleden vragen om een reflectie van de regering op deze zienswijze.

Zoals hiervoor al is uiteengezet over het toezicht op technische risico's bij de uitvoering van de hackbevoegdheid, is deze effectiever in de fase van uitvoering. Daarbij toetst de TIB ex ante nog steeds op de op het moment van de aanvraag bekende technische risico's. Wel is het zo dat de afweging of bepaalde risico's wel of niet aanvaardbaar zijn primair door de diensten zelf – onder verantwoordelijkheid van de voor de dienst verantwoordelijke minister – zullen worden gemaakt, immers bij de aanvraag van de toestemming zal omtrent die afweging verantwoording afgelegd moeten worden. Daarbij komt dat het minimaliseren van technische risico's van groot belang is bij het uitvoeren van hackoperaties. Niet alleen omdat de diensten zorgvuldig werken en de met de inzet gepaard gaande technische neveneffecten zo klein mogelijk willen houden, maar ook omdat het voor de diensten essentieel is om bij de uitvoering van de hackbevoegdheid niet onderkend te worden. Daarom zullen de diensten bij de uitvoering van de hackbevoegdheid ervoor zorgen dat de technische risico's zo klein mogelijk. De voor de afweging benodigde technische en juridische expertise is bij de diensten voorhanden. Bij de te maken afweging worden uitdrukkelijk ook de gevolgen voor bijvoorbeeld de rechten van derden betrokken, met name in de proportionaliteitstoetsing.

De fractieleden van GroenLinks-PvdA stellen dat hoewel de Evaluatiecommissie Wiv heeft aangedrongen op een nadere duiding van de strategische inzet van de hackbevoegdheid, het wetsvoorstel deze niet lijkt te geven. Het wetsvoorstel biedt daarmee mogelijk onvoldoende handvatten voor de TIB voor haar beoordeling van de strategische inzet van de hackbevoegdheid. In de memorie van toelichting staat een passage over het 'alvast' hacken van bedrijven, omdat het later misschien nuttig kan zijn, aldus de fractieleden.[57] Zij vragen welke waarborgen hierbij van toepassing zijn die getoetst kunnen worden door de toezichthouder. Wij reageren hierop graag als volgt.

In paragraaf 2.2.2 van de memorie van toelichting is een nadere duiding gegeven van de strategische inzet van de hackbevoegdheid. De strategische inzet van bevoegdheden is onder de Wiv 2017 al mogelijk. Desalniettemin bestond in de praktijk de behoefte duidelijkheid te verschaffen over deze werkwijze. Bestaande bevoegdheden worden dus ingezet in een strategische operatie. Het gaat hier dus niet om een nieuwe, aparte bevoegdheid. Daarnaast wenst de regering te benadrukken dat de Tijdelijke wet niet het stelsel van waarborgen wijzigt voor een strategische operatie ten opzichte van de Wiv 2017. Dit betekent dat de TIB als toetsingscommissie dezelfde toets uitvoert op een verleende toestemming ten aanzien van de (onderbouwing van de) noodzaak, proportionaliteit, subsidiariteit en gerichtheid, voorafgaand aan de inzet van een bevoegdheid. Wel zal daarbij de door de regering uiteengezette noties waar het gaat om welke technische risico's bij een TIB-toets aan de orde zijn, betrokken dienen te worden.

De fractieleden van GroenLinks-PvdA constateren dat in het jaarverslag van de TIB van 2022[58] enkele passages zwart zijn gelakt. Deze leden vragen of het mogelijk is om deze passages vertrouwelijk in te zien, en zo nee, op basis waarvan niet. Wij beantwoorden deze vraag als volgt.

Er zijn door de wetgever in het belang van de nationale veiligheid enkele beperkingen gesteld aan de openbare verslaglegging. Zo moeten de gegevens die zicht geven op de door de diensten

[56] Schriftelijke inbreng Bits of Freedom voor het rondetafelgesprek van woensdag 5 april 2023 in de Tweede Kamer inzake de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma tegen Nederlandse belangen, p. 2.
[57] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 7-8.*
[58] https://www.tib-ivd.nl/documenten/jaarverslagen/2023/03/24/jaarverslag-tib-2022.

aangewende middelen in concrete aangelegenheden, de door de diensten gebruikte geheime bronnen en het actuele kennisniveau van de diensten achterwege blijven. Het ontwerpjaarverslag van de TIB wordt – hoewel niet wettelijk verplicht – voor een zogeheten check op mogelijke staatsgeheime informatie aan de verantwoordelijke ministers voorgelegd. De diensthoofden worden aldus in de gelegenheid gesteld om – vanuit de op hen berustende zorgplicht ex artikel 23 en 24 Wiv 2017 – aan te geven of het jaarverslag gerubriceerde gegevens bevat. Dit is het geval geweest in het jaarverslag 2022 van de TIB. Er is door de diensten gewezen op enkele passages die staatsgeheime informatie bevatten. Het betreffen hier passages die zicht geven op de door de diensten aangewende middelen in concrete aangelegenheden, de door de diensten gebruikte geheime bronnen en het actuele kennisniveau van de diensten. De TIB heeft er vervolgens voor gekozen om de betreffende passages te lakken.

Deze gerubriceerde gegevens zijn met de Tweede Kamer gedeeld via de daartoe geëigende kanalen, namelijk de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD). Aangezien de Eerste Kamer geen daarmee vergelijkbare voorziening heeft, kunnen deze gegevens niet ter inzage worden gegeven.

De fractieleden van het CDA stellen dat het wetsvoorstel de nodige complexiteit meebrengt als het gaat om het toezicht op de diensten. Zij wijzen erop dat in dit verband de Raad van State een vraagteken heeft geplaatst bij de beoogde operationele snelheid en wendbaarheid. De fractieleden vragen hoe de regering haar wetsvoorstel in dit licht al met al waardeert. Wij beantwoorden deze vraag als volgt.

Voor het antwoord op deze vraag wordt verwezen naar het hiervoor gegeven antwoord op een soortgelijke vraag van de leden van de GroenLinks-PvdA-fractie waarin zij verzoeken om een algemene reflectie van de regering op de door de Raad van State geschetste complexiteit

De fractieleden van het CDA roepen in herinnering dat de CTIVD bevestigt dat zij de bulkdatasets waarvoor een nieuwe eindtermijn dient te worden vastgesteld op grond van de haar bindende bevoegdheid, zal beoordelen aan de wettelijke criteria. Toch menen de leden dat hierbij vanzelfsprekend de kans blijft bestaan dat – in het licht van de bescherming van grondrechten – de diensten op dit punt onnodige risico’s nemen. De fractieleden vragen de regering hoe zij de reikwijdte van hun nieuwe bevoegdheden ten aanzien van bulkdata beoordelen. Wij beantwoorden deze vraag graag als volgt.

Met de Tijdelijke wet wordt het mogelijk om, voor bulkdatasets waarvan de eindtermijn verloopt, onder voorwaarden een nieuwe eindtermijn te stellen voor het gebruik van een bulkdataset in het geval van dringende redenen met het oog op de nationale veiligheid. Op grond van de uitwerking van de wettelijke criteria in het toestemmingsverzoek beoordeelt de bevoegde minister of alles afwegende, inderdaad sprake is van dringende redenen met het oog op de nationale veiligheid. Zo moet onder andere de noodzaak, proportionaliteit en subsidiariteit gemotiveerd worden alsmede aangegeven worden hoelang de bulkdataset reeds wordt bewaard en wat de verwachte potentiële bijdrage is aan enig lopend onderzoek. Als extra waarborg kan de afdeling toezicht van de CTIVD bindend toezicht houden op het besluit tot het vaststellen van een nieuwe eindtermijn waarbij naar aanleiding van het amendement Hammelburg de afdeling toezicht van de CTIVD in elk geval de rechtmatigheid onderzoekt van het derde opeenvolgende besluit tot het vaststellen van een nieuwe eindtermijn.[59] Naar ons oordeel kan de afdeling toezicht effectief ingrijpen indien zij oordeelt dat er sprake is van onnodige risico’s.

De leden van de CDA-fractie heeft er kennis vangenomen dat, zoals benadrukt door de TIB, sommige waarborgen voor grondrechten en privacy niet meer vooraf, maar tijdens en achteraf getoetst worden. Op basis van praktijkervaring hoeft dat mogelijk niet problematisch te zijn. De leden vragen of de regering bereid is maatregelen te nemen als toch te vaak blijkt dat achteraf tot de conclusie wordt gekomen dat bevoegdheden ten onrechte zijn aangewend, althans daar op een verkeerde manier gebruik van is gemaakt. Ons antwoorde op deze vraag luidt als volgt.

[59] *Kamerstukken II 2022/23, 36 26e, nr. 31.*

Vanzelfsprekend is de regering bereid om maatregelen te nemen als te vaak blijkt dat achteraf tot de conclusie wordt gekomen dat bevoegdheden ten onrechte zijn aangewend. Het is de verwachting dat dit, gelet op het gebalanceerde stelsel van waarborgen dat is opgetuigd in de Tijdelijke wet, niet aan de orde zal zijn. De TIB houdt in bijna alle gevallen een rol bij de toetsing voorafgaand aan de inzet van bevoegdheden. In overige gevallen heeft de afdeling toezicht van de CTIVD onder de Tijdelijke wet de bevoegdheid bindend toezicht uit te oefenen tijdens de inzet van de bevoegdheid. Daarnaast behoudt de afdeling toezicht van de CTIVD hun reguliere toezichtstaak op de rechtmatige uitvoering van de wet door de diensten. Indien de afdeling toezicht van de CTIVD bij uitvoering van het bindend toezicht tot het oordeel komt dat bepaalde bijzondere bevoegdheden onrechtmatig zijn aangewend, informeert de bevoegde minister beide Kamers der Staten-Generaal over het oordeel van de CTIVD (artikel 12, zesde lid, Tijdelijke wet). Het parlement kan de minister ter zake ter verantwoording roepen.

De fractieleden van D66 merken op dat in de Tweede Kamer het amendement-Bisschop en Van der Graaf[60] is aangenomen. In een brief aan de Tweede Kamer geeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aan hoe het amendement geïnterpreteerd dient te worden en dat daarbij aansluiting dient te worden gezocht bij de memorie van toelichting op de wet.[61] In de brief die de Eerste Kamer op 7 december 2023 van de TIB ontving, lijkt de TIB een andere opvatting van de invulling en uitvoering van dit amendement te hebben dan de minister, aldus de fractieleden.[62] Zij vragen de regering toe te lichten welke opvatting gevolgd dient te worden. Wij beantwoorden deze vraag graag als volgt.

Voor het antwoord op deze vraag wordt verwezen naar het hiervoor gegeven antwoord op vragen van de leden van de fractie van GroenLinks-PvdA waarin zij vragen naar een reactie van de regering op de interpretatie van het betreffende amendement van de TIB

De fractieleden van D66 constateren dat wat betreft het bewaren van bulkdatasets de TIB al heeft aangegeven dat, omdat zij de bepaling in de tijdelijke wet ziet als een ongelimiteerde bewaartermijn, zij dit mee wil wegen in haar proportionaliteitstoets.[63] Maar zoals de fractieleden het wetsvoorstel lezen, moet de TIB vooraf een oordeel geven over het verwerven van de gegevens en kan de CTIVD vervolgens gedurende en na het onderzoek toezicht houden. Ook moet de CTIVD een bindend oordeel uitspreken bij het derde verzoek tot het opnieuw vaststellen van de eindtermijn (zie het aangenomen amendement-Hammelburg c.s.[64]). De leden vragen hoe de ene toezichthouder zich in dit geval tot de andere verhoudt, aangezien de CTIVD bindend de rechtmatigheid kan toetsen bij het vaststellen van de nieuwe eindtermijn. Wij reageren hierop graag als volgt.

De regering wenst op te merken dat in het wetsvoorstel wordt voorzien in een eindtermijn van anderhalf jaar. Er is dus geen sprake van een ongelimiteerde bewaartermijn. De rol van de TIB is om een rechtmatigheidstoets uit te voeren op de toestemming van de minister om een bijzondere bevoegdheid (verwerving) in te zetten waarbij, indien het toestemmingsverzoek betrekking heeft op de verwerving van een bulkdataset, moet worden uitgegaan van de eindtermijn van anderhalf jaar. Weliswaar is – in navolging van het advies van de Raad van State – voorzien in een mogelijkheid om na deze eerste termijn een nieuwe eindtermijn vast te stellen indien er sprake is van dringende redenen met het oog op de nationale veiligheid, maar het is geen vanzelfsprekendheid dat hiervan gebruik zal worden gemaakt. De CTIVD houdt bindend toezicht op het vaststellen van een nieuwe eindtermijn en de verdere verwerking van rechtmatig verworven gegevens.

De hiervoor gegeven uitleg is onderdeel van de parlementaire geschiedenis en beoogt duidelijkheid te verschaffen over de uitleg van de Tijdelijke wet zodat een beroepsprocedure bij de Afdeling bestuursrechtspraak op dit punt voorkomen kan worden.

