

Vergaderjaar 2022–2023

36 263

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 (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma)

Nr. 4 TWEDE HERDRUK¹

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT²

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 22 juni 2022 en het nader rapport d.d. 28 november 2022, aangeboden aan de Koning door de Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister van Defensie. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt

Blijkens de mededeling van de Directeur van Uw kabinet van 10 mei 2022, nr. 2022001014, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij en in afschrift aan mijn ambtgenoot van Defensie te doen toekomen. Dit advies, gedateerd 22 juni 2022, nr. W04.22.0073/l, bied ik U hierbij aan. Dit nader rapport is mede namens de Minister van Defensie opgesteld.

De tekst van het advies treft u hieronder cursief aan, voorzien van mijn reactie.

Bij Kabinetsmissive van 10 mei 2022, no. 2022001014, heeft Uwe Majesteit, op voordracht van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de Minister van Defensie, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet houdende 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 (Tijdelijke wet onderzoeken AIVD en

¹ I.v.m. enkele tekstuele correcties onder punt 11.

² De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

MIVD naar landen met een offensief cyberprogramma), met memorie van toelichting.

Het wetsvoorstel voorziet in een tijdelijk, van de Wiv 2017 afwijkend regime voor het onderzoek van de AIVD en de MIVD naar landen met een offensief cyberprogramma. Het bestaande regime van de Wiv 2107 belemmert de diensten om dit onderzoek effectief uit te voeren, aldus de toelichting. Het doel van het voorstel is meer operationele snelheid en wendbaarheid mogelijk te maken, terwijl het niveau van toezicht gelijk blijft. Het voorstel verruimt daartoe de inzetmogelijkheden van enkele cyberbevoegdheden, brengt verschuivingen aan in het stelsel van toezicht en creëert voor geschillen tussen de Minister(s) en de toezichthouder(s) een beroepsprocedure bij de Afdeling bestuursrechtspraak van de Raad van State.

Het wetsvoorstel is in belangrijke mate gebaseerd op recente rapportages van de Evaluatiecommissie, de Algemene Rekenkamer en de CITVD. Daarin worden knelpunten gesignaleerd en geanalyseerd met betrekking tot de werking van het bestaande wettelijke regime. Mede gelet op de genoemde rapportages concludeert de Afdeling advisering van de Raad van State dat overtuigend is toegelicht dat het noodzakelijk is de geconstateerde knelpunten op korte termijn te adresseren. Daarbij is van belang dat het gaat om een tijdelijke wet die specifiek is gericht op de serieuze dreiging die uitgaat van landen met een offensief cyberprogramma. Wel acht de Afdeling meer waarborgen in het wetsvoorstel noodzakelijk.

In het wetsvoorstel dient een balans te worden gevonden tussen enerzijds de bescherming van de democratische rechtsstaat door de effectieve inzet van de bevoegdheden van de inlichtingen- en veiligheidsdiensten en anderzijds het waarborgen van de in de Grondwet en verdragen neergelegde grondrechten. Voor dat laatste is effectief toezicht op het werk van de AIVD en de MIVD essentieel.

Met het oog op die noodzakelijke balans moeten de wettelijke waarborgen op een aantal punten worden versterkt. Zij adviseert met het oog daarop het wetsvoorstel dan wel de toelichting aan te passen.

Dit betreft in de eerste plaats de voorgestelde bevoegdheid om onder strikte voorwaarden ongerichte verkenning mogelijk te maken ten behoeve van onderzoeksoopdrachtgerichte kabelinterceptie in een latere fase. Gelet op de knelpunten die in de hiervoor genoemde rapportages zijn geconstateerd en de in het voorstel opgenomen randvoorwaarden acht de Afdeling deze verruiming begrijpelijk. Wel acht zij het cruciaal dat in het voorstel wordt gewaarborgd dat gegevens die zijn verkregen met het verkennen van de kabel niet mogen worden uitgewisseld met buitenlandse diensten. Ook adviseert zij op dit punt een zo kort mogelijke bewaartermijn op te nemen.

Ten aanzien van de voorgestelde regeling voor de beoordelingstermijn voor bulkdatasets adviseert de Afdeling te motiveren waarom niet wordt aangesloten bij door de Evaluatiecommissie gedane aanbevelingen, en de jaarlijkse verlenging van de beoordelingstermijn te maximaleren. Met betrekking tot de technische risico's bij de inzet van de hackbevoegdheid adviseert zij in het voorstel de verplichting op te nemen om de redelijkerwijs voorzienbare technische risico's te omschrijven in de toestemmingsaanvraag.

De verschuivingen in het toezicht leiden ertoe dat de betekenis van het onafhankelijk bindende toezicht door de TIB voorafgaande aan de inzet

van enkele specifieke cyberbevoegdheden afneemt. Dit wordt volgens de Afdeling in voldoende mate gecompenseerd door het voorgestelde bindende toezicht van de CTIVD tijdens en na de inzet van deze bevoegdheden. De geschillenprocedure bij de Afdeling bestuursrechtspraak kan daarnaast bijdragen aan de goede balans tussen de bescherming van de nationale veiligheid en de bescherming van de persoonlijke levenssfeer. De Afdeling wijst er wel op dat deze procedure, gelet op de hoog specialistische materie en de bestuurlijke context, in het stelsel als geheel een complex element vormt. Zij dient slechts bij uitzondering te worden aangewend.

Tot slot acht de Afdeling het geen gegeven dat met de voorgestelde maatregelen de beoogde operationele snelheid en wendbaarheid zal worden bereikt. Het stelsel van toezicht neemt door het voorstel toe in complexiteit en zal, met name tijdens en na de inzet van bevoegdheden, veel extra inspanning vragen. Het succes van het voorgestelde stelsel zal bovendien in sterke mate afhangen van de bereidheid van de betrokken instanties tot rolvaste en constructieve samenwerking. De Afdeling vindt het gelet daarop van groot belang dat de ervaringen met de voorgestelde maatregelen reeds tijdens de looptijd van de tijdelijke wet gemonitord worden. Door monitoring en het tijdig uitvoeren van een invoeringstoets kan worden geconstateerd wat de effecten van het voorstel zijn op de operationele wendbaarheid alsmede op de bescherming van grondrechten. Deze effecten dienen vervolgens te worden betrokken bij de totstandkoming van de voorgenomen brede wijziging van de Wiv 2017.

In verband met deze opmerkingen is aanpassing van het voorstel en de toelichting wenselijk.

1. Achtergrond en inhoud van het voorstel

a. Voorgeschiedenis

In mei 2018 trad de Wet op de inlichtingen- en veiligheidsdiensten 2017 in werking (Wiv 2017). De hoofddoelstelling van de Wiv 2017 was een modernisering en verruiming van de bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Een belangrijk nieuw element was met name dat de wet kabelinterceptie mogelijk maakt.³ Tegelijkertijd werden de waarborgen voor een rechtmatige inzet versterkt. Onder de Wiv 2002 bestond al het rechtmatigheidstoezicht tijdens en achteraf (ex durante en ex post) door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). De Wiv 2017 introduceerde een Toetsingscommissie Inzet Bevoegdheden (TIB) die vooraf (ex ante) bindend de rechtmatigheid van de inzet van de meest indringende bijzondere bevoegdheden toetst.

De Wiv 2017 kwam tot stand na een uitgebreid parlementair en maatschappelijk debat. In maart 2018 volgde een raadgevend referendum met een afwijzende uitspraak. De regering heeft vervolgens een wijzigingsvoorstel ingediend om de waarborgen in de Wiv 2017 te verduidelijken en de ruimte die de wet in de uitvoeringspraktijk biedt in te perken. Deze wijziging van de Wiv 2017 trad in juli 2021 in werking.

Twee jaar na de inwerkingtreding van de Wiv 2017 startte de wetsevaluatie. In het in januari 2021 gepubliceerde rapport stelde de Evaluatiecommissie Jones-Bos vast dat de Wiv 2017 de waarborgen aanzienlijk heeft versterkt maar dat de wet onvoldoende aansluit op de technolo-

³ Kamerstukken II 2016/17, 34 588, nr. 3, paragraaf 1.1.

gische complexiteit en de dynamiek van de operationele praktijk van de diensten.⁴ De Evaluatiecommissie deed diverse aanbevelingen om hieraan tegemoet te komen. De Ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en van Defensie zegden toe een brede wijziging van de Wiv 2017 voor te bereiden met de aanbevelingen van de Commissie als uitgangspunt.⁵ Ook een in april 2021 verschenen rapport van de Algemene Rekenkamer over de slagkracht van de AIVD en de MIVD⁶ zou daarbij betrokken worden. Dat gold eveneens voor de uitkomsten van enkele debatten. In dat verband is met name de in de Tweede Kamer aangenomen motie van belang dat er in toekomstige wetgeving geen sprake mag zijn van afschaling van toezicht.⁷

b. Aanleiding en doel van het wetsvoorstel

Voor een deel van de werkzaamheden van de AIVD en de MIVD willen de Ministers de uit de evaluatie voortvloeiende wetswijziging niet afwachten. De Wiv 2017 belemmert het onderzoek naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen volgens de regering zozeer dat een oplossing op korte termijn noodzakelijk wordt geacht.⁸ Daartoe strekt dit wetsvoorstel.

Het voorstel voor een tijdelijke wet creëert een apart regime voor het onderzoek van de AIVD en de MIVD naar landen met een offensief cyberprogramma en voor het toezicht daarop. Het doel van de tijdelijke wet is om snelheid en wendbaarheid te creëren in het operationeel onderzoek. De mogelijkheden tot effectieve inzet van bepaalde bijzondere bevoegdheden worden vergroot. Tegelijkertijd is het streven om de waarborgen waarmee die inzet moet zijn omgeven op een hoog en ten minste gelijkwaardig niveau te houden en te voorzien in een passend en sluitend stelsel van toezicht.⁹

Het aparte regime dat de tijdelijke wet creëert, ziet enkel op het onderzoek dat de AIVD en de MIVD doen naar landen met een offensief cyberprogramma tegen Nederland en Nederlandse belangen, zoals dat in de Geïntegreerde Aanwijzing als onderzoeksopdracht is geformuleerd.¹⁰ De toelichting geeft aan dat een offensief cyberprogramma er onder meer op is gericht om digitaal op heimelijke wijze de beschikking te verkrijgen over vertrouwelijke informatie, economische en technologische kennis of andere informatie van burgers of organisaties. De Nederlandse infrastructuur zou daarbij ook kunnen worden misbruikt bij het uitvoeren van cyberaanvallen op andere landen.¹¹ Rusland en China worden als voorbeeld genoemd van landen met een offensief cyberprogramma.

Op de uitvoering van alle andere taken blijft de Wiv 2017 van toepassing. De tijdelijke wet zal vier jaar gelden.¹² Het streven is dat binnen die tijd de brede herziening van de Wiv 2017 naar aanleiding van het rapport van de Evaluatiecommissie zijn beslag krijgt. De ervaringen opgedaan met de

⁴ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88.

⁵ Kamerstukken II 2020/21, 34 588, nr. O.

⁶ Algemene Rekenkamer, Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt, Kamerstukken 2020/21, 29 924, nr. 210.

⁷ Kamerstukken II 2020/21, 34 588, nr. 90 en Kamerstukken II 2020/21, 29 924, nr. 218.

⁸ Memorie van toelichting, paragraaf 1, Inleiding.

⁹ Memorie van toelichting, paragraaf 1, Inleiding en paragraaf 2.3, Overzicht van de voorgestelde maatregelen.