---

[60] *Kamerstukken II 2023/24, 36 263, nr. 27.*
[61] *Kamerstukken II 2023/24, 36 263, nr. 33, p. 2.*
[62] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 8.
[63] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 6.
[64] *Kamerstukken II 2023/24, 36 263, nr. 30.*

Daarnaast kan worden gewezen op de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 die ook van toepassing zal zijn op de bulkdatasets die onder de regeling op grond van dit wetsvoorstel vallen. Deze regeling bepaalt dat na een, twee of drie jaar getoetst moet worden of de bulkdataset langer gebruikt mag worden en is er een autorisatie voor toegang en gebruik regime van toepassing, afhankelijk van de beperking die het gebruik van deze bulkdataset kan hebben op het recht op de eerbiediging van de persoonlijke levenssfeer. Hiermee is de voorgestelde regeling omgeven met voldoende waarborgen.

Benadrukt wordt dat de TIB een andersoortige rol heeft dan de afdeling toezicht van de CTIVD: de TIB heeft een rol in de autorisatiefase voorafgaand aan de inzet van (bepaalde) bijzondere bevoegdheden en toetst de door de minister verleende toestemming op rechtmatigheid (vergelijkbaar met de figuur van goedkeuring als bedoeld in afdeling 10.2.1 Algemene wet bestuursrecht). De afdeling toezicht heeft een andersoortige taak en functie en ziet toe op de rechtmatige uitvoering van de Wiv 2017, waaronder de verdere verwerking van de gegevens. Waar de TIB voorafgaand de toestemming voor inzet van bijzondere bevoegdheden toetst, houdt de CTIVD toezicht op het daaruit voortkomende handelen van de diensten over de gehele linie. Dit kan achteraf, maar op grond van de Tijdelijke wet ook tijdens een operatie.

De leden van de D66-fractie vragen of de regering een toelichting kan geven op de getroffen waarborgen waar het gaat om de bijschrijfmogelijkheid zoals beschreven in de artikelen 9 en 10 van het wetsvoorstel wanneer het gaat om advocaten en journalisten (waar het gaat om het willen achterhalen van hun bronnen). Wij beantwoorden deze vraag graag als volgt.

De eisen en waarborgen van de Wiv 2017 blijven onverkort van toepassing waar het gaat om de inzet van bevoegdheden op advocaten en journalisten. Bij de inzet van een bijzondere bevoegdheid jegens advocaten en journalisten is artikel 30 Wiv 2017 van toepassing. Op basis van artikel 30 Wiv 2017 kan de inzet van een bijzondere bevoegdheid enkel worden ingezet na toestemming van de rechtbank Den Haag op verzoek van de betrokken minister en voor de maximale duur van vier weken. Dat geldt ook voor de bijschrijfmogelijkheid in het kader van de Tijdelijke wet op het moment dat de desbetreffende dienst vaststelt dat een journalist gebruik maakt van het kenmerk waarop de inzet is gericht. Daarnaast is in artikel 27, tweede lid, van de Wiv 2017 nog een extra waarborg geregeld als het gaat om gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en dien cliënt verkregen door de uitoefening van een bijzondere bevoegdheid. In dit geval wordt niet direct ingezet op een advocaat (zoals in bovenstaande situatie), maar moet de vertrouwelijke communicatie meer als bijvangst worden beschouwd. Deze gegevens moeten terstond worden vernietigd, tenzij de verdere verwerking ervan noodzakelijk is voor het onderzoek en enkel na toestemming van de rechtbank Den Haag.

De leden van de PVV-fractie constateren dat met dit wetsvoorstel op onderdelen de ex ante-toetsing door de TIB vervalt, waaronder bij het gerichtheidscriterium bij OOG-interceptie. De TIB wordt echter nog wel geacht te toetsen op proportionaliteit. Deze leden vragen of de regering kan aangeven in hoeverre de TIB effectief kan toetsen op proportionaliteit als de mate van gerichtheid buiten beschouwing moet worden gelaten. Deze leden vragen of de mate van gerichtheid niet inherent is aan de proportionaliteitsafweging. Wij beantwoorden deze vraag als volgt.

Het gerichtheidscriterium wordt uitsluitend buiten toepassing gelaten ten aanzien van de mogelijkheid tot verkenning ten behoeve van OOG-interceptie. Ten aanzien van de daaropvolgende daadwerkelijke OOG-interceptie blijft het gerichtheidscriterium onverkort van toepassing, evenals voor alle andere bevoegdheden. Met de opbrengst van de verkenning kan de aanvraag voor de OOG-interceptie zo goed mogelijk onderbouwd worden. Voor de verkenning geldt dat hiernaar de aard van de bevoegdheid een grote mate van ongerichtheid bij hoort. Als de bevoegdheid met grote gerichtheid ingezet zou kunnen worden, dan was immers geen verkenning nodig. Dit is geenszins een belemmering voor het uitvoeren van een proportionaliteitstoets. Bij het beoordelen van de proportionaliteit spelen immers vele aspecten mee, zoals het doel van de inzet, hoe belangrijk de verwezenlijking van dat doel is, hoe grootschalig de inzet is, etc. Ook wanneer een aanzienlijke mate van ongerichtheid een gegeven is, kan dus wel degelijk een gedegen proportionaliteitstoets worden uitgevoerd.

De fractieleden van de PVV wijzen erop dat de memorie van toelichting ten aanzien van OOG-

interceptie spreekt over een "bepaalde mate van ongerichtheid bij het verzamelen van gegevens" en dit verbindt aan 'technisch onderzoek'.[65] De leden vragen of de regering kan aangeven hoe deze mate van ongerichtheid bepaald kan worden om de proportionaliteit en de rechtmatigheid te kunnen beoordelen, en in hoeverre bijvoorbeeld een kabelinterceptie kan plaatsvinden bij een grote internetprovider, waarmee in één keer het volledige gegevensverkeer van alle gebruikers verzameld wordt. Wij reageren hierop graag als volgt.

Het merendeel van de gegevens die worden geïntercepteerd zal altijd zien op personen en/of organisaties die niet in onderzoek bij de diensten zijn en dat ook nooit zullen zijn. De noodzaak van OOG-interceptie ligt met name in het onderkennen van ongekende dreigingen. Juist het feit dat het gaat om het blootleggen van ongekende (cyber)dreigingen maakt dat dit middel alleen effectief is als sprake is van een bepaalde mate van ongerichtheid bij het verzamelen van gegevens. De gegevens die uiteindelijk door de diensten worden opgeslagen, zijn gerelateerd aan de onderzoeksopdrachten van de diensten. Juist de verkennende bevoegdheid tot OOG-interceptie – en het daarbij behorende technisch onderzoek op de verkregen gegevensstromen – draagt bij aan het beter kunnen onderbouwen van de aanvraag tot OOG-interceptie voor de inlichtingenonderzoeken. Immers zou het vernietigen van alle gegevens die niet direct te relateren zijn aan reeds bekende dreigingen, targets en netwerken het onderzoeken van ongekende dreiging onmogelijk maken. De toepassing van filters bij OOG-interceptie kent een mate van geheimhouding, omdat targets anders kunnen anticiperen op deze filters om zo te voorkomen dat ze onderdeel worden van een onderzoek van de diensten. Gegevensstromen zijn dynamisch en wijzigen voortduren. De filters moeten daarop worden aangepast. Daarom kan bij de aanvraag voor het inzetten van het middel slechts een beschrijving worden gegeven voor de wijze waarop de diensten van plan zijn de gegevens te reduceren. Op de uitvoering van dit gehele proces houdt de afdeling toezicht van de CTIVD toezicht.

In reactie op de tweede vraag merken wij in het algemeen op dat kabelinterceptie bij grotere en kleinere internetproviders alsmede bij andere aanbieders van communicatiediensten kan plaatsvinden. Daarbij hoort de kanttekening dat anders dan bijvoorbeeld een gerichte internet- of telefoontap, welke gericht is op een apparaat van een persoon en/of organisatie en betrekking heeft op alle communicatie (inhoud en metadata) die daarmee plaatsvindt waardoor een vollediger beeld van deze persoon en/of organisatie kan worden verkregen, kabelinterceptie gericht is op gegevensstromen. Deze gegevensstromen bevatten slechts gedeelten (fragmenten) van de communicatie van personen en organisaties in het digitale domein. Het levert – anders dan bij gerichte interceptie – geen volledig (en ononderbroken) beeld op van de communicatie van een persoon of organisatie. De diensten richten zich op communicatiestromen die internationaal gegevensverkeer bevatten. Zoals eerder in deze nota naar aanleiding van het verslag is uiteengezet, is vanwege de technische inrichting van het internet en de wijze waarop gegevensstromen daarop plaatsvinden, het nimmer uit te sluiten dat daarin ook gedeelten van gegevens van communicatieverkeer van Nederlandse burgers in zitten.

De leden van de PVV-fractie hebben kennisgenomen van de op 7 december 2023 door de Eerste Kamer ontvangen brieven van de TIB[66] en de CTIVD[67] over dit wetsvoorstel. In deze brieven, met name in de brief van de TIB, worden veel kritische opmerkingen gemaakt over dit wetsvoorstel. De fractieleden vragen de regering – puntsgewijs – een reactie te geven op álle kritiekpunten uit deze brieven. Wij reageren graag als volgt op dit verzoek.

In de brief van de TIB worden verschillende punten en zorgen benoemd. Hieronder worden deze (kort) samengevat en voorzien van een reactie of terugverwijzen indien de vraag al eerder is gesteld. De brief van de CTIVD bevat geen kritiekpunten op het wetsvoorstel en blijft derhalve onbesproken.

> De TIB signaleert dat het gerichtheidscriterium na de uitslag van het raadgevend referendum in 2018 over de Wiv 2017 expliciet en voor alle bijzondere bevoegdheden van toepassing is verklaard waarbij geen onderscheid is gemaakt tussen verschillende

[65] *Kamerstukken II 2022/23, 36 263, nr. 3, p. 21.*
[66] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394.
[67] Brief van de CTIVD van 7 december 2023 aan de Eerste Kamer met kenmerk 174394.01.

bijzondere bevoegdheden en evenmin tussen de verkenningsfase en de productiefase van kabelinterceptie.

Dit is juist en dat beoogt het wetsvoorstel te wijzigen. Met de wijziging van de Wiv 2017, waarmee het gerichtheidscriterium werd gecodificeerd, is aangegeven dat de TIB bij haar beoordeling in gevallen waarbij de gerichtheid een rol speelt het criterium "in hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus" hanteert.[68] De regering achtte dit een bruikbaar criterium en er was geen aanleiding onderscheid te maken tussen de verschillende bevoegdheden. Met het voortschrijden van de tijd en de ontwikkelingen bij het operationaliseren van kabelinterceptie is dit anders geworden. Zoals ook de CTIVD heeft aangegeven in haar rapport over kabelinterceptie ten behoeve van verkenning[69], past strikte toepassing van de eis van gerichtheid niet goed bij het verkennen. Dat betekent evenwel niet dat deze wijze van kabelinterceptie (volstrekt) ongericht is. Er ligt immers wel een motivering voor de keuze voor de te intercepteren kabels aan ten grondslag, waarvoor ook een oordeel van de TIB vereist is. Ook in de praktijk is het gerichtheidscriterium lastig toepasbaar gebleken aangezien de TIB voor de interceptie ten behoeve van verkenning het gerichtheidscriterium inmiddels zo uitlegt dat de diensten moeten aantonen dat de gegevens die de diensten willen intercepteren een aanzienlijke potentiële inlichtingenwaarde moeten bevatten. Deze inschatting kunnen de diensten in de fase van de verkenning echter nog niet maken. Het is juist het doel van de verkenning om te toetsen of de verwachting dat gegevens die worden getransporteerd via de te intercepteren kabels een bijdrage kunnen leveren aan het beantwoorden de onderzoeksvragen van de diensten.

De TIB stelt voorts dat zij thans in alle fasen van kabelinterceptie moet toetsen in hoeverre sprake is van een zo gericht mogelijke uitvoering van de interceptie met gebruikmaking van de volgende definitie: «in hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus».

Zoals hiervoor aangegeven is dit onder de Wiv 2017 juist, maar beoogt het wetsvoorstel hier voor de interceptie ten behoeve van verkenning een wijziging in aan te brengen.

De TIB merkt op dat de Tijdelijke wet een ongerichte verkenningsbevoegdheid creëert die voorheen niet bestond.

In de praktijk sinds de invoering van de Wiv 2017 kreeg de verkenningsbevoegdheid als onderdeel van artikel 48 Wiv 2017 gestalte. Dit werd daarmee een extra fase in het proces van kabelinterceptie. Ten opzichte van de Wiv 2017 voorziet artikel 6 van de Tijdelijke wet in een zelfstandige (geen nieuwe) juridische grondslag voor de bevoegdheid tot verkennen ten behoeve van OOG-interceptie. Daarmee wordt tevens uitvoering gegeven aan een aanbeveling van de CTIVD[70] en de ECW[71]. Ook de TIB ziet een aparte, zelfstandige wettelijke regeling als een welkome wijziging.[72]

De TIB stelt dat de verkenningsbevoegdheid neerkomt op ongerichte kabelinterceptie binnen het toepassingsbereik van de Tijdelijke wet.