¹⁰ Memorie van toelichting, paragraaf 1, Inleiding. Geïntegreerde Aanwijzing 2022, besluit van 16 november 2021, Staatscourant 2021, 48257.

¹¹ Memorie van toelichting, paragraaf 1, Inleiding.

¹² Voorgesteld artikel 17.

maatregelen in de tijdelijke wet zullen daarin een belangrijke rol spelen, aldus de toelichting.¹³

c. Knelpunten Wiv 2017 en de maatregelen in het wetsvoorstel

Het inlichtingenonderzoek naar landen met een offensief cyberprogramma ziet vaak op verborgen dreigingen. Daarbij is op voorhand niet duidelijk ten aanzien van wie de bevoegdheden nu precies worden ingezet. Om activiteiten van landen met een offensief cyberprogramma effectief te kunnen volgen, moeten de diensten kunnen meebewegen als van digitale infrastructuur wordt gewisseld. De inzet van deze bevoegdheden is daarmee een dynamisch proces waarbij lopende de operatie meer zicht ontstaat op de precieze uitvoering.¹⁴

De toelichting stelt dat de diensten onder de Wiv 2017 onvoldoende mogelijkheden hebben om dit dynamische onderzoek uit te voeren. Het wordt in de praktijk als knellend ervaren dat de Wiv 2017 het zwaartepunt legt bij verantwoording vooraf. De knelpunten manifesteren zich met name bij cyberbevoegdheden zoals de inzet van de hackbevoegdheid¹⁵ en de inzet van de zgn. onderzoeksopdrachtgerichte (OOG) interceptie op de kabel.¹⁶ Deze knelpunten hebben ook betrekking op het toezicht daarop.

i. Inzetmogelijkheden bevoegdheden

Het voorstel voorziet per bevoegdheid in ruimere inzetmogelijkheden. De belangrijkste knelpunten en de met het oog daarop voorgestelde wijzigingen op dit terrein zijn, blijkens de toelichting, de volgende:

- *De Wiv 2017 veronderstelt dat de risico's van de inzet van de hackbevoegdheid op voorhand kunnen worden overzien, terwijl dat in het onderzoek naar landen met een offensief cyberprogramma niet altijd blijkt te lukken. Het voorstel schrapt de plicht om in de toestemmings- of verlengingsaanvragen voor de hackbevoegdheid de technische risico's daarvan te omschrijven, waaronder ook het al dan niet gebruik maken van onbekende kwetsbaarheden. De CTIVD houdt bindend toezicht tijdens de inzet van de hackbevoegdheid.¹⁷*
- *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. Dat levert vertraging op. In het voorstel worden 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. Ook hierop houdt de CTIVD bindend toezicht.¹⁸*
- *In onderzoeken naar landen met een offensief cyberprogramma blijkt het niet altijd haalbaar om, zoals de Wiv 2017 voorschrijft, zgn. bulkdatasets tijdig op relevantie te beoordelen. Het is niet gelukt hier, mede naar aanleiding van een toezichtsrappport van de CTIVD, binnen het kader van de Wiv 2017 een oplossing voor te vinden. Het wetsvoorstel beoogt een andere systematiek. De diensten krijgen de mogelijkheid de bewaartermijn van nog niet op relevantie beoordeelde*

¹³ Memorie van toelichting, paragraaf 2.4, De verhouding van de tijdelijke wet tot de Wiv 2017.

¹⁴ Memorie van toelichting, paragraaf 2.2.1, De inzet van bijzondere bevoegdheden.

¹⁵ Artikel 45 Wiv 2017.

¹⁶ Artikel 48 Wiv 2017. Onderzoeksopdrachtgerichte interceptie ziet op het verwerven van communicatie over de kabel of in de ether, zonder dat deze interceptie is gericht op een specifiek persoon of organisatie. De interceptie dient wel te relateren te zijn aan één of meerdere onderzoeksopdrachten van de diensten.

¹⁷ Voorgestelde artikelen 5 en 13.

¹⁸ Voorgestelde artikelen 5, 10, 11 en 13.

bulkdatasets jaarlijks te verlengen. De CTIVD houdt hier bindend toezicht op.¹⁹

- *De Wiv 2017 voorziet niet in de bevoegdheid om, voorafgaande aan OOG-interceptie, de communicatie-infrastructuur ongericht te verkennen. Daardoor hebben de diensten onvoldoende zicht op welke gegevensstromen van belang zijn voor het onderzoek. Het voorstel creëert hiervoor een grondslag. De TIB toetst vooraf de rechtmatigheid van de inzet.²⁰*

ii. Verschuivingen in het toezicht

Waar het bij deze voorstellen tot de verruiming van de inzetmogelijkheden ten koste gaat van de bindende toets vooraf (ex ante) door de TIB, introduceert het voorstel een bindende toets tijdens (ex durante) en na de inzet (ex post) door de afdeling toezicht van de CTIVD.²¹ De toelichting merkt meer in zijn algemeenheid op dat een onafhankelijke toets vooraf zoals de TIB die op basis van de Wiv 2017 uitvoert, naar zijn aard minder geschikt is als het gaat om onderzoek naar landen met een offensief cyberprogramma.²² In de uitvoering van de wet is het niet gelukt om overeenstemming te bereiken tussen de Minister en de TIB over wanneer de dynamische inzet van cyberbevoegdheden voldoet aan de eisen van de Wiv 2017.²³ Een toets tijdens of na de inzet van de bevoegdheid past beter bij de uitvoeringspraktijk, aldus de regering.²⁴

Het voorstel is daarom ook om de bindende toets door de TIB vooraf bij bepaalde bevoegdheden in zijn geheel te vervangen door een bindende toets door de CTIVD tijdens of na de inzet. Het gaat daarbij om het verkennen van geautomatiseerde werken²⁵ en de geautomatiseerde data-analyse van OOG-metadata.²⁶ Bij de overige bevoegdheden waarin de Wiv 2017 voorziet in een bindende toets vooraf door de TIB, blijft deze gehandhaafd.²⁷

iii. Geschillen tussen Ministers en toezichthouders

Het bestaande bindend karakter van de toets vooraf door de TIB betekent dat in de huidige situatie niet alleen in een concrete casus maar ook in de uitleg van de toepasselijke wettelijke begrippen en criteria de TIB het laatste woord heeft. De toelichting geeft aan dat in de praktijk van het onderzoek naar landen met een offensief cyberprogramma dit tot

¹⁹ Voorgestelde artikelen 6 en 13. Bulkdatasets die worden verkregen uit OOG-interceptie zijn hiervan uitgezonderd. Deze behouden het eigen regime van artikel 48 Wiv 2017.

²⁰ Voorgesteld artikel 7.

²¹ De CTIVD bestaat uit een afdeling toezicht en een afdeling klachtbehandeling, artikel 97, eerste en tweede lid, Wiv 2017. In dit advies dient waar kortweg «CTIVD» staat de afdeling toezicht gelezen te worden.

²² Memorie van toelichting, paragraaf 2.2.3, De wijze van verwerking van gegevens en 3.2.1, Algemeen.

²³ Memorie van toelichting, paragraaf 1, Inleiding.

²⁴ Memorie van toelichting, paragraaf 2.2.1, De inzet van bijzondere bevoegdheden.

²⁵ Voorgestelde artikelen 4 en 13.

²⁶ Voorgestelde artikelen 9 en 13. Metadata zijn die gegevens van telecommunicatie, welke nit de inhoud van de telecommunicatie betreffen.

²⁷ Het gaat daarbij op grond van artikel 32, tweede lid, Wiv 2017 om het toepassen van observatiemiddelen in woningen, het doorzoeken van woningen, het verrichten van DNA-onderzoek en de verlenging van de vernietigingstermijn van het celmateriaal, het binnendringen in een geautomatiseerd werk, de inzet van de gerichte af luisterbevoegdheid, de inzet van de onderzoeksoopdrachtgerichte (OOG) interceptiebevoegdheid, het onderzoek aan de gegevens die zijn verworven met OOG-interceptie, het selecteren van gegevens die zijn verworven met OOG-interceptie, het verzoeken om de medewerking van aanbieders van communicatiediensten bij de ongerichte of gerichte verwerving van telecommunicatie, met betrekking tot telecommunicatiegegevens en met betrekking tot de ontsluiting van communicatie.

problemen heeft geleid.²⁸ De Ministers en de TIB hebben in bepaalde situaties verschillende zienswijzen over de interpretatie van de wet en hebben dit niet weten op te lossen. Daardoor kunnen bepaalde onderzoeken in het cyberdomein niet worden opgestart dan wel niet voortvarend worden uitgevoerd, aldus de toelichting.²⁹ Met de CTIVD is de afgelopen jaren een verschil van inzicht ontstaan over eisen die de Wiv 2017 stelt aan de omgang met bulkdatasets.³⁰ Het wetsvoorstel beoogt deze impasses te doorbreken door de Afdeling Bestuursrechtspraak van de Raad van State te belasten met geschilbeslechting en het doen van richtinggevende uitspraken over de uitleg van wettelijke normen en begrippen.³¹

2. Constitutionele uitgangspunten

Bij het onderhavige wetsvoorstel zijn fundamentele constitutionele uitgangspunten aan de orde. Enerzijds is van cruciaal belang dat onze democratische rechtsstaat met de inzet van de inlichtingen- en veiligheidsdiensten tijdig en effectief beschermd kan worden tegen ernstige bedreigingen van buitenaf. Dat belang is hier nadrukkelijk aan de orde. Anderzijds kunnen de voor die inzet noodzakelijke bevoegdheden een vergaande inbreuk op grondrechten met zich brengen. Het is in een democratische rechtsstaat noodzakelijk dat gebruik van deze bevoegdheden wettelijk begrensd zijn en dat daarvoor passende waarborgen gelden, met name effectief toezicht.

De dreiging die uitgaat van landen met een offensief cyberprogramma is, zoals de toelichting overtuigend illustreert, reëel en actueel. Het is de taak van de AIVD en de MIVD deze dreigingen te onderkennen en andere instanties in staat te stellen de benodigde maatregelen te treffen. Daarmee vervullen deze diensten een essentiële rol in de bescherming van onze democratische rechtsorde. Dit vraagt van de AIVD en de MIVD een hoog niveau van technische expertise en doortastendheid. In hun onderzoek naar deze dreigingen kunnen zij, zo is in algemene zin geaccepteerd, heimelijk bijzondere bevoegdheden inzetten.

Bij het gebruik van deze bevoegdheden is onvermijdelijk dat de diensten toegang krijgen tot persoonsgegevens, niet alleen van personen die zij in onderzoek hebben, maar ook van anderen. De diensten maken met hun onderzoeken dan ook, zij het met toepassing van wettelijke voorwaarden en waarborgen, een substantiële inbreuk op in de Grondwet en de in het Europees Verdrag voor de Rechten van de Mens (EVRM) verankerde grondrechten. In het bijzonder zijn deze bevoegdheden een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer.³²

Over de inzet van deze bijzondere bevoegdheden heeft zich over een lange reeks van jaren rechtspraak ontwikkeld van het Europees Hof voor de Rechten van de Mens (EHRM). Als het gaat om bevoegdheden waarbij

²⁸ Memorie van toelichting, paragraaf 1, Inleiding.

²⁹ Memorie van toelichting, paragraaf 1, Inleiding en paragraaf 3.2.5, Verduidelijking bijschrijfmogelijkheid.

³⁰ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 1.2.

³¹ Voorgestelde artikelen 14 en 15.

³² Artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Ook artikel 13 Grondwet, het telefoon- en telegraafgeheim, is van belang. In de Eerste Kamer ligt in tweede lezing een voorstel tot wijziging van artikel 13 van de Grondwet dat beoogt dit recht techniekonafhankelijk te beschermen en te wijzigen in het telecommunicatiegeheim. Een beperking van dit recht in het belang van de nationale veiligheid is slechts mogelijk bij in de wet genoemde gevallen en met machtiging van hen die daartoe in de wet zijn aangewezen. Zie Kamerstukken II 2020/21, 35 700, nr. 2. Aan die voorwaarden is in het onderhavige wetsvoorstel voldaan.

door inlichtingen- en veiligheidsdiensten grote hoeveelheden data worden verworven, blijkt dat het EHRM veel waarde hecht aan onafhankelijk toezicht in alle fasen van het interceptieproces. Burgers zijn doorgaans niet op de hoogte van de interceptie van hun data. Dat maakt het van groot belang dat een rechter of een (andere) onafhankelijke overheidsinstantie dat wel kan zijn en over de toepassing van de wettelijke bevoegdheden een onafhankelijk oordeel kan uitspreken.

De wettelijke mogelijkheid voor de diensten om heimelijk persoonsgegevens te verwerven en te verwerken brengt met zich dat de rechtsbescherming een ander, van het normale stramen afwijkend karakter draagt. Vanwege de vaak geheime aard van de activiteiten van de diensten ligt bij de inrichting van wettelijke waarborgen van oudsher de nadruk niet op de normaal geldende individuele rechtsbescherming maar op effectief systeemtoezicht. Het recht op een eerlijk proces als bedoeld in artikel 6 EVRM met zijn hoge eisen aan rechterlijke procedures is niet van toepassing. Wel voorziet artikel 13 EVRM in het recht voor burgers op een effectief en daadwerkelijk rechtsmiddel als grondrechten zijn geschonden. De diverse onderdelen van het wettelijke toezicht (met inbegrip van de bindende klachtenbehandeling door de CTIVD) dienen in deze context te worden begrepen.

Het EHRM vindt een onafhankelijke bindende toets voorafgaande aan de inzet van bevoegdheden een belangrijke waarborg ter bescherming van grondrechten.³³ Hetzelfde geldt voor onafhankelijk toezicht op de verdere verwerking van de verworven data. Deze waarborgen dienen niet los van elkaar te worden beoordeeld. Het gaat er blijkens de rechtspraak van het EHRM uiteindelijk om dat het stelsel van toezicht als geheel in evenwicht dient te zijn. Het stelsel dient waarborgen te bevatten die in hun onderlinge samenhang adequate en effectieve garanties bieden tegen willekeur en het risico van misbruik.³⁴

De Afdeling signaleert dat landen binnen Europa ieder voor zich hun eigen systematiek hebben van rechtsstatelijke waarborgen en checks and balances, overeenkomstig het nationale constitutionele recht. Er zijn belangrijke verschillen tussen landen in hoe inlichtingen- en veiligheidsdiensten zijn gepositioneerd, over welke bevoegdheden zij beschikken en op welke wijze onafhankelijk toezicht is georganiseerd. De uitspraken van het EHRM bieden dan ook geen blauwdruk voor een stelsel van toezicht. De nadruk op de balans binnen en de effectiviteit van het stelsel als geheel maakt dat eventuele beperkingen in de ene fase van het proces van gegevensverwerking, veelal kunnen worden gecompenseerd door andere waarborgen.

De beschouwingen en adviesopmerkingen die hierna volgen moeten in de sleutel van het voorgaande worden geplaatst. Zij hebben allen betrekking op de concrete uitwerking in het wetsvoorstel van uit constitutioneel oogpunt wezenlijke punten: de reikwijdte en begrenzing van bevoegdheden, het onafhankelijk toezicht en de rechtsbescherming.

³³ EHRM 21 mei 2021, 35252/08 (Centrum för Rättvisa v. Sweden), para 264; EHRM 21 mei 2021, 58170/13, 62322/14 en 24960/15 (Big Brother Watch and others v. The United Kingdom), para. 350.

³⁴ EHRM 21 mei 2021, 35252/08 (Centrum för Rättvisa v. Sweden), par 270–271; EHRM 21 mei 2021, 58170/13, 62322/14 en 24960/15 (Big Brother Watch and others v. The United Kingdom), par. 356–357.

3. Algemene beschouwing

Uit het voorgaande komt als hoofdlijn naar voren dat bij het wettelijk reguleren van de werkzaamheden van de AIVD en de MIVD een balans moet worden gevonden tussen enerzijds het bereiken van de noodzakelijke effectiviteit van het operationele vermogen van de diensten en anderzijds het waarborgen van de grondrechten, inclusief effectief toezicht op deze werkzaamheden.³⁵ Uiteraard is dat niet nieuw. Het streven van de Wiv 2017 was daar ook op gericht. Deze wet kwam tot stand na een indringend politiek en maatschappelijk debat juist over deze punten. Het gewenste evenwicht is echter, zo beargumenteert de toelichting, nog niet in voldoende mate bereikt.

Het voorgaande moet worden begrepen in het licht van de eerder geschetste voorgeschiedenis. Vanaf de inwerkingtreding in mei 2018 is de implementatie van de wet in de praktijk op de voet gevolgd. De CTIVD publiceerde hierover halfjaarlijks voortgangsrapportages. Op verzoek van de Eerste Kamer was bovendien de evaluatie naar voren gehaald; in 2020, drie jaar eerder dan wettelijk vereist, werd een Evaluatiecommissie ingesteld.³⁶ In dezelfde periode heeft ten slotte ook de Algemene Rekenkamer onderzoek gedaan naar de effecten van de Wiv 2017.

Uit de genoemde rapporten komt steeds naar voren dat de Wiv 2017 op onderdelen onvoldoende aansluit op de technologische complexiteit en de dynamiek van de operationele praktijk van de diensten.³⁷ De knelpunten die het voorstel voor de tijdelijke wet adresseert, zijn grotendeels dezelfde als in rapporten van de Evaluatiecommissie en de Algemene Rekenkamer. De toelichting motiveert overtuigend op welke wijze het onderzoek naar landen met een offensief cyberprogramma, essentieel ter bescherming van de democratische rechtsorde (zie hiervoor punt 2), hierdoor wordt belemmerd en waarom dit op korte termijn dient te worden opgelost.

De totstandkoming en praktijk van de Wiv 2017 illustreren dat het effectief reguleren van een nog niet uitgekristalliseerde technische praktijk niet eenvoudig is. Het wetsvoorstel beoogt hierin verbetering aan te brengen. De veronderstelling is, zo blijkt uit de toelichting, dat dit aangepaste regime de mogelijkheden van diensten vergroot om snel en wendbaar onderzoek te doen en dat het bovendien de effectiviteit van het toezicht ten goede komt. De Afdeling acht het geen gegeven dat met het wetsvoorstel dat doel wordt bereikt. Dit hangt vooral samen met de complexiteit van het voorgenomen nieuwe stelsel van toezicht (zie hierna punt 4b). Het wetsvoorstel heeft bovendien tot gevolg, zo blijkt ook uit de toelichting, dat twee wettelijke regimes (de tijdelijke wet en de Wiv 2017) gelijktijdig van toepassing zijn op dezelfde organisaties en werkprocessen. De daarmee gepaard gaande complexiteit en overlap kan de beoogde operationele snelheid en wendbaarheid belemmeren.

³⁵ Advies van de Afdeling advisering van 21 september 2016 over de Wet op de inlichtingen- en veiligheidsdiensten 20. (W04.16.0097/I), Kamerstukken II 2016/17, 34 588, nr. 4 en Evaluatie door de Commissie Dessens van de Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen, p. 8.

³⁶ Handelingen I, 2016/17, 35, nr. 8, p. 4, en Kamerstukken II 2017/18, 34 700, nr. 34, p. 4 (Regeerakkoord 2017–2021 «Vertrouwen in de toekomst»).

³⁷ Reactie CTIVD aan ECW 11 augustus 2020, www.ctivd.nl, Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, belangrijkste bevindingen en conclusies. Algemene Rekenkamer, Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt, Kamerstukken II 2020/21, 29 924, nr. 210.

De Afdeling acht het met het oog op de dreiging die uitgaat van landen met een offensief cyberprogramma niettemin begrijpelijk om thans, vooruitlopend op een definitievere wetswijziging, een aangepast regime voor een beperkt deel van de taken en bevoegdheden tijdelijk te beproeven. In dit licht is van belang dat veel van de in het wetsvoorstel gekozen oplossingen corresponderen met de grondig gemotiveerde aanbevelingen van de Evaluatiecommissie. In verband met de ingrijpendheid van het voorstel vindt de Afdeling het wel van groot belang dat de ervaringen met de voorgestelde maatregelen, naast de voorziene evaluatie, reeds tijdens de looptijd van de tijdelijke wet worden gemonitord. Door monitoring (met inbegrip van het tijdig uitvoeren van een invoeringstoets) kan worden geconstateerd wat de effecten zijn van het wetsvoorstel op de operationele wendbaarheid alsmede op de bescherming van grondrechten.

De resultaten daarvan kunnen vervolgens worden meegenomen in de thans al voorziene eindevaluatie. Op deze manier kan worden beoordeeld of de voorgenomen wijzigingen de beoogde doelstellingen waarmaken, en of daarbij de voorgestelde waarborgen voldoende robuust zijn. Met het oog daarop dient vooraf duidelijk te zijn op welke wijze de voorziene evaluatie zal worden uitgevoerd.

De Afdeling adviseert in het voorstel een evaluatiebepaling op te nemen. Voorts adviseert zij in de toelichting in te gaan op de wijze waarop deze evaluatie (met inbegrip van de hiervoor bedoelde monitoring) inhoudelijk en processueel zal worden vormgegeven.

Hieronder gaat de Afdeling nader in op de vraag of het wetsvoorstel, gelet op de hiervoor geschetste constitutionele uitgangspunten, de grondrechten in voldoende mate en op een evenwichtige wijze waarborgt. Zij bespreekt het voorgestelde stelsel van toezicht, waaronder ook de nieuwe beroepsgang bij de Afdeling, in het licht van de eisen die de Grondwet en de verdragen hieraan stellen (punten 4 en 5). Ook komen de voorgestelde wijzigingen in de vormgeving van bepaalde bevoegdheden aan de orde. Op onderdelen adviseert zij het wetsvoorstel dan wel de toelichting aan te passen (punten 6–11).

De Afdeling wijst er terecht op dat met het in het wetsvoorstel opgenomen aangepaste regime ten opzichte van de Wiv 2017 wordt beoogd de mogelijkheden van diensten te vergroten om snel en wendbaar onderzoek te doen en dat dit bovendien de effectiviteit van het toezicht ten goede komt. De praktijk zal moeten uitwijzen of dit doel met de in het wetsvoorstel opgenomen voorzieningen inderdaad wordt bereikt.