Het feit dat er niet aan het gerichtheidscriterium en de bijbehorende uitleg daarvan in de praktijk hoeft te worden gedaan, maakt dit daarmee niet ongericht. Kabelinterceptie begint bij de keuze van de locatie waarop de kabel wordt geïntercepteerd. De diensten dienen onder de Tijdelijke wet te motiveren waarom sprake is van hoofdzakelijk internationaal

[68] Kamerstukken II, 2020/21, 35 242, nr. D, p. 16
[69] Toezichtsrapport 75 over de inzet van kabelinterceptie door de AIVD en de MIVD - De snapshotfase (2022), p. 55
[70] Zie CTIVD-rapport nr. 75 over de inzet van kabelinterceptie door de AIVD en de MIVD
[71] Aanbeveling 19 van de ECW (die overigens spreekt van «metingen» bij bepaalde aanbieders)
[72] Brief van 14 april 2022 van de TIB aan de ministers van BZK en Defensie met reactie TIB op conceptwetsvoorstel Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma

gegevensverkeer en er dient, in lijn met Europese rechtspraak, enige verwachting te zijn dat er sprake is van relevant gegevensverkeer voor de inlichtingenonderzoeken van de diensten. Het fysieke ontvangstpunt bij een aanbieder van een communicatiedienst voor de geïntercepteerde gegevens wordt een accesslocatie genoemd. Op deze locatie vindt, na een TIB-toets, het verwerven van de voor de diensten relevante datastroom ten behoeve van de vastgestelde onderzoeksopdrachten plaats. Op de accesslocatie moeten de diensten vervolgens een keuze maken uit de aanwezige glasvezels, oftewel fibers van een kabel. Binnen de fibers kunnen weer 'tientallen' kanalen te onderscheiden zijn. De diensten identificeren de fibers en kanalen waarvan de gerede verwachting bestaat dat zij relevant zijn voor de uitvoering van één of meerdere van hun onderzoeksopdrachten. Hiertoe kunnen zij informatie opvragen bij een aanbieder, zoals een (markt)partij, waar de accesslocatie gerealiseerd zou kunnen worden. Ook kunnen de diensten verkennen om vast te stellen welke fibers en kanalen relevant zijn genoemd. Daarnaast moet ieder verzoek voldoen aan de eisen van subsidiariteit, noodzaak en proportionaliteit en dit wordt telkens op rechtmatigheid getoetst door de TIB.

Ook verwijst de TIB naar de toezeggingen die naar aanleiding van het referendum door de toenmalige minister zijn gedaan rondom de filtering van streamingsdiensten en verkeer dat oorsprong en bestemming heeft in Nederland (het zogenaamde Nederland-Nederlandverkeer). Dit verkeer zou niet geïntercepteerd worden, tenzij voor cyber defence. De waarborg uit de gedane toezegging dient volgens de TIB op grond van de nota naar aanleiding van het verslag zo gelezen te worden dat het vrijwel uitgesloten is dat de diensten OOG-interceptie zullen inzetten voor inlichtingen- onderzoek naar gegevens met oorsprong en bestemming Nederland, met uitzondering van de onderzoeken binnen cyber defence. Met andere woorden, de toezegging is niet zo bedoeld dat de interceptie van deze gegevens niet zal plaatsvinden. De waarborg zal dus niet gelden ten aanzien van de onderzoeken waar de Tijdelijke wet op ziet, aldus de TIB.

Dit is juist en naar oordeel van ons in lijn met de eerdere gedane toezegging ten tijde van invoering van de Wiv 2017, die als volgt luidt: "Het is daarom vrijwel uitgesloten dat OOG-interceptie op de kabel de komende jaren wordt ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek in het kader van *cyber defence*, omdat bij digitale aanvallen misbruik wordt gemaakt van de Nederlandse digitale infrastructuur en OOG-interceptie op de kabel noodzakelijk kan zijn om dit te onderkennen)."[73] Dit uitgangspunt zal dus ook gelden voor onderzoeken waar de Tijdelijke wet op ziet.

De TIB stelt dat het onduidelijk is wanneer sprake is van verkeer dat oorsprong en bestemming heeft in Nederland. Zij vragen zich specifiek af of verkeer dat in Nederland begint en eindigt, maar een weg via het buitenland aflegt, hieronder valt. Hetzelfde vragen zij zich af ten aanzien van surfgedrag van Nederlanders op social media. De TIB wijst op het ontbreken van concrete indicatoren in de Tijdelijke wet waarmee dit onderscheid gemaakt wordt.

Het opnemen van concrete indicatoren in de Tijdelijke wet is om twee redenen niet wenselijk. Ten eerste lenen dergelijke gegevens, die voortdurend aan verandering onderhevig zijn, zich niet voor het wettelijk vastleggen. Daarnaast zou daarmee inzicht worden gegeven in de staatsgeheime informatie, namelijk het actuele kennisniveau en modus operandi van de diensten. Overigens is het niet mogelijk om op voorhand en categorisch gegevensstromen uit te sluiten van interceptie, bijvoorbeeld op basis van technische eigenschappen, zoals de oorsprong of bestemming van communicatie of de soort (streaming)dienst die wordt aangeboden.

De TIB stelt dat de Tijdelijke wet een wettelijke grondslag introduceert voor het onder voorwaarden delen van (ongeëvalueerde) bulkdata met buitenlandse partnerdiensten. De Wiv 2017 bevat volgens de TIB op dit moment geen specifieke bepaling die dat mogelijk maakt.

[73] *Kamerstukken II* 2017/18, 34 588, nr. 70.

Zoals ook is aangegeven in reactie op vragen van de fractie van GroenLinks-PvdA is het onjuist dat de Wiv 2017 geen specifieke bepaling zou bevatten die het delen van (ongeëvalueerde) bulkdata met buitenlandse diensten mogelijk maakt en dat in de Tijdelijke wet hiervoor een grondslag wordt geïntroduceerd. De artikelen 62, 64 en 89 van de Wiv 2017 bevatten een grondslag voor de diensten om ongeëvalueerde gegevens te delen met buitenlandse diensten. Ook bij toepassing van de Tijdelijke wet is dit de grondslag voor het delen van gegevens met buitenlandse diensten en wordt er niks aan gewijzigd.

Ook verwijst de TIB naar het advies van de Raad van State die adviseerde de mogelijkheid tot het delen van ongeëvalueerde gegevens afkomstig uit de bevoegdheid tot verkennen uit het wetsvoorstel te schrappen. De TIB stelt dat de bezwaren van de Raad van State aan de orde blijven.

Vooropgesteld wordt dat de mogelijkheid om ongeëvalueerde gegevens afkomstig uit de bevoegdheid tot verkennen ten behoeve van technisch onderzoek te delen met buitenlandse diensten voor de diensten in internationale samenwerkingsrelaties en voor onze onderzoeken onmisbaar is. Zoals aangegeven in antwoord op vragen van de leden van de fractie van de ChristenUnie, de fractie van GroenLinks-PvdA en de fractie van de PvdD bevat de Tijdelijke wet voor deze vorm van internationale samenwerking diverse beperkingen en waarborgen.

De TIB stelt dat de Wiv 2017 de bevoegdheid tot bijschrijven 'koppelt' aan de persoon of organisatie waarop binnen de toestemming wordt ingezet en dat de minister bij het verlenen van die toestemming niet zonder meer ook toestemming heeft verleend voor het bijschrijven van infrastructuur die ook door anderen wordt gebruikt.

Dat klopt en zal onder de Tijdelijke wet ook niet anders worden. Er is geen sprake van dat *zonder meer* toestemming wordt verleend voor het bijschrijven van een infrastructuur die ook door anderen wordt gebruikt. Dat mag alleen als het target waarvoor al een door de TIB als rechtmatig beoordeeld toestemmingsverzoek loopt, gebruik is gaan maken van deze infrastructuur. En dan nog mogen kenmerken uitsluitend binnen de grenzen van het door de TIB als rechtmatig beoordeelde toestemmingsverzoek. Zo moet voldaan worden aan de eisen van noodzaak, proportionaliteit en subsidiariteit. De CTIVD houdt bindend toezicht hierop.

10. De TIB stelt dat bij het bijschrijven van niet-exclusieve servers al het verkeer van de andere gebruikers van en naar die servers als bijvangst door de diensten kan worden opgeslagen en bewaard. Dit heeft volgens de TIB gevolgen voor de weging van de proportionaliteit en de TIB zal nadrukkelijk bezien of deze voldoende garanties bevatten dat de data van de overige legitieme gebruikers op geen enkele wijze ter beschikking komt in het inlichtingenproces van de diensten.

Deze elementen uit de werkwijze van de diensten horen bij de verdere verwerking van gegevens en vallen dus onder het toezicht van de CTIVD. Dat geldt zowel voor de bijschrijving, als de omgang met deze gegevens. Het is daarbij een beschreven praktijk die niet aansluit bij de werkwijze van de diensten. Het bijschrijven van kenmerken gebeurt alleen als wordt voldaan aan de vereisten van noodzaak, gerichtheid, proportionaliteit en subsidiariteit. Vervolgens wordt bepaald welke gegevens ontsloten moeten worden voor inlichtingenonderzoeken. En de wijze waarop de diensten vervolgens met verworven gegevens omgaan wordt onder andere bepaald door het relevantieregime. Genoemde gegevens moeten zo spoedig mogelijk op hun relevantie worden beoordeeld en moeten anders worden vernietigd. Wanneer van een bijgeschreven server gegevens worden overgenomen waarvan wordt vastgesteld dat deze niet relevant zijn voor het onderzoek of enig ander lopend onderzoek van de desbetreffende dienst, worden deze gegevens terstond vernietigd.

De Tijdelijke wet bevat volgens de TIB geen waarborgen ten aanzien van de legitieme gebruikers van de gedeelde of gehackte servers, evenmin voor de gebruikers van niet-exclusief gebruikte getapte communicatiemiddelen.

De bescherming van de rechten en belangen van zowel betrokken actoren als derden wordt onder de Tijdelijke wet niet minder, maar juist beter.

Nu zou voor overnemen van een dergelijke server een verzoek bij de TIB worden gedaan. Na verkregen toestemming en rechtmatigheidsoordeel zijn de eisen van de Wiv 2017 van toepassing. Onder de Tijdelijke wet wordt het mogelijk een dergelijke server bij te schrijven. Daarbij gelden zowel de eisen van de Wiv 2017 (inclusief hierboven eerder beschreven toestemmingsaanvraag die door de TIB als rechtmatig moet zijn beoordeeld) én de eisen die de Tijdelijke wet daaraan toevoegt, zie artikel 5, 9 en 10 van de Tijdelijke Wet. Zo komt er bindend toezicht van de CTIVD op de bijschrijving. Dat bindende toezicht op gegevensverwerking is er niet onder de Wiv 2017.

De Tijdelijke wet voorziet alleen een bulkdataregime voor bulkdatasets die zijn verkregen middels de inzet van bijzondere bevoegdheden. Hierdoor ontstaat een verschil in waarborgenniveau ten aanzien van de bescherming van fundamentele rechten van burgers op basis van de manier waarop een bulkdataset is verkregen en niet op basis van de omvang van de inbreuk op de grondrechten van burgers. Voor de TIB en CTIVD is niet begrijpelijk waarom dit onderscheid gemaakt zou moeten worden.

In reactie op vragen van de fractieleden van GroenLinks-PvdA is hiervoor reeds het volgende geantwoord. Er wordt toegewerkt naar een uniform regime voor bulkdatasets. Nu wordt een acuut knelpunt opgelost, namelijk de relevantiebeoordelingstermijn voor bulkdatasets verkregen met bijzondere bevoegdheden. Daarnaast blijft de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 onverkort van kracht, waarmee afhankelijk van de aard van de set na 1, 2 of 3 jaar moet worden bezien of een set verworven met algemene bevoegdheden nog langer door de diensten mag worden gebruikt. Deze regeling aanpassen is op dit moment niet uitvoerbaar. Bulkdatasets die met algemene bevoegdheden zijn verworven, zijn op een andere wijze ontsloten op de systemen van de diensten dan de bulkdatasets die met bijzondere bevoegdheden zijn verkregen. Dit gelijkschakelen zou betekenen dat bulkdatasets die met algemene bevoegdheden zijn verworven in hetzelfde systeem opgenomen moet worden als bulkdatasets die met bijzondere bevoegdheden zijn verworven. Eén bulkregime, waarbij de sets dus in de interne systemen van de diensten gelijk worden ontsloten, betreft een zeer omvangrijke IT-operatie en heeft gevolgen voor het implementatietraject. Een dergelijke ingrijpende operatie is niet passend voor een Tijdelijke wet die urgente problematiek adresseert en is dus niet uitvoerbaar op dit moment. Met de herziening van de Wiv 2017 zal in lijn met de ECW-aanbevelingen een geheel nieuw bulkstelsel opgenomen worden.