Ten aanzien van het advies van de Afdeling om, in verband met de ingrijpendheid van het wetsvoorstel, de ervaringen met de voorgestelde maatregelen tijdens de looptijd van de tijdelijke wet te monitoren alsmede een evaluatiebepaling op te nemen, wordt het volgende opgemerkt. In artikel 17 van het wetsvoorstel is erin voorzien dat de wet vier jaar na inwerkingtreding vervalt. In de toelichting is aangegeven dat de reden daarvoor is dat ter opvolging van de aanbevelingen van de Evaluatiecommissie Wiv 2017 (ECW), na het uitbrengen van een hoofdlijnennotitie, een traject tot herziening van de Wiv 2017 zal worden ingezet, waarvan de verwachting is dat deze binnen de werkingsduur van de tijdelijke wet kan worden bewerkstelligd. Tegen deze achtergrond laat een regulier traject van monitoring en eindevaluatie na afloop van de looptijd van vier jaar, voor zover het de bedoeling is dat vervolgens de resultaten daarvan worden betrokken bij de voorbereiding en totstandkoming van de voorgenomen herziening van de Wiv 2017, zich niet inpassen. Immers

voorbereiding en totstandkoming van die herziening zal parallel aan de werking van de tijdelijke wet plaatsvinden. Het opnemen van een evaluatiebepaling als door de Afdeling wordt voorgesteld in het wetsvoorstel ligt daarom niet voor de hand. Dat ligt anders waar het gaat om het voorstel tot monitoring. Na inwerkingtreding van de Tijdelijke wet zal gedurende de looptijd (tussentijds) de uitvoering van de wet intern door de diensten worden gemonitord. De (tussentijdse) resultaten daarvan zullen met de stelselpartners (de CTIVD, de TIB en de Afdeling bestuursrechtspraak van de Raad van State) worden gedeeld en besproken. Ongeveer een jaar na inwerkingtreding zal volgens de methode van de invoeringstoets gekeken worden naar de gevolgen voor de doelgroep en de uitvoering waarbij ook actief naar knelpunten op zoek zal worden gegaan. Hierbij kan in het bijzonder ook aandacht worden besteed aan de vraag in hoeverre het voorgestelde stelsel van toets en toezicht als geheel zich verhoudt tot de beoogde operationele snelheid en wendbaarheid. De resultaten zullen tijdens de voorbereiding van de herziening van de Wiv 2017 beschikbaar komen en daar worden ingebracht, zodat daarmee zoveel als naar de stand van het voorbereidingsproces mogelijk is, daarmee rekening kan worden gehouden. Daarnaast kunnen de voorlopige centrale vragen van de invoeringstoets in deze interne evaluatie worden betrokken.³⁸ Op deze wijze kan het proces van monitoring van de Tijdelijke wet zo goed mogelijk worden afgestemd op de voorgenomen herziening van de Wiv 2017, die, zoals vermeld, gedurende de looptijd van de Tijdelijke wet vorm zal krijgen.

4. Stelsel van toezicht

a. Verenigbaarheid met de Grondwet en de verdragen

In het onder de Wiv 2017 geldende stelsel van toezicht op de AIVD en de MIVD is sprake van een bindende toets vooraf door de TIB bij de inzet van de meest indringende bijzondere bevoegdheden. De CTIVD oefent op dit moment geen bindend toezicht uit op de rechtmatigheid van de werkzaamheden van de diensten. De behandeling van klachten van burgers over het optreden van de AIVD en de MIVD vindt wel bindend plaats bij de afdeling klachtbehandeling van de CTIVD. Met dit stelsel werd beoogd in lijn met de Europese jurisprudentie (zie hiervoor punt 2) te voorzien in effectieve rechtsbescherming in alle fases waarin de bevoegdheden door de diensten worden ingezet.³⁹

Het voorstel beperkt de rol van de TIB bij de inzet van bepaalde cyberbevoegdheden.⁴⁰ Dat heeft tot gevolg dat een operatie vaker zonder onafhankelijke toets vooraf kan aanvangen. De waarborgfunctie van het toezicht vooraf voor de bescherming van de persoonlijke levenssfeer en van persoonsgegevens neemt daarmee in bepaalde gevallen af.

Het voorstel compenseert dit door op alle punten waar de toets vooraf door de TIB wordt geschrapt of ingeperkt, de rol van de CTIVD te versterken. Het toezicht van de CTIVD tijdens en na de inzet van deze bevoegdheden krijgt, voor het eerst, bindende kracht.⁴¹ De toelichting motiveert deze verschuiving met de stelling dat toezicht tijdens of na de inzet dynamisch kan worden ingezet en daardoor beter past bij de aard

³⁸ Zie daarover de Kamerbrief van 21 april 2022 van de Minister voor Rechtsbescherming, Kamerstukken II 2021/22, 35 510, nr. 96.

³⁹ Kamerstukken II 2016/17, 34 588, nr. 3, paragraaf 1.2.1.

⁴⁰ De TIB krijgt er wel de bevoegdheid bij om vooraf bindend de rechtmatigheid van de verkenningsbevoegdheid ten behoeve van de OOG-interceptie te toetsen, zie voorgesteld artikel 7.

⁴¹ Wel heeft de Afdeling klachtbehandeling van de CTIVD al de bevoegdheid bindende uitspraken te doen in klachtzaken, zie artikel 124 Wiv 2017.

van cyberbevoegdheden dan een meer statische toets vooraf. Daarbij heeft de CTIVD, anders dan de TIB, direct en onbeperkt toegang tot de systemen van de AIVD en de MIVD. Men kan letterlijk over de schouder van de medewerker meekijken.

De effectiviteit van deze manier van toezicht wordt door de Evaluatiecommissie benadrukt, onder meer vanwege de gespecialiseerde kennis en de technische expertise van de CTIVD.⁴² Van belang is voorts dat de voor de uitvoering van de extra taken benodigde extra capaciteit is toegezegd.⁴³ De Afdeling acht het aannemelijk dat daarmee een vorm van effectief toezicht kan worden bereikt waarmee het niveau van de bescherming van de persoonlijke levenssfeer en van de bescherming van persoonsgegevens gelijk blijft ten opzichte van de huidige situatie.

Daarnaast introduceert het voorstel een beroepsprocedure bij de bestuursrechter. Als de Minister zich niet kan vinden in de bindende oordelen van de TIB of de CTIVD, kan hij zich wenden tot de Afdeling Bestuursrechtspraak van de Raad van State. Deze onafhankelijke geschillenbeslechting kan bijdragen aan het vinden van een goede balans tussen de bescherming van de nationale veiligheid en de bescherming van de persoonlijke levenssfeer. Zo bezien vormt dit een extra waarborg in het stelsel.

Het beperken van de onafhankelijke toetsing vooraf door de TIB wordt voldoende gecompenseerd door het voorgestelde bindende toezicht van de CTIVD tijdens en na de inzet van bevoegdheden. De beoogde nieuwe rolverdeling voorziet in de mogelijkheid van effectief toezicht op verschillende momenten gedurende de inzet van bevoegdheden. De mogelijkheid van geschilbeslechting in laatste instantie door de Afdeling bestuursrechtspraak kan voorkomen dat impasses tussen de Minister(s) en de toezichthouders blijven bestaan als het gaat om de uitleg en toepassing van de wet. Dit kan bijdragen aan een beter en effectiever werkend evenwicht in het stelsel als geheel. Mede in het licht van de voorgestelde aanpassingen voldoet het wetsvoorstel op dit punt aan de eisen die daaraan door de Grondwet en de verdragen worden gesteld.

b. Complexiteit van het stelsel van toezicht

Het voorgestelde nieuwe stelsel van toezicht heeft echter wel een hoge mate van complexiteit. Het brengt verandering in de verhoudingen tussen de toezichthouders en de diensten en tussen de toezichthouders onderling. In het kader van de inzet van één bijzondere bevoegdheid kan op meerdere momenten een onafhankelijk oordeel volgen. Op basis van het voorstel voor de tijdelijke wet betekent dit bijvoorbeeld bij de inzet van hackbevoegdheid het volgende:

- de CTIVD kan het verkennen van het geautomatiseerde werk tijdens de inzet beoordelen (bindend);
- de TIB beoordeelt het binnendringen in het geautomatiseerde werk vooraf (bindend);
- de CTIVD kan tijdens het binnendringen de genomen technische risico's, de gebruikte onbekende kwetsbaarheden en bijgeschreven geautomatiseerde werken beoordelen (bindend);
- de CTIVD kan tijdens het binnendringen de verdere inzet en uitvoering beoordelen (niet bindend);

⁴² Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88, paragraaf 9.2.5.

⁴³ Memorie van toelichting, paragraaf 6.3, De uitvoeringsconsequenties voor de TIB, CTIVD en de Afdeling bestuursrechtspraak van de Raad van State. Zie ook de consultatiereactie van de CTIVD.

- *de Afdeling bestuursrechtspraak van de Raad van State kan uitspraak doen in een beroep van een Minister tegen één van de hierboven genoemde bindende oordelen van de toezichthouders (bindend).*
- *de afdeling klachtbehandeling van de CTIVD kan een klacht over de inzet beoordelen (bindend).*

Om ervoor te zorgen dat toezichthouders op de hoogte zijn van elkaars bevindingen voorziet het voorstel in een grondslag voor gegevensuitwisseling.⁴⁴

Ten aanzien van het toezicht onder de Wiv 2017 constateerde de Evaluatiecommissie dat de intensiteit van het contact tussen diensten, ministeries en toezichthouders over de toepassing van de Wiv 2017 mede de oorzaak was van de frictie die was ontstaan in de uitvoering van de wet.⁴⁵ Deze intensiteit neemt in het voorstel voor de tijdelijke wet niet af. Hoewel het gemakkelijker wordt voor de AIVD en de MIVD om te starten met de inzet van een bevoegdheid, kan er tijdens en na de inzet op meer momenten en door meer instanties een bindend oordeel plaatsvinden. Dat betekent naar alle waarschijnlijkheid veel extra werk voor diensten, ministeries, toezichthouders en de Afdeling bestuursrechtspraak. Er zullen nog steeds de nodige juridische en technische vragen rijzen. Dit geldt te meer daar dit wetsvoorstel bovenop de Wiv 2017 komt en daarmee twee wettelijke regimes gelijktijdig van toepassing zullen zijn op dezelfde organisaties en werkprocessen.

Het is daarmee geen gegeven dat met dit nieuwe stelsel van toezicht de door het wetsvoorstel beoogde operationele snelheid en wendbaarheid zal worden bereikt. Het succes van het voorgestelde stelsel zal dan ook in sterke mate afhangen van de bereidheid van de betrokken instanties tot rolvaste en constructieve samenwerking.

De Afdeling adviseert in het licht van het voorgaande bij de evaluatie van de tijdelijke wet in het bijzonder aandacht te besteden aan de vraag in hoeverre het voorgestelde stelsel van toezicht als geheel zich verhoudt tot de beoogde operationele snelheid en wendbaarheid.

Door de Afdeling wordt terecht gesignaleerd dat het geen gegeven is dat met het nieuwe stelsel van toetsing en toezicht de door het wetsvoorstel beoogde operationele snelheid en wendbaarheid zal worden bereikt, en dat het succes van het voorgestelde stelsel in sterke mate zal afhangen van de bereidheid van de betrokken instanties tot rolvaste en constructieve samenwerking. Zoals hiervoor onder 3 ten aanzien van de algemene beschouwing reeds is opgemerkt, zal de praktijk moeten uitwijzen of met het in het wetsvoorstel opgenomen voorzieningen de mogelijkheden van de diensten om snel en wendbaar onderzoek te doen worden vergroot. Ook wordt erkend dat – door het tijdelijk naast elkaar bestaan van het reguliere toezichtstelsel in de Wiv 2017 en het in de Tijdelijke wet deels daarvan afwijkende stelsel – de complexiteit in het toezichtstelsel toeneemt. Het is dan ook van belang dat deze periode zo kort mogelijk blijft en dat de herziening van de Wiv 2017 en de daarin voorziene aanpassing van het stelsel van toets en toezicht met voortvarendheid ter hand wordt genomen.

⁴⁴ Voorgesteld artikel 12.

⁴⁵ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88, belangrijkste bevindingen en conclusies.

5. Beroepsprocedure bij de Afdeling Bestuursrechtspraak van de Raad van State

a. Inleiding

In haar rapport typeerde de Evaluatiecommissie de situatie dat toezicht-houders het laatste woord hebben over de toepassing van de Wiv 2017 als praktisch onwenselijk en principieel niet passend. Deze «weeffout» in de wet diende volgens de commissie te worden hersteld door de bestuurs-rechter de taak te geven om de juridische grenzen van het speelveld te bepalen waarbinnen het toezicht op de bevoegdheidsuitoefening door de diensten plaatsvindt.⁴⁶

Het wetsvoorstel implementeert deze aanbeveling voor het onderzoek naar landen met een offensief cyberprogramma. De Minister kan bij de Afdeling Bestuursrechtspraak van de Raad van State beroep instellen tegen bindende oordelen van zowel de TIB als de CTIVD.⁴⁷ Het beroep heeft geen schorsende werking, maar de Afdeling kan wel desgevraagd een voorlopige voorziening treffen waarmee de werking van het bindende oordeel wordt opgeschort.⁴⁸ De behandeling van de zaak vindt plaats achter gesloten deuren, maar de uitspraak is openbaar, met uitzondering van staatsgeheime informatie.⁴⁹

b. Betekenis artikel 121 van de Grondwet

Met de geschetste procedure kan de Afdeling Bestuursrechtspraak geschillen tussen toezichthouders en Ministers beslechten en uitsluitsel geven over de uitleg van wettelijke begrippen. Het voorstel creëert daarmee een nieuwe taak, die volgens de toelichting nadrukkelijk moet worden onderscheiden van de rechtsprekende taak die de Afdeling in bestuursrechtelijke zaken. Het is een bijzondere vorm van geschillenbeslechting die op allerlei, hierna te bespreken manieren afwijkt van de klassieke bestuursrechtspraak. Niettemin gaat de toelichting ervan uit dat artikel 121 van de Grondwet ook geldt voor de uitspraken van de Afdeling Bestuursrechtspraak in de geschillenbeslechting op basis van het voorstel.⁵⁰

Artikel 121 van de Grondwet schrijft voor dat de uitspraak in het openbaar geschiedt. Hierop zijn, anders dan bij de andere twee waarborgen van artikel 121 (die betrekking hebben op de openbaarheid van terechtzittingen en de motivering van vonnissen), geen uitzonderingen mogelijk. Hoewel niet duidelijk is wat exact bedoeld is met het begrip «geschieden», stelt de toelichting dat algemeen wordt aangenomen dat artikel 121 niet impliceert dat uitspraken volledig publiekelijk moeten worden voorgelezen. Voorlezing van alleen het dictum volstaat, aldus de toelichting.

Hoewel de Grondwet naar de letter genomen niet geheel duidelijk is over of de daarin opgenomen waarborgen ook gelden voor onafhankelijke gerechten die niet tot de rechterlijke macht behoren, moet worden aangenomen dat artikel 121 Grondwet in algemene zin ook van

⁴⁶ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 9.5.

⁴⁷ Voorgesteld artikel 14.

⁴⁸ Voorgesteld artikel 15.

⁴⁹ Voorgesteld artikel 14, elfde en twintigste lid.

⁵⁰ Toelichting, paragraaf 4.3, Beroep op de Afdeling bestuursrechtspraak, zie ook voorgesteld artikel 14, eerste lid en artikel 30b, Wet op de Raad van State.

toepassing is op de Afdeling bestuursrechtspraak.⁵¹ Dit is echter niet zonder meer het geval voor de bijzondere vorm van geschillenbeslechting zoals nu voorgesteld. Deze wijkt in een aantal opzichten af van de reguliere bestuursrechtspraak.

In het wetsvoorstel gaat het om een bijzondere voorziening voor een geschil tussen twee overheidsorganen: de Minister enerzijds en de TIB/CTIVD anderzijds. De burger heeft, anders dan in de reguliere bestuursrechtelijke procedure, geen rol. Het gaat bovendien om een procedure in een bijzonder werkveld: een geschil over machtigingen voor en beoordeling van operaties van de inlichtingen- en veiligheidsdiensten. De onderliggende gegevens zijn in verband daarmee staatsgeheim. Om die reden ligt een vergelijking voor de hand met de in de Wiv 2017 geregelde procedure die een last vereist van de rechtbank Den Haag voor het openen van brieven en andere geadresseerde zendingen. In dat geval is de last evenmin openbaar.⁵²

De Afdeling adviseert om in de toelichting, anders dan nu het geval is, een duidelijk standpunt in te nemen over de toepasselijkheid van artikel 121 van de Grondwet in de geschillen die hier aan de orde zijn. Daarvoor is te meer reden omdat niet duidelijk is wat die bepaling precies voorschrijft. De grondwetsgeschiedenis biedt weliswaar aanknopingspunten voor het standpunt in de toelichting dat de uitspraak mondeling moet worden uitgesproken en dat daarbij kan worden volstaan met het dictum⁵³, maar de tekst van de bepaling («geschieden») dwingt daartoe niet. De vraag rijst of in het digitale tijdperk niet gekozen moet worden voor een andere uitleg.

Dit lijkt ook de gedachtegang die ten grondslag lag aan de wijziging van artikel 8:78 Awb. Het artikel is in 2017 gewijzigd in verband met de invoering van digitaal procederen en is nu op dit punt gelijklopend aan artikel 121 van de Grondwet. De wetsgeschiedenis vermeldt dat er voorheen van uit werd gegaan dat aan het beginsel van openbaarheid invulling moest worden gegeven door de uitspraak in het openbaar uit te spreken.⁵⁴ Dit dateert echter van voor het internettijdperk. Internet biedt volgens de toelichting bij die wet kansen om aan de openbaarheid van de uitspraak een meer eigentijdse invulling te geven. Zo is het bijvoorbeeld toegestaan om dagelijks een lijst van gedane uitspraken op te stellen en op rechtspraak.nl te plaatsen, onder vermelding van de uitspraakdatum en het zaaknummer.⁵⁵ De wetgever lijkt er in 2017 van te zijn uitgegaan dat deze wetswijziging in overeenstemming was met de vereisten in artikel 121 van de Grondwet en dus dat deze bepaling niet vereist dat de uitspraak in het openbaar moet worden voorgelezen.

Het voorgaande laat onverlet dat dat waar mogelijk openbaarheid moet worden betracht. Het voorstel stelt dat uitspraken openbaar zijn met uitzondering van staatsgeheime informatie.⁵⁶ Gelet daarop zullen de feiten, waaronder de operationele context en de technische toepassing, in een nader te bepalen mate geanonimiseerd en geabstraheerd moeten worden. Ook onder die omstandigheden kan tegemoet worden gekomen aan de in de buitenwereld bestaande behoefte aan duidelijkheid over de

⁵¹ De Afdeling bestuursrechtspraak behoort niet tot de rechterlijke macht maar is wel duurzaam met rechtspraak belast, zie artikel 1:4 Awb juncto 30b van de wet op de Raad van State. Het valt daarmee onder de reikwijdte van artikel 121 van de Grondwet, zie Kamerstukken II 1979/80, 16 162, nr. 3, p. 2, 4, 5 en 7.

⁵² Zie verder het advies van de Afdeling bestuursrechtspraak van 21 april 2022 PM.

⁵³ Kamerstukken II 1979/80, 16 162, nr. 3, p. 22–23.

⁵⁴ Kamerstukken II 2014/15, 34 059, nr. 3, p. 118.

⁵⁵ Kamerstukken II 2014/15, 34 059, nr. 3, p. 119.

⁵⁶ Voorgesteld artikel 14, twintigste lid.

juridische grenzen die worden gesteld aan de bevoegdheden van de AIVD en de MIVD. Zoveel blijkt ook uit de openbare toezichtsrapporten, jaarverslagen en klachtbeslissingen van de toezichthouders. Het creëren van meer duidelijkheid waar mogelijk over de betekenis van wettelijke begrippen en bevoegdheden is ook een belangrijke doelstelling van de beroepsprocedure. Het is met het oog daarop niet waarschijnlijk dat, zoals de toelichting stelt, steeds volstaan kan worden met openbaarmaking van enkel het dictum.

De Afdeling adviseert in de toelichting nader op voorgaande punten in te gaan.

In de toelichting is verduidelijkt de Afdeling bestuursrechtspraak een onafhankelijk rechterlijk orgaan is dat duurzaam met rechtspraak is belast. Artikel 121 Grondwet is in algemene zin dan ook van toepassing op de Afdeling bestuursrechtspraak. De nieuwe taak van de Afdeling bestuursrechtspraak op grond van dit wetsvoorstel wijkt echter dusdanig af van reguliere (bestuurs)rechtspraak dat artikel 121 Grondwet daarop niet van toepassing is.

De Afdeling signaleert wel terecht dat er desalniettemin behoefte is aan duidelijkheid over de juridische grenzen die worden gesteld aan de bevoegdheden van de AIVD en de MIVD. Daarom wordt voorzien in openbaarmaking van de uitspraak door de Afdeling met inachtneming van de noodzakelijke geheimhouding van daarvoor in aanmerking komende staatsgeheime gegevens. Het wetsvoorstel is in deze zin aangepast.

c. Rol van de Afdeling bestuursrechtspraak

De toelichting gaat in beperkte mate in op de wijze waarop de Afdeling bestuursrechtspraak het geschil, gegeven de bijzondere aard daarvan (zie hiervoor onderdeel b), dient te beoordelen. Vermeld wordt dat het de Afdeling vrij staat om te bepalen op welke wijze en met welke intensiteit zal worden getoetst. Wel is de mate waarin de wetgever marges heeft gelaten in dit kader van belang. In de Wiv 2017 kunnen deze per bevoegdheid verschillen, aldus de toelichting. Hierdoor zal ook de toetsingsintensiteit bij de Afdeling kunnen verschillen. Binnen een en dezelfde uitspraak kunnen er bovendien onderdelen zijn die zich lenen voor verschillende soorten toetsingsintensiteit. Zo zal wetsuitleg doorgaans niet voor marginale toetsing in aanmerking komen, waar dat bij de beoordeling van een feitencomplex soms wel aangewezen kan zijn, aldus de toelichting.⁵⁷

De vraag rijst of deze algemene passage voldoende recht doet aan de te verwachten praktijk. Terughoudende beoordeling zal gelet op de aard van de geschillen naar verwachting de hoofdregel zijn. De Afdeling wijst er in dat verband op dat de TIB en de CTIVD gespecialiseerde onafhankelijke instanties zijn. Zij beschikken over de expertise 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.

Het ligt in de rede 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

⁵⁷ Toelichting, paragraaf 4.3, Beroep op de Afdeling bestuursrechtspraak.

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.

De Afdeling advisering wijst er in samenhang met het voorgaande verder op dat de beroepsprocedure slechts in uitzonderlijke gevallen soelaas kan bieden. Het moet gezien worden als een ventiel in een complex en belast systeem. De complexiteit heeft zowel betrekking op de geavanceerde en zich snel ontwikkelde technologie als de bestuurlijke constellatie waarin het geschil moet worden beoordeeld. Zij sluit zich in verband daarmee dan ook nadrukkelijk aan bij de observatie van de Evaluatiecommissie dat de TIB, de CTIVD en de betrokken Ministers zich in de eerste plaats moeten inspannen eventuele problemen en verschillen van opvatting binnen het stelsel zélf op te lossen.⁵⁸ De gang naar de Afdeling bestuursrechtspraak kan een uitkomst bieden als dit onverhoopt niet lukt, maar dient als uitzondering zeer spaarzaam aangewend te worden. Van een generieke herkansingsmogelijkheid van de Minister na een hem onwelgevallig bindend oordeel van één van de toezichthouders kan gelet op het voorgaande geen sprake zijn.