De TIB constateert onder verwijzing naar de ECW en het advies van de Raad van State dat De Tijdelijke wet geen fatale bewaartermijn bevat. Het Europees Hof voor de Rechten van de Mens heeft al eerder uitgesproken dat het wenselijk is een zo kort mogelijke bewaartermijn op te nemen in wet- en regelgeving. Een ongelimiteerde bewaartermijn zou een punt kunnen vormen dat aan de orde komt bij de proportionaliteitstoets door de TIB.

Zoals ook aangegeven in reactie op de vragen van de ChristenUnie-fractie en de PvdD-fractie heeft de Raad van State geadviseerd te voorzien in een wettelijke eindtermijn met daarbij tevens een nauwkeurig begrensde mogelijkheid om daarvan bij wijze van uitzondering af te wijken indien dringende redenen met het oog op de nationale veiligheid dat strikt noodzakelijk maken. Daaraan is in het wetsvoorstel gevolg gegeven, voorzien van bindend toezicht door de CTIVD.

Voor wat betreft de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) wordt opgemerkt dat het Hof in een concrete zaak het stelsel als geheel in aanmerking neemt en daarbij beziet of het stelsel voldoende waarborgen bevat die in hun onderlinge samenhang adequate en effectieve garanties bieden tegen willekeur en het risico

van misbruik. Hoewel het Hof belang hecht aan een zo kort mogelijke bewaartermijn, stelt het Hof niet de eis dat altijd sprake moet zijn van een vaste of fatale termijn.

Overigens gaat de TIB hier ook voorbij aan het feit dat dit een Tijdelijke wet is, die naar zijn aard een beperkte duur zal kennen. Op grond daarvan kan een ongelimiteerde bewaartermijn niet aan de orde zijn. Tot slot verdient opmerking dat de beoordeling of er sprake is van een rechtmatig opnieuw vastgestelde eindtermijn door de CTIVD plaatsvindt.

De TIB stelt ten aanzien van de beroepsprocedure dat met toetsing door de TIB reeds voorzien is in een vorm van voorafgaande rechterlijke toetsing.

Zoals ook aangegeven in reactie op de vragen van de leden van de PvdD-fractie is de TIB niet belast met rechterlijke toetsing. Aanleiding voor de introductie van de TIB in de Wiv 2017 was de modernisering van de bijzondere bevoegdheden van de diensten en de noodzaak om deze gepaard te laten gaan met een onafhankelijke bindende toets voorafgaand aan de inzet van de bevoegdheden die in potentie kunnen leiden tot de zwaarste inbreuk op de persoonlijke levenssfeer. Gekozen is voor een gespecialiseerde commissie, waarin kennis en expertise worden gebundeld en die volledig onafhankelijk is. De TIB voldoet volledig aan de eisen die ingevolge het EVRM en de daarmee samenhangende jurisprudentie worden gesteld. Van rechterlijke toetsing is evenwel geen sprake.

Ook is de TIB verbaasd dat er geen beroepsprocedure wordt voorgesteld ten aanzien van de beslissingen die nu worden genomen door de rechtbank Den Haag ten aanzien van de inzet van bijzondere bevoegdheden op advocaten en journalisten, ook niet voor zover die inzet onder het bereik van de Tijdelijke wet zou vallen.

Er is een wezenlijk verschil tussen de taak van de rechtbank Den Haag, die toestemming verleent, en de taak van de TIB, die een reeds verleende toestemming toetst. Juist in het laatste geval kan een verschil van mening ontstaan tussen de minister en de TIB over de uitleg of toepassing van de wet. Bij de herziening van de Wiv 2017 zal het gehele stelsel van toetsing en toezicht (alsmede beslissingen inzake de behandeling van klachten en vermoedens van misstanden) en de rol van de rechter daarbij opnieuw en in onderlinge samenhang worden bezien.

Ook merkt de TIB op dat de beroepsprocedure bij de Raad van State slechts openstaat voor één partij, de minister. Andere belanghebbenden die door een beslissing mogelijk worden geraakt (degene op wie de inzet van de bevoegdheden ziet, al dan niet vertegenwoordigd door NGO's) kunnen geen beroep instellen.

Zoals aangegeven in antwoord op vragen van de PvdD-fractie voorziet de Tijdelijke wet in de mogelijkheid om in onderzoeken van de diensten een rechterlijke uitspraak te verkrijgen inzake geschillen tussen de verantwoordelijke minister en de afdeling toezicht van de CTIVD of de TIB over de rechtmatigheid van de oordelen over de toepassing van bijzondere bevoegdheden door de diensten. Het instellen van beroep is inderdaad voorbehouden aan de verantwoordelijke minister omdat niet valt in te zien tegen welke beslissingen de TIB of CTIVD de mogelijkheid zou moeten hebben om in beroep te gaan.

De burger is geen partij in de procedure en kan dat ook niet zijn. De beslissingen waartegen beroep bij de Afdeling bestuursrechtspraak kan worden opengesteld, betreffen beslissingen inzake operationele activiteiten van de diensten. Dergelijke activiteiten hebben uit de aard der zaak een staatsgeheim karakter, zijn niet openbaar en lenen zich niet voor betrokkenheid van derden. Dit is reeds uitgebreid toegelicht in de nota naar aanleiding van het verslag.[74] Burgers en NGO’s kunnen zich in geval van klachten over het optreden van de AIVD en de MIVD overigens altijd wenden tot de afdeling klachtbehandeling van de CTIVD

[74] Kamerstukken II, 2022–23, 36 263, nr. 9, p. 73

die bindend kan oordelen. Deze procedure voorziet in een effectief en daadwerkelijk rechtsmiddel als bedoeld in artikel 13 EVRM.

Voor de TIB is het een gegeven dat zij, conform Europese jurisprudentie, een volledige rechtmatigheidstoets moet uitvoeren. Daarbij hoort een volle toetsing op de gronden van noodzaak, proportionaliteit en subsidiariteit. Ten aanzien van de proportionaliteitstoets bij OOG-interceptie bevat het wetsvoorstel twee elementen die betrokken moeten worden bij de proportionaliteitstoets, naast andere elementen die hierin moeten worden betrokken, waaronder de feitelijke inbreuk die het voorgestelde middel heeft op de grondrechten van burgers.

Zoals aangegeven in reactie op de vragen van de leden van de fractie van GroenLinks-PvdA, de fractie van D66 en de fractie van de PvdD is in de brief aan de voorzitter van de Tweede Kamer van 24 oktober 2023 aangegeven dat artikel 7 van het wetsvoorstel, ook na aanname van het amendement van de leden Bisschop (SGP) en Van der Graaf (ChristenUnie), richting geeft aan de proportionaliteits- en gerichtheidstoets. Door de woorden ‘met name’ te laten vervallen wordt sterker tot uitdrukking gebracht dat specifiek deze aspecten betrokken worden. Dat laat onverlet dat uiteindelijk wel voldaan dient te worden aan de uit het EVRM en de jurisprudentie daarop voortvloeiende eisen, zoals de toets op subsidiariteit. Volgens de regering is het amendement dan ook niet te zien als een beperking van de proportionaliteitstoets.

De TIB ziet dat de diensten de wens hebben om kabelinterceptie uit te voeren op een wijze die de proportionaliteit van het middel onder druk zet. Dit zou kunnen worden 'hersteld' als een zeer gerichte filtering en tijdige vernietiging van data zal plaatsvinden. Bij het uitblijven daarvan is niet ondenkbaar dat de TIB en diensten van mening blijven verschillen over wat een proportionele inzet van dit middel is in een democratische samenleving.

Wij zijn niet van oordeel dat de beoogde werkwijze van de diensten onder de Tijdelijke wet een proportionele inzet van kabelinterceptie onder druk zet. Integendeel, onder de Tijdelijke wet is en blijft de proportionaliteit als kernbegrip bij de inzet van bevoegdheden van kracht. Bovendien, zoals aangeven in antwoorden op vragen van de fractieleden van GroenLinks-PvdA betreft OOG-interceptie een ketenbenadering. Een belangrijk onderdeel daarvan is graduele benadering van inbreuken bij de diverse handelingen die vallen onder OOG-interceptie. Bij elke fase in deze keten vindt er een TIB-toets plaats. Daarnaast vindt er al bij de eerste fase van verwerving en opslag van gegevens de (eerste) filtering plaats, waarbij een groot deel van de gegevens vernietigd wordt. Tot slot houdt de CTIVD toezicht op de verdere verwerking van gegevens.

De TIB voert ook een volledige proportionaliteitstoets uit ten aanzien van hackoperaties door de diensten. Per brief van 31 maart 2023 hebben de toenmalig minister van BZK en de minister van Defensie uiteengezet dat de Tijdelijke wet geen beperking van de proportionaliteitstoets zal betekenen. Onderdeel van deze proportionaliteitsafweging bij hackoperaties is of door de inzet van het middel inbreuken worden gemaakt op de fundamentele rechten van burgers en of de inzet van het middel zwaarder weegt dan deze inbreuken. Het hacken beperkt zich overigens niet alleen tot een target, maar kan zich ook richten ook op non targets of derden. Ook hun belangen worden bij de beoordeling betrokken, aldus de TIB.

Zoals aangegeven in reactie op de vragen van de leden van de fractie van GroenLinks-PvdA staat de regering achter haar standpunt zoals verwoord in de brief d.d. 31 maart 2023. De regering heeft niet beoogd de wijze waarop de TIB de proportionaliteitstoets uitvoert in te perken. Wel is beoogd te verduidelijken hoe de TIB op het moment van het verzoek om toestemming voor inzet van de bevoegdheid bekende risico’s in haar proportionaliteitstoets kan betrekken.

Tot slot stelt de TIB dat de wet geen duidelijkheid geeft wanneer sprake is van een land met een offensief cyberprogramma. Dat zou 'ad hoc' bepaald moeten worden en dus mogelijk geschillen kunnen opleveren. Het is aan de diensten te kiezen of zij een verzoek om

toestemming willen indienen op basis van de Tijdelijke wet of op basis van de Wiv 2017 waardoor 'geshopt' kan worden op zoek naar de vorm die het laagste niveau van toezicht met zich meebrengt.

In antwoord op vragen van de GroenLinks-PvdA-fractie is uiteengezet hoe bepaald wordt of er sprake is van een onderzoek naar een land met een offensief cyberprogramma. Zoals aangegeven in de reactie op de vragen van de leden van de fractie van D66, delen wij stelling van de TIB dat er 'geshopt' zou kunnen worden naar de laagste vorm van toezicht niet. Er is geen sprake van een laagste of een hoogste vorm van toezicht.

De hiervoor gegeven uitleg is onderdeel van de parlementaire geschiedenis en beoogt duidelijkheid te verschaffen over de uitleg van de Tijdelijke wet zodat een beroepsprocedure bij de Afdeling bestuursrechtspraak op dit punt voorkomen kan worden.

Dit wetsvoorstel is in de visie van de ChristenUnie-fractieleden mede tot stand gekomen tegen de achtergrond van de constatering van een aantal knelpunten in uitleg en toepassing van de Wiv 2017. Bepaalde kernbegrippen zijn niet altijd even consistent, helder, techniekonafhankelijk geformuleerd en afgebakend en wanneer er geschillen ontstaan, biedt de huidige wet geen mogelijkheid tot geschilbeslechting. Daarin wordt voorzien in het voorgestelde artikel 13, dat uitsluitend de minister een beroepsmogelijkheid biedt bij de Afdeling bestuursrechtspaak van de Raad van State. Tijdens de behandeling in de Tweede Kamer is in dit verband aandacht gevraagd voor aanbeveling 48 van de Evaluatiecommissie Wiv, waarin het gaat over het betrekken van de rechter voor het doen van richtinggevende uitspraken over de uitleg van wettelijke normen en begrippen.[75] De beroepsmogelijkheid voor de minister is een van de denkbare uitwerkingen, maar een eveneens besproken pendant is de mogelijkheid tot het stellen van prejudiciële vragen. De regering bleek hiervan geen voorstander, maar de leden van de ChristenUnie-fractie vragen hierop toch nog een nadere reflectie.

Voornoemde fractieleden vragen of het juist tegen de geschetste achtergrond van geschillen en onduidelijkheden, in combinatie met potentieel forse inbreuken op grondrechten van burgers, niet verstandig is om een snelle en laagdrempelige rechterlijke betrokkenheid te realiseren, en of juist het tijdelijke karakter van dit wetsvoorstel niet een uitgelezen kans biedt om met zo'n prejudiciële procedure ervaring op te doen die bij de herijking van de Wiv 2017 kan worden betrokken. Wij reageren hierop graag als volgt.

Een prejudiciële procedure is primair bedoeld om een richtinggevende uitspraak te krijgen van de hoogste rechter zodat lagere rechters deze uitspraak in vergelijkbare zaken met dezelfde rechtsvraag kunnen toepassen. Dit bevordert de rechtseenheid. Dat is hier echter niet aan de orde. Uitsluitend de TIB toetst de door de minister verleende toestemmingen op rechtmatigheid, het risico op verschillen in uitleg of toepassing door verschillende instanties speelt derhalve niet. Zoals al vaker is aangegeven, zou de invoering van een prejudiciële procedure daarnaast vergen dat de TIB wordt omgevormd tot rechterlijke instantie dan wel dat dat de taak van de TIB belegd wordt bij een rechter. Beide opties betekenen een fundamentele wijziging van het stelsel en de taken, bevoegdheden en positionering die de betrokken instanties thans op grond van de Wiv 2017 hebben. Een dergelijke fundamentele wijziging leent zich niet voor het opdoen van ervaring met de Tijdelijke wet.