De Afdeling adviseert in de toelichting op het bovenstaande in te gaan.

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. 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 toelichting is in lijn met het voorgaande aangepast. Waar het gaat om de opmerking van de Afdeling dat de gang naar de Afdeling bestuursrechtspraak spaarzaam aangewend dient te worden en van een generieke herkansingsmogelijkheid van de Minister naar het oordeel van de Afdeling geen sprake kan zijn, wordt het volgende opgemerkt. In de beroepsregeling worden geen inhoudelijke voorwaarden gesteld aan de bevoegdheid van de Minister om beroep in te stellen tegen een oordeel van de TIB of de afdeling toezicht van de CTIVD. Het is dus aan de verantwoordelijke Minister om te bepalen of een specifieke zaak zich leent voor beoordeling door de Afdeling bestuursrechtspraak. De beroepsprocedure moet als een uitzonderlijke procedure worden gezien waartoe niet lichtvaardig zal worden besloten. Naar verwachting zal dan ook met name beroep worden ingesteld ten aanzien van meer principiële kwesties, zoals de uitleg van wettelijke begrippen en de invulling van de toetsingsnormen. De regeling is hiertoe echter niet beperkt.

6. Verkennende bevoegdheid ten behoeve van OOG-interceptie

a. Achtergrond: gerichtheid van kabelinterceptie

De Wiv 2017 introduceerde een verruiming van de interceptiebevoegdheid zodat ook interceptie op de kabel mogelijk werd, naast interceptie van niet-kabelgebonden communicatie.⁵⁹ De interceptiebevoegdheid is in de huidige wet techniekonafhankelijk opgesteld en wordt aangeduid als onderzoeksopdrachtgerichte interceptie (OOG-interceptie). Met interceptie van niet-kabelgebonden communicatie werd op de bestaande bevoegdheid gedoeld om communicatie uit de ether te onderscheppen,

⁵⁸ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88, p. 5.

⁵⁹ Artikel 48 Wiv 2017.

zoals radio en satellietverkeer. In de aanloop naar de Wiv 2017 en na inwerkingtreding daarvan is het debat echter met name gegaan over interceptie van de kabel, nu dit een nieuwe bevoegdheid was.

Tijdens de totstandkoming van de Wiv 2017 en de daaropvolgende wijziging van de Wiv 2017 is sterk de nadruk gelegd op de gerichtheid van de OOG-interceptie. De motie-Recourt riep op tot het betrekken van de gerichtheid bij de OOG-interceptie.⁶⁰ Na het raadgevend referendum over de Wiv 2017 hebben de Ministers van BZK en Defensie beleidsregels vastgesteld, waaronder een beleidsregel over de zo gericht mogelijke inzet van bijzondere bevoegdheden. Het gerichtheidsvereiste is vervolgens gecodificeerd met de wijziging van de Wiv 2017.⁶¹ Dat ook kabelinterceptie zo gericht mogelijk dient te zijn, neemt niet weg dat kabelinterceptie inherent een grote mate van ongerichtheid kent; dat betekent dat communicatie in bulk wordt onderschept.⁶²

b. Kabelinterceptie en verkenning van de kabel

Kabelinterceptie verloopt in grote lijnen als volgt. Eerst wordt een «accesslocatie» geoperationaliseerd, een fysiek ontvangstpunt bij een aanbieder.⁶³ Dan maken de diensten een keuze uit de aanwezige glasvezels, of «fibers» van een kabel. Binnen de fibers kunnen weer verschillende kanalen te onderscheiden zijn. Relevante fibers en kanalen worden langs deze weg onderschept. Na interceptie van de gegevens vindt filtering plaats. Er wordt negatief gefilterd: op basis van bepaalde kenmerken worden bepaalde gegevens niet opgeslagen. Met positieve filtering worden op basis van bepaalde kenmerken gegevens juist wel opgeslagen. Na filtering worden de gegevens onderzocht om de interceptie te optimaliseren, en vervolgens geselecteerd om te worden gebruikt voor inlichtingendoeleinden.⁶⁴ Kabelinterceptie is tot nu toe slechts beperkt ingezet, met name voor het «snapshotten» (het verkennen van de kabel).

De wetgever heeft bij de totstandkoming van de Wiv 2017 en de wijziging daarvan nadien besloten dat de kabelinterceptie (met inbegrip van de verkennende fase) zo gericht mogelijk moet zijn, nu zij ongericht onderscheppen toen ongewenst achtte. De diensten zouden op grond van de wettelijke informatieplicht die geldt voor aanbieders van communicatiediensten voldoende kennis moeten vergaren om de kabelinterceptie zo gericht mogelijk te laten plaatsvinden. Zoals de CTIVD beschrijft en ook de Evaluatiecommissie uitvoerig uiteenzet, is inmiddels in de praktijk gebleken dat dit niet goed mogelijk is, omdat de op dat moment beschikbare informatie onvoldoende inzicht geeft in de aard van het verkeer, en de aannames op basis van deze informatie niet altijd kloppen.⁶⁵ Daarvoor is eerst nodig om de kabel ongericht te intercepteren om vervolgens op grond daarvan te bepalen of en zo ja, op welke wijze een gegevensstroom relevant kan zijn voor de concrete onderzoeksvraag.

⁶⁰ Kamerstukken II 2016/17, 34 588, nr. 66.

⁶¹ Artikel 26, vijfde lid Wiv 2017, Staatsblad 2021, 300.

⁶² CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224, p. 12.

⁶³ Artikel 52 Wiv 2017.

⁶⁴ Respectievelijk artikel 49, eerste lid, en artikel 49, tweede lid, Wiv 2017. Zie hier uitgebreid CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224.

⁶⁵ CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224, p. 54.

Verkenning van de kabel kent onder de Wiv 2017 echter geen zelfstandige wettelijke grondslag. Dit betekent dat verkennen slechts kan onder de voorwaarden van de wel in de wet geregelde kabelinterceptie: verkennen moet in dat kader zo gericht mogelijk zijn. De CTIVD beschrijft in haar recente rapport dat daarmee een probleem ontstaat: de wettelijke vereisten die van toepassing zijn op interceptie worden onverkort toegepast. Daarmee wordt voorbij gegaan aan het doel van snapshotten. Dit zou juist een brede inzet vereisen, zodat de daaropvolgende fase zo gericht mogelijk kan worden uitgevoerd.⁶⁶ Het voorstel regelt daarom een zelfstandige grondslag om voorafgaand aan de kabelinterceptie van artikel 48 de kabel eerst te kunnen verkennen om zo de toestemmingsaanvraag voor kabelinterceptie te voorzien van een betere, technische onderbouwing.⁶⁷ In de nu voorgestelde bepaling die de zelfstandige grondslag regelt, blijft het gerichtheidsvereiste gelet op het voorgaande buiten toepassing.⁶⁸

Het voorgaande betekent dat het wetsvoorstel de (al bestaande) verkenningbevoegdheid expliciteert⁶⁹ maar deze vanwege de ongerichtheid van deze verkennende fase ook verruimt. De Afdeling erkent de ingrijpendheid daarvan, mede in het licht van de eerder gemaakte politieke keuze. In dat verband is essentieel dat de ongerichte verkenning geen doel op zichzelf is, maar uitsluitend in dienst staat van het mogelijk maken van een zo gericht mogelijke OOG-interceptie. Voorts wijst de Afdeling op de betekenisvolle waarborgen waarmee de bevoegdheid is omkleed. Een belangrijke waarborg die in het wetsvoorstel is opgenomen is met name dat de met de verkenning verworven gegevens niet voor inlichtingdoeleinden verwerkt mogen worden. Deze worden alleen benut om vast te stellen welke gegevensstromen van belang zijn. Gelet daarop en in het licht van de inmiddels in de praktijk geconstateerde knelpunten (zie hiervoor) acht de Afdeling het begrijpelijk dat, anders dan tijdens de behandeling van de Wiv 2017 en de wijziging van de Wiv 2017 destijds, op basis van de toen bestaande inzichten, is besproken, nu wordt gekozen voor de hiervoor geschetste benadering.⁷⁰

Dat neemt niet weg dat het wetsvoorstel op bepaalde punten verbetering behoeft. Met het oog daarop maakt de Afdeling hierna enkele opmerkingen over de van toepassing zijnde waarborgen die moeten leiden tot aanpassing van het voorstel. Deze hebben betrekking op de techniekonafhankelijkheid van de voorgestelde bepaling, de van toepassing zijnde waarborgen en de grenzen daarvan (onderdelen c-f).

c. Techniekonafhankelijkheid

Zoals de toelichting aangeeft, geldt de voorgestelde regeling van de verkenningsbevoegdheid voor beide vormen van OOG-interceptie: op zowel kabel- als etherinterceptie.⁷¹ Aanleiding voor regeling van de verkennende bevoegdheid is echter de problematiek die zich voordeed bij de kabelinterceptie, een nieuwe bevoegdheid bij de inwerkingtreding van

⁶⁶ CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224, p. 54.

⁶⁷ Voorgesteld artikel 7.

⁶⁸ Voorgesteld artikel 7, vierde lid.

⁶⁹ Zie Kamerstukken II 2016/17, 34 588, nr. 3, p. 81 (MvT Wiv 2017), p. 110.

⁷⁰ Dat wil overigens niet zeggen dat de introductie van de verkennende bevoegdheid niet betekent dat daarmee de interceptie minder intensief wordt, zoals de toelichting ook vermeldt. Zie memorie van toelichting, paragraaf 3.3.2.

⁷¹ Memorie van toelichting, paragraaf 3.3.1.

de Wiv 2017. De toelichting spitst zich daarom toe op de verkennende bevoegdheid ten behoeve van de kabelinterceptie.⁷²

De Afdeling constateert dat hiermee onduidelijk blijft wat de verkennende bevoegdheid specifiek betekent voor etherinterceptie. Indien deze verkennende bevoegdheid niet noodzakelijk is voor de goede uitvoering van de etherinterceptie, dan zou deze gelet op het proportionaliteitsvereiste niet verleend moeten worden. De Afdeling adviseert in dat geval enkel een regeling te treffen voor een verkennende bevoegdheid ten behoeve van kabelinterceptie en niet voor etherinterceptie.

De Afdeling adviseert het voorstel in deze zin aan te passen, tenzij alsnog wordt gemotiveerd dat deze bevoegdheid ook noodzakelijk is voor etherinterceptie.

Het belang van de verkennende bevoegdheid is voor zowel OOG-interceptie van de kabel als uit de ether even groot. Hoewel de in de toelichting beschreven problematiek zich tot op heden vooral voordoet bij OOG-interceptie van de kabel, is het uitgangspunt nog steeds dat wettelijke bepalingen zo veel mogelijk techniekonafhankelijk moeten worden geformuleerd. In de toelichting is gemotiveerd dat het introduceren van de verkennende bevoegdheid voor zowel OOG-interceptie van de kabel als uit de ether noodzakelijk is. Hoewel de bevoegdheid tot kabel- en etherinterceptie in aard en omvang verschillen, is het doel en het belang van verkennen van zowel kabelgebonden- als etherverkeer gelijk, namelijk zorgen voor het onderbouwen van een toestemmingsaanvraag voor interceptie ten behoeve van het inlichtingenproces.

d. Bewaartermijn

Het verkennen van de kabel gebeurt nu nog onder de wettelijke voorwaarden voor de kabelinterceptie zoals geregeld in de Wiv 2017. Voortvloeiend uit de wettelijke bewaartermijn voor gegevens verkregen uit OOG-interceptie worden bij het verkennen van de kabel de geïntercepteerde gegevens op dit moment maximaal één jaar opgeslagen.⁷³ Dit betekent dat de Wiv 2017 voor de gegevens die zijn verkregen in de verkennende fase geen specifieke, daarop toegespitste bewaartermijn kent.

Het voorstel regelt naast de zelfstandige grondslag voor het verkennen een aantal waarborgen die gepaard gaan met de inzet ervan. Eén van die waarborgen is dat de bij de verkenning verworven (bulk)data na een periode van ten hoogste twaalf maanden worden vernietigd, voor zover zij niet relevant zijn voor het doel om vast te stellen op welke gegevensstromen een verzoek om toestemming voor kabelinterceptie betrekking dient te hebben.⁷⁴ Volgens de toelichting wijst de praktijk uit dat een bovengrens voor de bruikbaarheid van de gegevens 12 maanden blijkt te zijn.⁷⁵

In het kader van de techniekonafhankelijke opstelling van de bepaling rijst de vraag in hoeverre daadwerkelijk een bovengrens van 12 maanden voor gegevens verworven uit verkenning van de kabel noodzakelijk is en of in

⁷² Memorie van toelichting, paragraaf 3.3.1.

⁷³ CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224 p. 33. Er wordt vanuit gegaan dat na een jaar het doel zou moeten zijn behaald, en een verlenging van de bewaartermijn (wat wettelijk mogelijk is voor gegevens verkregen uit OOG-interceptie) daarom niet in de lijn der verwachting is.

⁷⁴ Voorgesteld artikel 7, zesde lid.

⁷⁵ Memorie van toelichting, paragraaf 3.3.2.

dat kader niet kan worden volstaan met een kortere bewaartermijn. Zo blijkt bijvoorbeeld uit de beschreven waarborgen in het rapport van de CTIVD dat minimaal de helft van de gegenereerde metadata binnen drie maanden dienden te zijn vernietigd. De toelichting gaat hier niet op in.

De Afdeling wijst hierbij op jurisprudentie van het EHRM, waarin het Hof van oordeel is dat het wenselijk is om als in de praktijk een kortere bewaartermijn wordt gehanteerd dit tot uitdrukking te laten komen in wet- en regelgeving.⁷⁶ Gelet op de aanmerkelijke verruiming die de nieuwe verkennende bevoegdheid vanwege de ongerichtheid daarvan met zich brengt en de daarmee gepaard gaande inbreuk op het recht op de bescherming van de persoonlijke levenssfeer alsmede gelet op de tijdelijkheid van deze wet is het noodzakelijk in deze bepaling zo concreet mogelijk aan te geven wat de maximale bewaartermijn kan zijn voor de (bulk)data die wordt verkregen met het verkennen van de kabel.

De Afdeling adviseert in het voorstel een kortere bewaartermijn op te nemen voor verworven gegevens door kabelinterceptie, tenzij dragend kan worden gemotiveerd dat een langere termijn ook voor de kabel noodzakelijk is.

Aan dit advies is gevolg gegeven door in artikel 6, zesde lid, (voorheen artikel 7, zesde lid) een maximale termijn van zes maanden op te nemen. Daarna worden de gegevens vernietigd, voor zover deze niet bijdragen aan het doel van de verwerking.

e. Relevantie

De (bulk)data die in het kader van de verkenning is verworven, worden niet verwerkt voor inlichtingendoelinden («productie»). Zij worden na maximaal 12 maanden verwijderd, «voor zover de gegevens niet relevant zijn voor het doel van de verwerking».⁷⁷ Het doel van de verwerking is, ingevolge het voorstel, vast te stellen op welke gegevensstromen een verzoek om toestemming tot kabelinterceptie betrekking dient te hebben.⁷⁸

«Relevant verklaren» onder de Wiv 2017 heeft tot gevolg dat gegevens verkregen uit bijzondere bevoegdheden mogen worden bewaard en slechts worden vernietigd als zij geen betekenis (meer) hebben. De Afdeling begrijpt het «relevant verklaren» in de context van de nu voorgestelde verkenningsbevoegdheid echter zo dat niet wordt beoogd deze gegevens – voor zover zij relevant worden verklaard – voor de «productie» beschikbaar te stellen, maar dat deze in dat geval slechts beschikbaar blijven voor de voor de interceptie noodzakelijke toestemmingaanvraag. Het recente rapport van de CTIVD is daarmee in lijn; zij meldde daarin dat in die situatie slechts bij hoge uitzondering gegevens relevant werden verklaard, namelijk voor zover dat onvermijdelijk was met het oog op de beoordeling van de potentiële inlichtingenwaarde van een specifieke datastroom. Ook hier kwamen de gegevens in deze fase, parallel aan hetgeen thans wordt voorgesteld voor de met uitoefening van de verkenningsbevoegdheid verworven gegevens, niet ter beschikking van inlichtingenteams.⁷⁹

⁷⁶ EHRM 25 mei 2021 (GK), Big Brother Watch t. Verenigd Koninkrijk, nrs. 58170/13 62322/14 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, paragraaf 403 en 423.

⁷⁷ Voorgesteld artikel 7, zesde lid.

⁷⁸ Voorgesteld artikel 7, eerste lid.

⁷⁹ CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224, p. 34.

Uit het voorgaande kan worden afgeleid dat «relevant verklaren» in de context van de verkenning van de kabel een andere betekenis heeft dan met het oog op de kabelinterceptie die daarop eventueel volgt. De toelichting gaat echter op dit mogelijke verschil in betekenis niet in. De Afdeling acht verheldering hier noodzakelijk. Daarbij is essentieel dat het niet verder verwerken van de bij de verkenning verkregen gegevens voor inlichtingendoeleinden een noodzakelijke waarborg is om zo de inbreuk op het recht op bescherming van de persoonlijke levenssfeer zo beperkt mogelijk te laten zijn.

De Afdeling adviseert in de toelichting in te gaan op de betekenis van het relevant verklaren.

Met de Afdeling ben ik van mening dat de term «relevant» in deze context niet geschikt is, omdat deze term onder de Wiv 2017 de betekenis heeft dat de gegevens mogen worden gebruikt bij de beantwoording van onderzoeksvragen. De term «relevant» is in de context van data die worden verworven en gebruikt voor het doel van verkennen op de kabel niet geschikt, omdat bij deze bevoegdheid de strikte waarborg geldt dat verworven data niet beschikbaar komt voor het inlichtingenproces. In artikel 6, zesde lid, (voorheen artikel 7, zesde lid) is bepaald dat de gegevens na een maximale termijn van 6 maanden worden vernietigd voor zover deze niet hebben bijgedragen aan het doel van de verwerking. Met deze bijdrage wordt bedoeld dat deze gegevens in de uiteindelijke toestemmingsaanvraag voor OOG-interceptie worden gebruikt bij de indicatie van de te verwerven gegevensstromen.

f. Uitwisseling gegevens met buitenlandse diensten

Het voorstel schrijft voor dat (bulk)data die wordt verkregen door middel van de verkennende bevoegdheid, niet mogen worden verwerkt voor andere doeleinden dan het doel vast te stellen op welke gegevensstromen een verzoek om toestemming voor OOG-interceptie betrekking dient te hebben.⁸⁰ De toelichting gaat niet in op de vraag of en onder welke voorwaarden (bulk)data die tijdens de verkenning zijn verkregen, mogen worden uitgewisseld met buitenlandse inlichtingendiensten.

Ingevolge de Wiv 2017 is het in beginsel mogelijk om gegevens uit te wisselen met buitenlandse inlichtingendiensten. Onder voorwaarden mag ook (bulk)data die nog niet is onderzocht (ongeëvalueerde gegevens) met buitenlandse diensten worden uitgewisseld. Uit het voorstel blijkt niet of dit ook is toegestaan voor de bulkdata die wordt verkregen met de verkennende bevoegdheid. De vraag rijst in dat kader ook of hier sprake is van een verschil tussen kabelinterceptie en etherinterceptie. Van belang daarbij is dat bij etherinterceptie in de nabije toekomst sprake zal zijn van grensoverschrijdende samenwerking met een buitenlandse dienst aangezien enkele satellietshotels op korte termijn zullen worden verplaatst naar het buitenland.⁸¹

De (bulk)data die wordt verkregen door middel van de verkennende bevoegdheid leent zich niet voor uitwisseling met buitenlandse diensten. Het betreft immers gegevens die ook de Nederlandse inlichtingendiensten binnen de eigen rechtsorde niet verder mogen verwerken. Bovendien is overdracht van deze gegevens, mede gelet op de ongerichtheid van de

⁸⁰ Voorgesteld artikel 7, zesde lid.

⁸¹ Kamerstukken II 2020/21, 29 924, nr. 213.

verkenningbevoegdheid, een ernstige inbreuk op het recht op de bescherming van de persoonlijke levenssfeer.⁸²

De Afdeling adviseert in het licht van het voorgaande in het voorstel te regelen dat deze gegevens niet mogen worden uitgewisseld met buitenlandse diensten.

Door de Afdeling wordt er terecht op gewezen dat in het zesde lid van artikel 7 (thans vernummerd naar artikel 6) is voorgesteld dat gegevens die zijn verworven op grond van de in artikel 7, eerste lid, (thans vernummerd naar artikel 6, eerste lid) genoemde bevoegdheid niet worden verwerkt voor andere doeleinden dan waarvoor de bevoegdheid bedoeld is. In de toelichting is nader uiteengezet waarom het van groot belang is dat er een mogelijkheid blijft bestaan om gegevens verworven met de bevoegdheid van verkennen te delen met buitenlandse diensten maar dan enkel en alleen ten behoeve van technisch onderzoek. Het uitgangspunt is dus dat deze gegevens voor geen enkel ander doel dan voornoemd doel worden verstrekt aan een buitenlandse collegadienst. Toegelicht wordt dat het doel van de verkenningbevoegdheid is omschreven in het eerste lid, te weten het vaststellen op welke gegevensstromen een uiteindelijk verzoek tot OOG-kabelinterceptie (artikel 48 Wiv 2017) betrekking dient te hebben. De geïntercepteerde gegevens moeten hiervoor technisch worden onderzocht, zodat de verworven gegevens kunnen worden gestructureerd, geanalyseerd en geduid. In het kader van dit technisch onderzoek is het soms noodzakelijk ondersteuning te krijgen van een buitenlandse collegadienst. Er zijn namelijk situaties denkbaar waarin een buitenlandse collegadienst beschikt over kennis of technische mogelijkheden waar Nederland (nog) niet over beschikt. Hierbij worden de voor dat technisch onderzoek benodigde gegevens aan de desbetreffende collegadienst verstrekt. Deze verstrekking vindt plaats met het expliciete verbod deze gegevens te gebruiken voor inlichtingendoel-einden. De AIVD en de MIVD zijn immers ook gebonden aan deze waarborg bij de uitoefening van de bevoegdheid. Daarnaast zijn de kaders en waarborgen omtrent internationale samenwerking die voortvloeien uit de Wiv 2017 onverkort van toepassing. Deze gegevens mogen dus voor geen enkel ander doel worden verstrekt aan een buitenlandse collegadienst.