In haar brief van 7 december 2023 zet de TIB uiteen hoe zij aankijkt tegen knelpunten die gesignaleerd zijn in het rapport van de evaluatiecommissie-Jones-Bos, die onder meer betrekking hebben op waarborgen bij kabelinterceptie, toetsing van technische risico's bij hackoperaties, de bewaartermijn, de relevantiebeoordeling bij bulkdatabestanden en de inzet van geautomatiseerde data-analyse.[76]

De PvdD-fractieleden vragen de regering aan te geven op welke punten zij de standpunten van de TIB omtrent de vereiste waarborgen niet deelt en op welke gronden.

---

[75] *Kamerstukken II* 2023/24, 36 263, nr. 35, p. 35-36.
[76] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394.

Voor het antwoord op deze vraag wordt verwezen naar het antwoord dat hiervoor is gegeven op een vergelijkbare vraag van leden van de PVV-fractie waarin werd verzocht om een puntsgewijze reactie op alle kritiekpunten van de TIB.

De fractieleden van de PvdD vragen of indien de minister (optredende voor de diensten) andere standpunten inneemt dan de TIB, in welke gevallen dat aanleiding zal kunnen vormen voor een beroep als bedoeld in artikel 13 van het wetsvoorstel. Aansluitend vragen zij of de regering een opsomming kan geven van de geschilpunten die naar verwachting zullen leiden tot een geschil waarop artikel 13 betrekking heeft. Wij beantwoorden deze vragen graag als volgt.

De beroepsprocedure is in het leven geroepen om zogenaamde "patstellingen" bij de uitleg van de wet tussen enerzijds de voor de diensten verantwoordelijke ministers en anderzijds de TIB en de afdeling toezicht van de CTIVD door een onafhankelijke rechterlijke instantie te laten beslechten. Het ontbreken van een beroepsmogelijkheid in de Wiv 2017 wordt – in navolging van de ECW - als een weeffout gezien in het stelsel, dat op deze manier opgelost wordt. Door middel van de beroepsmogelijkheid kan er een uitspraak worden gevraagd over de invulling van open normen en op welke wijze die vertaald moeten worden naar de operationele, technische praktijk.

Waar het gaat om de gevraagde opsomming van geschilpunten, merken we in algemene zin het volgende op. Sinds de inwerkingtreding van de Wiv 2017 zijn er verscheidende kwesties geweest waarbij er een verschil van inzicht was met de TIB en CTIVD over de invulling van wettelijke begrippen. De verschillen betroffen vooral de uitleg en reikwijdte van wettelijke begrippen, de wijze waarop de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid in de aanvragen moeten worden beschreven en de intensiteit van ex ante toetsing door de TIB. Dit wetsvoorstel beoogt duidelijkheid te verschaffen over de inzet van bepaalde bevoegdheden naar landen met een offensief cyberprogramma, waarmee naar wij verwachten een aantal grote knelpunten kunnen worden weggenomen. Voor zover die zich nog wel gaan voordoen krijgt de Afdeling bestuursrechtspraak van de Raad van State de rol van geschillenbeslechter. Na de inwerkingtreding van de Tijdelijke wet zal de praktijk uitwijzen welke zaken aan de Afdeling ter geschillenbeslechting zullen worden voorgelegd.

De fractieleden van de PvdD vragen of volgt uit artikel 13 van het wetsvoorstel op welke gronden beroep kan worden ingesteld, zo ja, uit welk voorschrift, en zo nee, of het beroep dan beperkt is tot een rechtmatigheidstoetsing en welke gronden de Afdeling bestuursrechtspaak van de Raad van State dan dient te hanteren. Wij reageren hierop graag als volgt.

In de praktijk zal sprake zijn van een geschil tussen de afdeling toezicht van de CTIVD of de TIB enerzijds en de verantwoordelijke minister anderzijds over de vraag of de verleende toestemming dan wel de uitvoering van een bevoegdheid in overeenstemming is met het gestelde bij of krachtens de Wiv 2017, het bepaalde in dit wetsvoorstel en de toepasselijke internationaal- en Europeesrechtelijke normen. Het beroepschrift zal derhalve gronden bevatten ter onderbouwing van het standpunt van de minister inzake een verleende toestemming (bij een oordeel van de TIB) dan wel inzake de uitvoering van de in artikel 12, eerste lid, genoemde bevoegdheden (bij een oordeel van de afdeling toezicht van de CTIVD).

Het staat de Afdeling bestuursrechtspraak vrij om te bepalen op welke wijze en met welke intensiteit zal worden getoetst. Het aan haar voorgelegde geschil, met name het feitencomplex en de gerezen rechtsvragen, zijn daarbij richtinggevend. Wel is de mate waarin de wetgever marges heeft gelaten in dit kader van belang. In de Wiv 2017 kunnen de marges per bevoegdheid verschillen waardoor de toetsingsintensiteit ook voor de TIB en de afdeling toezicht van de CTIVD kan verschillen. Dit betekent logischerwijs ook dat de marges voor de bij de Afdeling bestuursrechtspraak ter toetsing voorliggende oordelen kunnen verschillen. Voor zover er complexe technische aspecten aan de orde zijn kan de Afdeling op grond van artikel 13, tiende lid, altijd deskundigen inschakelen ten behoeve van de oordeelsvorming.

De fractieleden van de PvdD stellen dat geschillen die leiden tot een beroep als bedoeld in artikel 13, betrekking zullen hebben op inbreuken op grondwettelijk of verdragsrechtelijk beschermde grondrechten, en dat maatschappelijke organisaties die de bescherming van grondrechten

nastreven, procesbelang kunnen hebben bij de beoordeling van de (on)rechtmatigheid van de toepassingen als bedoeld in artikel 12, eerste lid en van toestemmingen waarop artikel 13, eerste lid, onder b en c betrekking heeft. De fractieleden vragen of zulke organisaties partij kunnen zijn in een beroep ingevolge artikel 13 en zo ja, uit welke wettelijke voorschriften dat volgt. Ons antwoord op deze vraag luidt dat alleen de minister beroep kan instellen. Dit volgt uit artikel 13, eerste lid, van de Tijdelijke wet.

Aansluitend vragen de fractieleden van de PvdD of, als zulke organisaties geen partij kunnen zijn in een beroep ingevolge artikel 13, dan voor die organisaties de weg open staat van een geding bij de burgerlijke rechter en zo nee, uit welke wettelijke voorschriften dat volgt. Wij beantwoorden deze vraag als volgt.

Indien een burger of organisatie meent dat door de AIVD of de MIVD een onrechtmatige daad is gepleegd, dan kan de zaak aangebracht worden bij de civiele rechter. Ook kunnen zij zich in geval van klachten over het optreden van de AIVD en de MIVD wenden tot de afdeling klachtbehandeling van de CTIVD die bindend kan oordelen.

De fractieleden van de PvdD vragen vervolgens of, als de organisaties een rechtmatigheidsoordeel kunnen vragen aan de burgerlijke rechter, deze dan gehouden is om het oordeel van de Afdeling bestuursrechtspraak van de Raad van State te volgen en zo ja, of die organisaties in dat geval – gegeven het feit dat zij niet in het beroep ingevolge artikel 13 konden participeren – een rechtsbescherming hebben die voldoet aan de vereisten die voortvloeien uit het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en andere verdragsrechtelijke voorschriften. Aansluitend vragen de leden of, als de burgerlijke rechter tot een ander oordeel komt dan de Afdeling bestuursrechtspraak van de Raad van State, welke uitspraak dan voorrang heeft. Wij beantwoorden deze vragen graag als volgt.

Zoals hiervoor en in de nota naar aanleiding van het verslag is toegelicht[77], kunnen burgers en maatschappelijke organisaties geen partij zijn in de beroepsprocedure bij de Afdeling, omdat de inzet daarvan een geschil is tussen de betrokken minister en de betrokken toezichthouder over de rechtmatigheid van een operationele activiteit van een dienst die naar zijn aard staatsgeheim en niet-openbaar is. Burgers en maatschappelijke organisaties kunnen zich met klachten over het optreden van de diensten wel wenden tot de afdeling klachtbehandeling van de CTIVD die daarover vervolgens een bindend oordeel kan vellen. Deze procedure voorziet in een effectief en daadwerkelijk rechtsmiddel als bedoeld in artikel 13 EVRM. Dit neemt niet weg dat de burgerlijke rechter in een andersoortige procedure tegen de Staat wordt gevraagd zich uit te laten over een rechtsvraag die vergelijkbaar is met die waarover de Afdeling reeds heeft geoordeeld. In zo'n geval is de Afdelingsuitspraak uiteraard een belangrijk en richtinggevend gegeven waarmee de burgerlijke rechter rekening zal houden - een van de partijen in die civiele procedure kan zich daarop ook beroepen – maar de burgerlijke rechter is formeel niet gebonden aan de eerdere Afdelingsuitspraak.

De fractieleden van de PvdD verwijzen naar de brief van de TIB van 7 december 2023, waarin zij erop wijst dat het beroep voor zover dat gericht is tegen oordelen als bedoeld in artikel 13, eerste lid, onder b en c, in feite een beroep betreft tegen een oordeel van een onafhankelijk orgaan dat in meerderheid bestaat uit leden die ten minste zes jaar ervaring als rechter hebben. De TIB stelt: "In een vorm van voorafgaande rechterlijke toetsing is op deze wijze dus reeds voorzien."[78] De fractieleden vragen de regering hierop te reflecteren. Onze reflectie hierop luidt als volgt.

De TIB toetst vooraf de rechtmatigheid van de inzet van bijzondere bevoegdheden door de AIVD en de MIVD. De TIB is thans een rechtsfiguur *sui generis*; zij voert een voorafgaande en bindende toetsing uit, maar is geen rechterlijke instantie.

Aanleiding voor de introductie van de TIB in de Wiv 2017 was de modernisering van de bijzondere bevoegdheden van de diensten en de noodzaak om deze gepaard te laten gaan met een onafhankelijke bindende toets voorafgaand aan de inzet van de bevoegdheden die in potentie kunnen leiden tot de zwaarste inbreuk op de persoonlijke levenssfeer. Gekozen is voor een

[77] Kamerstukken II 2022/23, 36 263, nr. 9, p. 89.
[78] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 7.

gespecialiseerde commissie, waarin kennis en expertise worden gebundeld en die volledig onafhankelijk is. De TIB voldoet volledig aan de eisen die ingevolge het EVRM en de daarmee samenhangende jurisprudentie worden gesteld. Van rechterlijke toetsing is evenwel geen sprake.

Op pagina 16 van het advies van de Afdeling advisering van de Raad van State en het nader rapport merkt de Afdeling advisering over de toetsing door de Afdeling bestuursrechtspraak van de Raad van State in een beroep als bedoeld in artikel 13 het volgende op:

"*De Afdeling wijst er in dat verband op dat de TIB en de CTIVD gespecialiseerde onafhankelijke instanties zijn. Zij beschikken over de expertises om een goede inschatting te maken van zowel de operationele en technische context van de inzet van een bevoegdheid als van de rechtmatigheid ervan. Zij zijn daartoe beter geëquipeerd dan de Afdeling bestuursrechtspraak, die per definitie op grotere afstand staat en technisch minder is ingevoerd.*"[79]

De leden van de fractie van de PvdD vragen of de regering het met hen eens is dat het aannemelijk is dat de Afdeling bestuursrechtspraak van de Raad van State het bestreden oordeel slechts marginaal zal toetsen, en zo nee, op grond van welke overwegingen de regering tot dat oordeelkomt. Ook vragen de leden hoe dat oordeel zich verdraagt met de opmerking van de Afdeling advisering dat het "in de rede" ligt dat de Afdeling bestuursrechtspraak van de Raad van State "terughoudend zal toetsen".[80] Wij beantwoorden deze vragen graag als volgt.

In haar advies gaf de Afdeling advisering aan dat het in de rede ligt dat de Afdeling bestuursrechtspraak *de operationele en technische context van het gebruik van bevoegdheden* terughoudend zal toetsen. Bij de uitleg van wettelijke begrippen kan een indringender toetsing aangewezen zijn maar ook hier geldt dat sprake kan zijn van ruime beoordelingsmarges. Dat geldt met name ook voor de in de toelichting genoemde toetsingsmaatstaven voor de toepassing van bevoegdheden: noodzaak, proportionaliteit, subsidiariteit en gerichtheid. Voor zover de daarbij behorende belangenafweging samenhangt met de operationele en technische context, kan ook dan aanleiding bestaan voor een (enigszins) terughoudende beoordeling, aldus de Afdeling advisering. Het is aan de Afdeling bestuursrechtspraak om te bepalen op welke wijze en met welke intensiteit zal worden getoetst. Het aan haar voorgelegde geschil, met name het feitencomplex en de gerezen rechtsvragen, zijn daarbij richtinggevend. Wel is de mate waarin de wetgever marges heeft gelaten in dit kader van belang. In de Wiv 2017 kunnen de marges per bevoegdheid verschillen waardoor de toetsingsintensiteit ook voor de TIB en de afdeling toezicht van de CTIVD kan verschillen. Dit betekent logischerwijs ook dat de marges voor de bij de Afdeling bestuursrechtspraak ter toetsing voorliggende oordelen kunnen verschillen.

De fractieleden van de PvdD vragen of, als mag worden aangenomen dat de TIB en de CTIVD vasthouden aan de eerder ingenomen standpunten over de waarborgen die zij uit een oogpunt van bescherming van grondrechten noodzakelijk achten, welke gevolgen dan zijn te verwachten ten aanzien van de uitvoerbaarheid van het wetsvoorstel als aannemelijk is dat de Afdeling bestuursrechtspraak van de Raad van State die standpunten in beginsel zal respecteren en slechts zal ingrijpen indien deze toezichthouders in 'willekeur' tot hun oordeel zijn gekomen. Wij reageren hierop graag als volgt.

Zoals aangegeven in het antwoord op de voorgaande vraag, staat het de Afdeling bestuursrechtspraak vrij om te bepalen op welke wijze en met welke intensiteit zal worden getoetst. De Afdeling toetst aan het gestelde bij of krachtens de Wiv 2017, het bepaalde in dit wetsvoorstel en de toepasselijke internationaal- en Europeesrechtelijke normen. Daarbij kan de Afdeling kijken naar een specifieke casus, maar ook tot de invulling van open normen komen. Indien de Afdeling tot het oordeel komt dat de TIB of de CTIVD een juiste afweging heeft gemaakt om tot een oordeel te komen, dan zijn de diensten daaraan gehouden en dient de uitvoeringspraktijk daarop te worden aangepast.

De fractieleden van de PvdD wijzen op de stelling van de TIB dat zij "in alle fasen van kabelinterceptie moet toetsen in hoeverre sprake is van een zo gericht mogelijke uitvoering van de

[79] Onderstreping in het citaat toegevoegd door de leden van de PvdD-fractie.
[80] *Kamerstukken II* 2022/23, 36 263, nr. 4, p. 16.

interceptie."[81] De fractieleden vragen of de regering dat standpunt onderschrijft. Ook vragen de fractieleden of de regering kan aangeven of en, zo ja, welke onaanvaardbare gevolgen zouden ontstaan indien artikel 6, vierde lid, zou worden ingetrokken. Wij beantwoorden deze vragen als volgt.

De regering onderschrijft het standpunt van de TIB niet. Uit de totstandkoming van de Wiv 2002 en Wiv 2017 blijkt dat het inherent is aan de onderzoeksopdrachtgerichte interceptie, zowel op de kabel als op de ether, dat deze gericht is op het onderzoek in plaats van op personen of organisaties, zoals bijvoorbeeld bij de inzet van de tapbevoegdheid). Bulkverwerving is gericht op het verkrijgen van een informatiepositie bij een dreiging waarvan de targets nog niet of maar deels bekend zijn.

Het gerichtheidsvereiste, dat later werd toegevoegd aan de Wiv 2017, is van toepassing op inzet van alle bijzondere bevoegdheden, ook de bevoegdheid tot inzet van kabelinterceptie. Bij de codificatie van het gerichtheidsvereiste in de toelichting is opgenomen dat bij de beoordeling van de gerichtheid medebepalend is in welke fase het onderzoek zich bevindt. Het bij de toepassing van het gerichtheidscriterium eisen van een (te) scherpe afbakening veronderstelt echter dat de verwerving gericht is op gekende dreiging met gekende targets, en miskent de aard van bulkverwerving.

De afgelopen jaren is gebleken dat het niet mogelijk is voorafgaand aan kennisname van de gegevens, en dus voor uitvoering van OOG-interceptie, valide uitspraken te doen over de aard en kenmerken van de gegevensstromen. De verwachtingen in de praktijk blijken niet te stroken met de technische realiteit, bijvoorbeeld omdat een gegevensstroom niet in gebruik is door een partij waar dit wel wordt verwacht – en de aard van de gegevens daardoor totaal anders kan zijn, of dat de verwachting over een partij juist was maar deze geen of geheel andere typen gegevens transporteert dan verwacht. De verkennende bevoegdheid (onder de Tijdelijke wet maar ook als snapshotbevoegdheid onder de Wiv 2017) is daarom niet bedoeld als verificatie om te controleren of de verwachtingen zich in de praktijk verwezenlijken, maar om meer fundamenteel onderzoek te doen naar de aard en kenmerken van gegevensstromen om aldus vast te stellen of deze kunnen bijdragen aan het beantwoorden van onderzoeksvragen. Daarnaast ontbreekt voorafgaand aan OOG-interceptie de kennis en ervaring om filters te ontwikkelen die de gegevensstroom zo snel mogelijk na het moment van verwerving kunnen reduceren. Dit maakt het noodzakelijk dat de verkenningsfase onderdeel wordt van de ketenbenadering van OOG-interceptie, om na bredere interceptie op grond van de verkennende bevoegdheid daarna gerichter te werk te kunnen gaan.

Omdat de toepassing van de bevoegdheid tot OOG-interceptie ten behoeve van verkennen juist dient om de gerichtheid van OOG-interceptie te versterken, is de eis van gerichtheid bij de uitoefening van de verkenningsbevoegdheid naar zijn aard niet toepasbaar. Daarom is in artikel 6, vierde lid, van het wetsvoorstel het gerichtheidsvereiste hier buiten toepassing verklaard. Als belangrijke waarborg verbiedt dit wetsvoorstel de opbrengst van de verkenning te gebruiken voor inlichtingendoeleinden.

De regering onderschrijft echter wel dat zo duidelijk mogelijk moet worden omschreven welke gegevensstromen worden geïntercepteerd. Dat kan alleen door gegevensstromen van een kabel te intercepteren en daarna op basis van technisch onderzoek te bepalen of en hoe een gegevensstroom kan helpen bij de beantwoording van onderzoeksvragen. Technisch onderzoek kan onder meer betekenen het onderzoek naar de aanwezigheid van voor de onderzoeksvragen van de diensten van belang zijnde communicatie, het vaststellen van de aard van deze communicatie en de gebruikte technische protocollen.

Het gerichtheidsvereiste heeft bij de verkennende bevoegdheid voor OOG-interceptie geen betekenis. De verkenningsbevoegdheid is juist bedoeld om de daadwerkelijke interceptie ten behoeve van het inlichtingenproces zo gericht mogelijk te kunnen toepassen. Deze problematiek is eveneens onderkend door de ECW en de CTIVD.

De fractieleden van de PvdD verwijzen naar de standpunten van de TIB ten aanzien van de controle met betrekking tot het 'bijschrijven niet-exclusieve actorinfrastructuur'.[82] De fractieleden vragen of

[81] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 2.
[82] Brief van de TIB van 7 december 2023 aan de Eerste Kamer met kenmerk 174394, p. 4.

het juist is dat het hacken en het tappen van niet-exclusief gebruikte communicatiemiddelen volgens het wetsvoorstel toelaatbaar is zonder voorafgaande toestemming van de TIB. Wij reageren hierop graag als volgt.

Het is van belang onderscheid te maken tussen de hackbevoegdheid en de bijschrijfmogelijkheid. Voor de inzet van de hackbevoegdheid op basis van artikel 45, eerste lid, onder b, van de Wiv 2017 is toestemming van de minister nodig, die getoetst wordt door de TIB. Het bovenstaande geldt zowel wanneer de in de toestemming genoemde kenmerken exclusief in gebruik zijn door de target van het onderzoek, als wanneer deze kenmerken niet-exclusief in gebruik zijn door de target. Voor het starten van een hackoperatie is dus altijd toestemming van de minister nodig, en deze toestemming wordt altijd getoetst door de TIB. Voor het bijschrijven van geautomatiseerde werken die in niet-exclusief gebruik zijn door het onderwerp/target van onderzoek wordt in artikel 5 van het wetsvoorstel verduidelijkt dat geen nieuwe toestemming van de minister of het diensthoofd nodig is en dus is een rechtmatigheidstoets door de TIB daarbij ook niet aan de orde. De bijschrijving moet wel passen binnen de kaders van de eerder door de minister gegeven toestemming. Het voorgaande is van overeenkomstige toepassing op het tappen van communicatiemiddelen. De afdeling toezicht van de CTIVD wordt terstond geïnformeerd over een bijschrijving, zodat ze daar ook – indien de afdeling dat nodig acht – hun aandacht direct op kunnen richten teneinde de rechtmatigheid daarvan te beoordelen en zo nodig deze te doen beëindigen. De TIB oordeelt vervolgens weer over de kenmerken in de toestemming voor verlenging, waaronder ook kenmerken die eerder zijn bijgeschreven, die na akkoord van de minister aan de TIB ter toetsing worden voorgelegd.

De fractieleden van de PvdD citeren vervolgens de TIB: “Ten aanzien van deze bepalingen krijgt de CTIVD de bevoegdheid om op de feitelijke bijschrijving bindend toezicht te houden.” De fractieleden vragen hoe dat praktisch in zijn werk gaat en of de CTIVD zo’n bijschrijving kan verbieden, en wat er gebeurt met gegevens die op die wijze verzameld zijn, als de CTIVD oordeelt dat de bijschrijving ontoelaatbaar moet worden geoordeeld. Wij beantwoorden deze vragen als volgt.

Het is aan de afdeling toezicht van de CTIVD om te bepalen hoe zij feitelijk invulling gaat geven aan haar toezichtsbevoegdheden. De afdeling toezicht van de CTIVD kan concluderen dat er sprake is van een onrechtmatige bijschrijving waardoor de opbrengst uit de bijschrijving onrechtmatig is verkregen. Welke rechtsgevolgen de CTIVD aan deze onrechtmatigheid kan verbinden, is opgenomen in artikel 12 van het wetsvoorstel. Indien de CTIVD oordeelt dat de bijschrijving onrechtmatig is geweest, kan zij oordelen dat de bijschrijving moet worden stopgezet en dat eventueel verkregen gegevens terstond verwijderd en vernietigd te worden.

De leden van de PvdD-fractie wijzen erop dat in het voorgestelde artikel 7 twee aspecten worden genoemd. De fractieleden vragen of de regering het oordeel van de TIB onderschrijft, dat de bepaling zo moet worden gelezen dat in ieder geval die twee aspecten betrokken dienen te worden in de proportionaliteitstoets en dat die toets voor het overige een volle toets is, en zo nee, op welke gronden de regering tot dat oordeel komt. Ons antwoord op deze vraag luidt als volgt.

Zoals aangegeven in de reactie op de vragen van de leden van de fractie van GroenLinks-PvdA en de fractie van D66 is in de brief aan de voorzitter van de Tweede Kamer van 24 oktober 2023 aangegeven dat artikel 7 van het wetsvoorstel, ook na aanname van het amendement van de leden Bisschop (SGP) en Van der Graaf (ChristenUnie), richting geeft aan de proportionaliteits- en gerichtheidstoets. Er is voor deze criteria gekozen aangezien hiermee inzage kan worden gegeven in de mate van gerichtheid van de verwerving en de (direct daaropvolgende) verwerking (en dus reductie) van de gegevens, en daarmee ook de proportionaliteit van de inzet zorgvuldig kan worden getoetst. Een omschrijving van de gegevensstromen geeft immers een zekere mate van inzicht in de data die verworven wordt, bijvoorbeeld door aan te geven op welke klantkanalen geïntercepteerd zal worden. Door de woorden ‘met name’ te laten vervallen wordt sterker tot uitdrukking gebracht dat specifiek deze aspecten betrokken worden. Dat laat onverlet dat uiteindelijk wel voldaan dient te worden aan de uit het EVRM en de jurisprudentie daarop voortvloeiende eisen, zoals noodzakelijkheid en proportionaliteit. Volgens de regering wordt de TIB dan ook niet beperkt in haar proportionaliteitstoets.

De leden van de Volt-fractie merken op dat de tijdelijke wet het mogelijk maakt om in beroep te gaan bij de Afdeling bestuursrechtspraak van de Raad van State. Dit is volgens de leden vrij uniek in Europa. Zij vragen hoe de regering ervoor zorgt dat de veiligheid van de data en de privacy van het betrokken personeel gewaarborgd worden. Wij beantwoorden deze vraag graag als volgt.

Bij het vormgeven van het wetsvoorstel hebben meerdere overleggen, ketentesten en uitvoeringstoetsen plaatsgevonden, met de stelselpartners, waaronder de Afdeling bestuursrechtspraak van de Raad van State. De uitkomsten van die overleggen zijn betrokken bij het wetsvoorstel. Daarnaast is reeds gestart met de voorbereiding van de implementatie van de Tijdelijke wet. Bij dit implementatietraject wordt ook de Afdeling bestuursrechtspraak van de Raad van State betrokken en vinden hierover overleggen met hen plaats. De veiligheid van de data en de privacy van het betrokken personeel is hierbij onderwerp van gesprek.
Om het staatsgeheime karakter van de gegevens te waarborgen zullen de noodzakelijke maatregelen worden getroffen. Overigens heeft de Afdeling bestuursrechtspraak reeds ervaring met AIVD- en MIVD-gerelateerde zaken en de omgang met staatsgeheime informatie die daaraan inherent verbonden is. De benodigde randvoorwaarden in personele, organisatorische, technische en financiële zin zullen in overleg met de Afdeling bestuursrechtspraak van de Raad van State worden gerealiseerd.

Een jaar na inwerkingtreding zal een invoeringstoets worden uitgevoerd en tevens wordt er periodiek een uitvoeringsverslag opgesteld. De resultaten hiervan zullen vervolgens worden betrokken bij de herziening van de Wiv 2017. Conform de motie Hammelburg zal één jaar na inwerkingtreding van de Tijdelijke wet een invoeringstoets worden uitgevoerd die ziet op de balans tussen passende waarborgen en effectieve taakuitvoering.[83]

De fractieleden van Volt stellen dat de bewaartermijn iedere keer met 1,5 jaar verlengd kan worden door de toezichthouder. Technisch gezien is het dus mogelijk om bulkdata voor eeuwig te bewaren, zolang deze als relevant worden gezien door de CTIVD, aldus de Volt-fractieleden. Zij vragen in hoeverre het technisch mogelijk is dat het bewaren van bulkdata iedere keer verlengd wordt en datasets daardoor voor altijd bewaard zullen worden. Voorts vragen zij of er bij verlengingen ook wordt gekeken of de bulk kleiner gemaakt kan worden, en waarom wel of waarom niet. Tot slot vragen zij of de toetsingscriteria bij een verlenging van de bewaartermijn veranderen en waarom wel of waarom niet. Wij reageren hierop graag als volgt.

In de Tijdelijke wet wordt voorzien van een mogelijkheid onder voorwaarden, voor bulkdatasets waarvan de eindtermijn van anderhalf jaar verloopt, een nieuwe eindtermijn van een jaar te stellen voor het gebruik van een bulkdataset in het geval van dringende redenen met het oog op de nationale veiligheid en dus niet met anderhalf jaar zoals in de vraag is opgenomen. Door deze bepaling kunnen de diensten blijven beschikken over voor hen zeer relevante informatie, zolang onderbouwd kan worden dat het onder andere noodzakelijk, proportioneel en subsidiair is. Hierbij wordt ook meegenomen of er reeds een reductie van de bulkdataset heeft plaatsgevonden. De afdeling toezicht van de CTIVD zal bindend toezicht houden op het vaststellen van een nieuwe eindtermijn. Het kan voorkomen dat sets binnen anderhalf jaar vernietigd worden. Dit kan komen doordat de set niet waardevol blijkt te zijn voor lopende onderzoeken van de diensten. Bij elke vaststelling van een nieuwe eindtermijn, dient te worden voldaan aan de wettelijke criteria zoals neergelegd in artikel 14ba, tweede lid, van het wetsvoorstel. Dit betekent dat elke keer goed onderbouwd moet worden waarom de betreffende bulkdataset nog relevant is en het behoud van de set nodig is voor de nationale veiligheid. En ook of een langere beschikbaarheid van de bulkdataset geen disproportionele beperking inhoudt van het recht op bescherming van de persoonlijke levenssfeer van de personen waarvan gegevens in de bulkdatasets zijn opgenomen.

De fractieleden van Volt wijzen erop dat in 2011 de Eerste Kamer de evaluatie van de Richtlijn dataretentie heeft behandeld.[84] Zij vragen in hoeverre het wetsvoorstel strookt met de punten in de

[83] *Kamerstukken II 2022/23, 36 26, nr. 31.*
[84] Dossier E110022 op de EuropaPoort:
https://www.eerstekamer.nl/eu/edossier/e110022_evaluatierapport_over_de.

samenvatting ten aanzien van deze evaluatie[85] die destijds door de Eerste Kamer is opgesteld (zie in het bijzonder pagina 3 voor de implicaties). Wij beantwoorden deze vraag als volgt.

De Dataretentierichtlijn bevatte een bewaarplicht voor gegevens van aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk die door hen gegenereerd of verwerkt werden ten behoeve van onderzoek, opsporing en vervolging van ernstige criminaliteit. In Nederland werd in de wet van 18 juli 2009 een algemene bewaarplicht voor telecommunicatiegegevens geïntroduceerd voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[86] Deze bewaarplicht gold nadrukkelijk niet voor nationale veiligheid. In 2014 heeft het Hof van Justitie de Dataretentierichtlijn ongeldig verklaard wegens strijdigheid met het EU recht, meer in het bijzonder het Handvest van de grondrechten van de EU.[87] Het Hof oordeelde dat, gelet op alle overwegingen, de wetgever van de EU met de vaststelling van de richtlijn dataretentie de door het evenredigheidsbeginsel gestelde grenzen had overschreden die in het licht van het Handvest van de grondrechten in acht genomen moeten worden. Vervolgens is de Nederlandse wetgeving rond de bewaarplicht door de rechter buiten werking gesteld in een vonnis van de voorzieningenrechter Den Haag van 11 maart 2015.[88] Sindsdien geldt geen bewaarplicht meer en is geen sprake van de genoemde implicaties.

In algemene zin geldt dat de Tijdelijke wet, evenals de Wiv 2017, voldoet aan de eisen die daaraan vanuit het EVRM worden gesteld. Bij de Wiv 2017 is daar in de memorie van toelichting uitvoerig aandacht aan besteed en hetgeen dat is gesteld, geldt evenzeer voor de Tijdelijke wet, zij het met inbegrip van hetgeen specifiek in het kader van de behandeling van de Tijdelijke wet ter zake naar voren is gebracht.[89]

De leden van de Volt-fractie constateren dat het Hof van Justitie van de Europese Unie in 2014 oordeelde dat huidige richtlijnen met betrekking tot de bewaarplicht van bulkdata ongeldig zijn.[90] De leden vragen in hoeverre de bewaartermijn van 1,5 jaar standhoudt bij dit Hof. Wij beantwoorden deze vraag als volgt.

Het arrest waarnaar deze leden verwijzen betrof de bewaarplicht voor aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten van verkeers- en locatiegegevens ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. De in de Tijdelijke wet opgenomen eindtermijn voor het gebruik van bulkdatasets geldt voor de verdere verwerking in het kader van de nationale veiligheid van door de diensten verworven bulkdatasets en vloeit op geen enkele wijze voort uit EU-regelgeving. Het arrest van het EU Hof van Justitie heeft derhalve geen gevolgen voor deze regeling. Nationale veiligheid is krachtens artikel 4, tweede lid, van het EU-Verdrag immers de uitsluitende verantwoordelijkheid van de lidstaten.

5. Grondrechtelijke en mensenrechtelijke aspecten

De leden van de PVV-fractie wijzen erop dat in de memorie van toelichting wordt gesproken over situaties waarbij sprake is van "inbreuk op de privacy van andere gebruikers".[91] Deze leden vragen of de regering kan aangeven in hoeverre deze inbreuken gevolgen kunnen hebben voor deze "andere gebruikers". Wij beantwoorden deze vraag graag als volgt.

Dat hangt sterk af van de omstandigheden van het geval. In algemene zin kan worden gesteld dat de inbreuk binnen de grenzen moet blijven van de aanvraag waarvoor toestemming is gegeven. Deze bandbreedte wordt onder meer ingevuld door de onderbouwing van de vereisten van noodzaak, gerichtheid, subsidiariteit en proportionaliteit. Dit laatste vereiste vergt verantwoording van de afweging van het onderzoeksbelang van de dienst ten opzichte van de inbreuk op de privacy die optreedt bij toepassing van de aangevraagde bevoegdheid. Die inbreuk moet immers proportioneel zijn.

---

[85] https://www.eerstekamer.nl/eu/intern_stuk/20110428/uitgebreide_samenvatting_e110022/document.
[86] Stb. 2009, 333.
[87] Gevoegde zaken Digital Rights Ireland en Seitlinger (zaken C-293/12 en 594/12).
[88] ECLI:NL:RBDHA:2015:2498.
[89] *Kamerstukken II* 2022/23, 36 263, nr. 3, p. 39-42
[90] https://ecer.minbuza.nl/-/dataretentierichtlijn-ongeldig.
[91] *Kamerstukken II* 2022/23, 36 263, nr. 3, p. 7.

De fractieleden van de PVV vragen of de regering kan aangeven in hoeverre diensten in zulke gevallen 'bijvangst' van informatie kunnen gebruiken voor andere doelen dan onderzoek naar landen met een offensief cyberprogramma, bijvoorbeeld als bij een interceptie materiaal wordt aangetroffen over ernstige strafbare feiten, terroristische activiteiten of drugshandel of bij bijvoorbeeld gegevens over (grootschalige) belastingfraude. De leden vragen hoe dan met dergelijke informatie wordt omgegaan (al dan niet van Nederlandse burgers). Wij reageren hierop graag als volgt.

Zoals ook onder de Wiv 2017 het geval is, kunnen gegevens die in een onderzoek rechtmatig zijn verkregen ook gebruikt worden voor andere lopende onderzoeken als de gegevens relevant blijken. Meer specifiek betekent dat dus dat als gegevens zijn verworven door de inzet van de hackbevoegdheid onder de Tijdelijke wet voor een onderzoek naar bijvoorbeeld Rusland, deze gegevens ook mogen worden verwerkt voor een contraterrorisme-onderzoek. De AIVD en MIVD verrichten hun taken enkel en alleen in het kader van de nationale veiligheid. Artikel 13 van de Wiv 2017 verbiedt de diensten strafbare feiten op te sporen. De diensten doen geen onderzoek naar de genoemde voorbeelden, met dien verstande dat terroristische activiteiten wel voorwerp van onderzoek kunnen zijn op grond van de Wiv 2017. Relevante gegevens kunnen gedeeld worden met bijvoorbeeld het Openbaar Ministerie of de Belastingdienst, zodat deze instellingen – in het kader van de eigen taakuitvoering – kunnen handelen.

De fractieleden van de PVV roepen in herinnering dat bij de technische briefing van 14 november 2023 in de Eerste Kamer door de directeur Constitutionele Zaken en Wetgeving van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties werd aangegeven dat er "geen focus ligt op Nederlandse burgers". Deze fractieleden vragen of de regering nader kan duiden in hoeverre en onder welke voorwaarden Nederlandse burgers wel betrokken kunnen raken in een onderzoek. Wij beantwoorden deze vraag als volgt.

De uitleg van de directeur CZW was bedoeld om aan te geven dat de reikwijdte van de Tijdelijke wet ziet op landen met een offensief cyberprogramma en dus is gericht op het buitenland. Dat geldt zeker voor de bevoegdheid tot kabelinterceptie. Die bevoegdheid is gericht op communicatiestromen die internationaal gegevensverkeer bevatten. Vanwege de technische inrichting van het internet en de wijze waarop gegevensstromen daarop plaatsvinden, kan niet uitgesloten worden dat daarin ook gegevens van communicatieverkeer van Nederlandse burgers in zitten. De interceptie is daarop echter niet gericht. Dit is ook toegelicht in antwoord op vragen van de fractieleden van de PvdD over de stelling van de TIB dat volgens de TIB door de minister is toegezegd dat er geen interceptie zal plaatsvinden in het zogeheten Nederland-Nederland-verkeer, tenzij voor *cyber defence*.

Nederlandse burgers kunnen betrokken raken in onderzoeken van de diensten indien ernstige vermoedens bestaan dat zij door de doelen die zij nastreven, dan wel door hun activiteiten aanleiding geven dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen dan de staat. Onderzoek doen naar zulke personen of organisaties is een wettelijke taak van de AIVD (artikel 8, tweede lid, sub a Wiv 2017) waarbij geen onderscheid wordt gemaakt naar nationaliteit. Een voorbeeld waarbij een Nederlandse burger betrokken kan raken in een onderzoek naar een land met een offensief cyberprogramma en daarmee in het regime van de Tijdelijke wet valt is bijvoorbeeld wanneer de dienst een ernstig vermoeden heeft dat die Nederlandse burger het land met een offensief cyberprogramma helpt door bedrijfsgeheimen te delen met dat land, of indien hij onderdeel is van een groot netwerk dat door het land met een offensief cyberprogramma wordt gerund. Dit zijn voorbeelden dat een Nederlandse burger zelf onderdeel uitmaakt van de uitvoering van een offensief cyberprogramma van een land en daarmee onderwerp van onderzoek kan worden van de diensten. Wat hierbij niet moet worden vergeten is dat Nederlandse burgers zelf doelwit kunnen worden van vijandelijke statelijke actoren, namelijk landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen. Hun doelwitten zijn namelijk persoonsgegevens, belangrijke hightech innovaties, politieke standpunten, militaire geheimen, kwetsbaarheden van onze vitale infrastructuur, informatie over dissidenten en nog veel meer. Het gaat dus om economische schade, militaire schade, fysieke schade en/of geopolitieke schade veroorzaakt bij zowel Nederlandse organisaties als ook individuele Nederlanders. Bijvoorbeeld doordat routers van Nederlanders worden gebruikt vanuit Rusland door hackers van de GRU. Of doordat

persoonsgegevens van Nederlandse burgers worden buitgemaakt.

De fractieleden van de ChristenUnie halen aan dat het tijdens de behandeling van het wetsvoorstel in de Tweede Kamer, maar ook tijdens de recent gehouden deskundigenbijeenkomsten in de Eerste Kamer onder meer ging over de bevoegdheid tot het bijschrijven van niet-exclusief in gebruik zijnde actorinfrastructuur. Een zeer wezenlijk kenmerk van het niet-exclusieve karakter is dat ook data worden verkregen van voor het onderzoek volstrekt niet-relevante actoren, terwijl die data wel zeer gevoelig zouden kunnen zijn. Met het oog op de bescherming van de rechten en belangen van niet-betrokken actoren vragen de fractieleden de regering hoe bij toepassing van het voorgestelde artikel 5, tweede lid, de positie van die actoren beschermd en gewaarborgd wordt. Dezelfde vraag geldt waar het gaat om toepassing van de tapbevoegdheid zoals opgenomen in het voorgestelde artikel 9, eerste lid. De fractieleden vragen of hier een rol is weggelegd voor een of beide toezichthouders. Wij reageren hierop graag als volgt.

De bescherming van de rechten en belangen van niet-betrokken actoren wordt op verschillende manieren gewaarborgd. Bij de aanvraag wordt intern beoordeeld of is voldaan aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. Vervolgens wordt melding gedaan bij de afdeling Toezicht van de CTIVD, betreffende de bijschrijving. De CTIVD houdt hier bindend toezicht op. Als er een verlengingsaanvraag wordt gedaan, zullen de bijgeschreven kenmerken onderdeel zijn van de aanvraag en zijn deze dus onderdeel van de toets van de TIB. Al deze waarborgen zijn van toepassing op de art. 5, 9 en 10 van de Tijdelijke wet. Hiermee acht de regering de rechten en belangen van niet-betrokken actoren goed gewaarborgd. Na een interne beoordeling, houdt de CTIVD bindend toezicht op de uitvoering, en op het moment van een verlenging kan de TIB de bijgeschreven kenmerken in haar toets betrekken.

6. Gevolgen verbonden aan de uitvoering van de wet

De fractieleden van GroenLinks-PvdA constateren dat uit de evaluatie en het onderzoek van de Algemene Rekenkamer blijkt dat er bij de Wiv 2017 een aantal uitvoeringsknelpunten onvoldoende in beeld was.[92] Ook nu zijn er volgens deze leden zorgen over de uitvoerbaarheid van de tijdelijke wet. Zij willen in het kader van de rol van de Eerste Kamer graag kennisnemen van de uitvoeringstoets(en) en vragen of de regering bereid is deze te verstrekken. Indien de regering hiertoe niet bereid is, vragen deze leden waarom niet en ontvangen zij graag een reflectie van de regering op hoe dit zich verhoudt tot de expliciete rol van de Eerste Kamer bij het toetsen van de uitvoerbaarheid van wetsvoorstellen. Wij beantwoorden deze vragen graag als volgt.

De regering begrijpt de wens van deze leden om geïnformeerd te worden over onderwerpen die zij van belang acht. De regering heeft er dan ook naar gestreefd om een zo volledig mogelijk overzicht te verstrekken, dit is gebeurd in de memorie van toelichting. Een deel van de informatie is echter gerubriceerd en kan dan ook niet in het kader van deze openbare wetsbehandeling worden verstrekt. Daarnaast zal er gewerkt worden aan een invoeringstoets betreffende de inwerkingtreding van de Tijdelijke wet en een uitvoeringsverslag betreffende de punten waar de diensten tegen aanlopen vanuit de operationele praktijk.

De fractieleden van D66 hebben vernomen uit zowel het evaluatierapport van de commissie-Jones-Bos[93] als het rapport van de Algemene Rekenkamer[94] dat de diensten eigenlijk niet voldoende toegerust waren op de invoering van de Wiv 2017 in 2018. De fractieleden vragen welke organisatorische aanpassingen de regering verwacht te moeten doen om de implementatie van dit wetsvoorstel succesvol te laten zijn. Wij beantwoorden deze vraag als volgt.

De diensten zijn bij de voorbereiding van de Tijdelijke wet intensief bezig geweest met het vaststellen van de uitvoeringseffecten. Dat hebben de diensten gedaan door verschillende uitvoeringstoetsen uit te voeren waarbij ook nadrukkelijk aandacht is besteed aan de gevolgen op IT-gebied en voor de bedrijfsvoering. Concreet vergt de implementatie van de Tijdelijke wet diverse

[92] *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt* (onderzoeksrapport Algemene Rekenkamer), Den Haag: 2021.
[93] *Kamerstukken II 2020/21, 34 588, nr. 88*, bijlage Evaluatie 2020. Wet op de inlichtingen- en veiligheidsdiensten 2017.
[94] *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt* (onderzoeksrapport Algemene Rekenkamer), Den Haag: 2021.

wijzigingen in het IT-landschap van de diensten. Deze wijzigingen zijn in een eerder stadium al geïdentificeerd en ontwikkeld. De diensten hebben voorzien dat extra capaciteit nodig is. Er zal doorlopend gemonitord worden of de diensten voldoende capaciteit hebben of dat er zo nodig een herprioritering moet plaatsvinden.

Ook zal een jaar na inwerkingtreding een invoeringstoets worden uitgevoerd en wordt er periodiek een uitvoeringsverslag opgesteld. Bij deze invoeringstoets wordt al na een korte termijn gekeken naar de uitwerking van deze wet in de praktijk. Er wordt actief gezocht naar knelpunten, niet alleen bij de diensten maar ook bij de toezichthouders en andere betrokkenen bij deze wet. Hierbij kan in het bijzonder ook aandacht worden besteed aan de vraag in hoeverre het voorgestelde stelsel van toetsing en toezicht als geheel zich verhoudt tot de beoogde operationele snelheid en wendbaarheid. Tevens zorgt een uitvoeringsverslag ervoor te monitoren en helder te krijgen in welke veranderende wereld de diensten moeten opereren. Het dreigingsbeeld en technologische vernieuwingen zullen immers ook tijdens het werken onder de Tijdelijke wet veranderen. Zonder daarvoor telkens een wetswijziging nodig te hebben is het van belang de diensten binnen de wettelijke kaders bewegingsvrijheid hebben en de minister zo nodig hier uitspraken aan de kamer over doet en daarnaar gehandeld wordt. Zo is er een sluitend geheel van zicht vooraf op uitvoeringsaspecten en zicht tijdens de uitvoering van deze wet. De resultaten kunnen worden betrokken bij de uitvoering van de Tijdelijke wet, maar nadrukkelijk ook bij de voorbereiding van de herziening van de Wiv 2017.

De leden van de PVV-fractie constateren dat een reden voor het wetsvoorstel is dat de huidige Wiv 2017 zou tekortschieten. Zij vragen of de regering nader onderbouwd kan aangeven in hoeverre met dit wetsvoorstel de diensten nu wel in staat zijn om de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid adequaat te beschrijven. Wij reageren hierop graag als volgt.

De Tijdelijke wet heeft niet direct tot doel de vereisten van noodzaak, proportionaliteit, subsidiariteit en gerichtheid beter te kunnen onderbouwen. Wel beoogt de Tijdelijke wet een helder kader voor de inzet van bestaande bevoegdheden van de diensten te schetsen en deze effectiever in te kunnen zetten in onderzoeken naar landen met een offensief cyberprogramma. De Tijdelijke wet biedt op enkele punten tegelijkertijd wel degelijk handvatten om bij bepaalde bijzondere bevoegdheden de noodzaak, gerichtheid, proportionaliteit en subsidiariteit beter te omschrijven bij zowel de onderbouwing daarvan als de toets daarop. Zo wordt duidelijker dan in de Wiv 2017 aangegeven hoe de OOG-interceptie bevoegdheid gezien moet worden en wat er bij de toetsing voor de inzet ervan meegenomen moet worden. Hierbij wordt expliciet gewezen op de aard van de bevoegdheid. Ook is gewezen op het feit dat de vereisten van gerichtheid en proportionaliteit bij verschillende bevoegdheden een andere invulling vergen en dat ook verschilt per geval en fase van het onderzoek. De criteria zijn geen statische criteria. Daarnaast biedt de Tijdelijke wet verduidelijking over de noodzaak en de aard van de strategische inzet van bevoegdheden, ook wel strategische operaties genoemd.

De leden van de PVV-fractie constateren dat zowel voor onderzoek als toezicht dit wetsvoorstel extra personele inspanning zal vergen. Deze leden vragen de regering gelet op de personeelstekorten in de huidige arbeidsmarkt, aan te geven in hoeverre het wetsvoorstel in dit opzicht uitvoerbaar en handhaafbaar is. Wij beantwoorden deze vraag als volgt.

De benodigde extra capaciteit bij de toezichthouders om te anticiperen op de Tijdelijke wet is al langere tijd onderwerp van gesprek. Met de TIB en de CTIVD zijn vooruitlopend op de inwerkingtreding van de Tijdelijke wet afspraken gemaakt over capaciteitsuitbreiding. Het is de verwachting dat de toezichthouders met deze extra capaciteit hun werk naar behoren kunnen uitvoeren. Met name voor de CTIVD brengt de Tijdelijke wet door de taakuitbreiding extra werkdruk met zich mee. De FTE capaciteit van de CTIVD is met 10 fte uitgebreid. Voor de TIB geldt dat de formatie in overleg met de voorzitter van de TIB met 3 fte wordt uitgebreid. Voor de TIB en de CTIVD zijn de wervings- en selectieprocedures in volle gang. De CTIVD heeft aangegeven ervan uit te gaan dat de uitbreiding van haar taken kan worden gerealiseerd.

Een jaar na inwerkingtreding van Tijdelijke wet wordt een invoeringstoets uitgevoerd en daarnaast wordt periodiek een uitvoeringsverslag opgesteld. Bij deze invoeringstoets wordt al na een korte

termijn gekeken naar de uitwerking van deze wet in de praktijk. De diensten hebben voorzien dat extra capaciteit nodig is. Vast onderdeel van de doorlopende monitoring is de beoordeling van de vraag of de diensten voldoende capaciteit hebben of dat er zo nodig een herprioritering moet plaatsvinden. Daarnaast zijn de diensten, gezien de geleerde lessen van de implementatie van de Wiv 2017 en de daarop genomen acties, reeds financieel voldoende voorbereid op de implementatie van de Tijdelijk wet.

De fractieleden van Volt merken op dat de CTIVD voor de uitvoering van de wet meer personeel nodig heeft. Gezien de arbeidsmarktkrapte en de specifieke eisen die gesteld worden aan het werk, vragen deze fractieleden zich af of de uitvoering op tijd gereed is. Zij vragen hoe de regering ervoor zorgt dat er voldoende gekwalificeerd personeel tijdig is ingewerkt om de wet goed te kunnen uitvoeren.

Voor het antwoord op deze vraag wordt verwezen naar het hiervoor gegeven antwoord op de vraag van de leden van de PVV-fractie over de uitvoerbaarheid en handhaafbaarheid van het wetsvoorstel en het antwoord op de vraag van de leden van de GroenLinks-PvdA-fractie over de wens om het toezicht op peil te houden en de werklast voor de toezichthouders

De fractieleden van Volt merken tot slot op dat de CTIVD heeft aangegeven dat het vinden van passende huisvesting een uitdaging is. Want nu er meer personeel aangetrokken moet worden, is grotere huisvesting nodig. De fractieleden vragen hoe de plannen eruitzien om op tijd tot een passende huisvesting te komen, en hoe de regering ervoor zorgt dat de huisvesting ruim voor de invoering van de wet goed is geregeld. Wij beantwoorden deze vraag als volgt.

Omdat de CTIVD de komende jaren een forse groei zal doormaken, wordt al enige tijd gezocht naar een geschikte huisvestinglocatie voor de CTIVD. Hierbij dient rekening te worden gehouden met het bijzondere karakter van de CTIVD en de aard van de gegevens die door de CTIVD worden verwerkt. Op korte termijn wordt een schetsontwerp afgerond voor de toekomstige huisvesting van de CTIVD, waarna een goede prognose kan worden gegeven van de bouwtijd. Omdat de lange termijn-huisvesting niet direct gerealiseerd zal zijn, wordt ter overbrugging voorzien in een tijdelijke oplossing die ruimte biedt aan minimaal de extra capaciteit om uitvoering te geven aan de Tijdelijke wet. Conform de motie Hammelburg zal één jaar na inwerkingtreding van de Tijdelijke wet een invoeringstoets worden uitgevoerd die ziet op de balans tussen passende waarborgen en effectieve taakuitvoering.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Hugo de Jonge

De minister van Defensie,

drs. K.H. Ollongren