7. Toetsingskader OOG-interceptie

De Wiv 2017 bevat een afwegingskader voor de verzameling van gegevens in het kader van de inzet van de aan de diensten toegekende bevoegdheden. In dit afwegingskader zijn het proportionaliteits-, subsidiariteits- en gerichtheidsvereiste gecodificeerd.⁸³ Bij de toetsing op rechtmatigheid van toestemming voor de inzet van bevoegdheden toetst de TIB hieraan. Het voorstel voorziet in verduidelijking van het gerichtheids- en proportionaliteitsvereiste in het kader van toestemming voor OOG-interceptie. De toets dient met name (zwaarwegend) te betrekken:

- (i) Een indicatie van de te verwerven gegevensstromen. Hiermee wordt de feitelijke, technische aanduiding van de te intercepteren gegevensstromen bedoeld.⁸⁴*
- (ii) Een indicatie van de wijze waarop de reductie van gegevens binnen de gehele keten van verwerving invulling krijgt. Volgens de toelichting zijn gegevensstromen dynamisch en moeten filters (voor datareductie)*

⁸² Zie ook Advies van de Afdeling advisering van 21 september 2016 over de Wiv 2017 (W04.16.0097/l), Kamerstukken II 2016/17, 34 588, nr. 4, punt 4i.

⁸³ Artikel 26 Wiv 2017.

⁸⁴ Voorgesteld artikel 8 en memorie van toelichting, paragraaf 3.3.3.

voortdurend worden aangepast. Daarom kan vooraf slechts een indicatie worden gegeven op welke wijze gegevens worden gereduceerd.⁸⁵

In het verleden heeft de Minister aangegeven dat data waarvan aan de buitenkant te zien is dat ze niet relevant zijn niet worden opgeslagen (negatieve filtering, zie punt 5b).⁸⁶ Dit betrof bijvoorbeeld de data van streamingdiensten als Netflix en Youtube, en BitTorrentverkeer,⁸⁷ maar ook veel webbrowsereactiviteiten en Facebookverkeer. Dit leidde ertoe dat de TIB verlengingsverzoeken van de diensten die daarop betrekking hadden als onrechtmatig beoordeelde, omdat zij in strijd waren met de toezeggingen omtrent negatieve filtering.⁸⁸ Dat betekende dat volgens de TIB deze data niet zouden moeten worden opgeslagen.

Met het voorstel wordt dit als gevolg van veranderde inzichten hernomen: expliciet wordt aangegeven dat gegevensstromen (zoals streamingdiensten) niet op voorhand kunnen worden aangemerkt als niet-relevant.⁸⁹ Deze veranderde inzichten zijn op de toezichtspraktijk gebaseerd; ook de CTIVD stelt dat in het kader van het vinden van ongekende targets gegevens als streamingdiensten en BitTorrentverkeer mogelijk wel relevant kunnen zijn.⁹⁰ De toelichting geeft dan ook aan dat de diensten per geval een afweging kunnen maken welke gegevens gefilterd moeten worden en welke niet.⁹¹

De Afdeling begrijpt dat het niet altijd mogelijk zal zijn categorisch bepaalde gegevensstromen uit te sluiten. Tegelijkertijd constateert zij dat de genoemde gegevensstromen verschillende typen diensten inhouden, zoals video-on-demand-platformen (zoals Netflix), videoplatformdiensten (zoals Youtube), en sociale media (zoals Facebook). Daarmee rijst de vraag of het in het kader van de afweging tussen het recht op de bescherming van de persoonlijke levenssfeer en operationele belangen niet mogelijk is te differentiëren tussen de verschillende diensten. Een nadere toelichting hierbij is ook noodzakelijk voor de praktijk van de toezichthouder die de afweging van de diensten aan de wettelijke criteria zal moeten toetsen.

De Afdeling adviseert in de toelichting op het voorgaande in te gaan.

In de toelichting wordt uiteengezet dat kabelinterceptie bestaat uit verschillende stappen: de keten van verwerving. Het begint met het overnemen (kopiëren) van de in de toestemming aangeduide gegevensstromen. Deze gegevensstromen worden vervolgens gefilterd. Het doel van filtering is om gegevens te verwerven die later op enigerlei wijze een bijdrage kunnen leveren aan het beantwoorden van onderzoeksvragen. Het eindresultaat van dit proces leidt tot de gegevens die voor de diensten toegankelijk zijn bij het beantwoorden van onderzoeksvragen. Deze gehele keten van verwerven moet dus gezien worden als een proces van datareductie. Gegevensstromen zijn dynamisch en wijzigen voortdurend. De filters moeten daarop worden aangepast. Daarom kan bij de aanvraag voor het inzetten van het middel slechts een indicatie worden gegeven

⁸⁵ Voorgesteld artikel 8 en memorie van toelichting, paragraaf 3.3.3.

⁸⁶ Kamerstukken II 2016/17, 34 588, nr. 18, p. 71, en bijlage bij Kamerstukken II 2017/18, 34 588, nr. 69.

⁸⁷ Hiermee kunnen gebruikers onderling gegevens uitwisselen.

⁸⁸ TIB, Verkort jaarverslag 2019/20, bijlage bij Kamerstukken II 2019/20, 29 924, nr. 199, hoofdstuk 5.2.

⁸⁹ Memorie van toelichting, paragraaf 3.3.3.

⁹⁰ CTIVD, Toezichtsrapport over de inzet van kabelinterceptie door de AIVD en de MIVD: De snapshotfase (rapport 75), 26 januari 2022, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 224, p. 55.

⁹¹ Memorie van toelichting, paragraaf 3.3.3.

voor de wijze waarop de diensten van plan zijn om de gegevens te reduceren. Op de uitvoering van dit gehele proces houdt de afdeling toezicht van de CTIVD toezicht. Na inwerkingtreding van de Wiv 2017 is de eerste praktijkervaring opgedaan met kabelinterceptie. Uit deze praktijkervaring is gebleken dat actoren gebruik maken van veel verschillende protocollen en technieken om hun offensieve cyberprogramma uit te voeren en hun activiteiten te verhullen. Tevens innoveren deze actoren voortdurend hun werkwijze om hun offensieve doelen beter te bereiken en niet te worden onderkend. Bij het inzetten van kabelinterceptie ten behoeve van een onderzoek moet een indicatie gegeven worden van de reductie van gegevens.

Gelet op de hiervoor beschreven veranderlijke methode, is het niet mogelijk om op voorhand en categorisch gegevensstromen uit te sluiten van interceptie. Om het middel effectief ten behoeve van een onderzoek in te zetten, is het dus niet mogelijk 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. Het is van belang dat de diensten per geval een afweging kunnen maken welke gegevens gefilterd moeten worden en welke gegevens doorgelaten kunnen worden.

8. Bulkdatasets

a. *Inleiding*

Een bulkdataset wordt in het voorstel gedefinieerd als een omvangrijke gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden.⁹² In de Wiv 2017 bestaat geen specifiek regime voor bulkdatasets; de Wiv 2017 kent alleen bepalingen voor gegevens verworven via de in de wet geregelde bevoegdheden (waar ook bulkdata onder valt) en gegevens verworven uit de OOG-interceptie.

Voor de beoordeling van de verwerking van de betrokken gegevens gelden, afhankelijk van de fase, verschillende regimes. Gegevens, dus ook bulkdatasets, die verworven zijn door middel van bijzondere bevoegdheden moeten op grond van de Wiv 2017 zo spoedig mogelijk en binnen maximaal anderhalf jaar worden beoordeeld op relevantie (relevantie-regime). Niet-relevante gegevens worden vernietigd.⁹³ Gegevens die wel relevant zijn worden verwijderd als zij, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren (betekenis-regime).⁹⁴

Volgens de toelichting is de in de Wiv 2017 vastgelegde beoordelings-termijn van maximaal anderhalf jaar problematisch, omdat bulkdatasets vaak langer van waarde zijn dan de thans geldende maximale termijn van anderhalf jaar en ommekomst van de beoordelingstermijn er toe kan leiden dat mogelijk waardevolle gegevens moeten worden vernietigd.⁹⁵ Het voorstel regelt daarom dat in afwijking van de Wiv 2017 de beoordelingstermijn van bulkdatasets die verworven zijn met de uitoefening van

⁹² Voorgesteld artikel 1, sub d.

⁹³ Artikel 27, eerste lid, Wiv 2017.

⁹⁴ Artikel 20, eerste lid, Wiv 2017. Er zijn dus twee regimes voor gegevens verkregen uit bijzondere bevoegdheden: een relevantie-regime, en vervolgens een betekenisregime. Voor (bulk)data verkregen uit algemene bevoegdheden, zoals bijvoorbeeld verkregen via informanten, geldt alleen het betekenisregime. Zie uitgebreid rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 4.4.4.

⁹⁵ Memorie van toelichting, paragraaf 3.2.6.

een bijzondere bevoegdheid steeds met een jaar kan worden verlengd.⁹⁶ Het verzoek om toestemming daartoe wordt door het hoofd van de dienst aan de Minister gedaan. Het verzoek dient aan te geven waarom de bulkdataset voor een langere periode bewaard dient te worden. Op het proces van verlenging van de termijn als hiervoor bedoeld, houdt de CTIVD volgens het wetsvoorstel bindend toezicht.⁹⁷ De regeling is niet van toepassing op bulkdatasets die met behulp van OOG-interceptie zijn verworven, omdat deze bulkdata een eigen regeling kent in de Wiv 2017.

De afdeling toezicht van de CTIVD heeft eerder het in zijn geheel of grotendeels relevant beoordelen van bulkdatasets vanwege het aflopen van de beoordelingstermijn als onrechtmatig gekwalificeerd. De CTIVD onderkende weliswaar de operationele belangen om bulkdatasets langer te bewaren, maar was van oordeel dat de kern van bulkdata – dat zij gegevens bevat van personen en organisaties die geen onderwerp van onderzoek zijn – eraan in de weg staat dat zij in het geheel als relevant worden verklaard. De CTIVD beschouwt de wijze waarop bulkdatasets als relevant worden beoordeeld dan ook als een kunstgreep om de bewaartermijn van bulkdatasets te verlengen.⁹⁸ De Minister heeft de aanbevelingen van de CTIVD naar aanleiding van de onrechtmatigheidsverklaring niet opgevolgd.⁹⁹ Recent heeft de afdeling klachtbehandeling van de CTIVD naar aanleiding van een klacht van burgerrechtenvereniging Bits of Freedom bepaald dat de diensten niet zorgvuldig hebben gehandeld bij het periodiek (her)beoordelen van meerdere bulkdatasets. Deze bulkdatasets dienen te worden verwijderd en vernietigd.¹⁰⁰ Een beslissing van de afdeling klachtbehandeling is wel bindend. De Evaluatiecommissie heeft aan deze discussie uitgebreid aandacht besteed, en stelt voor een geheel nieuw bulkdataregime in te voeren.

b. Aansluiting bij evaluatie

De Evaluatiecommissie heeft in haar rapport een groot aantal aanbevelingen gedaan voor een nieuw bulkdataregime.¹⁰¹ Volgens de toelichting zullen de aanbevelingen worden meegenomen bij de brede herziening van de Wiv 2017. De verlengbare beoordelingstermijn die in dit voorstel wordt geregeld is in verband hiermee nadrukkelijk een tijdelijke oplossing dat bedoeld is om een belangrijk operationeel knelpunt op te lossen.¹⁰²

Gelet op de veelomvattende en integrale aanbevelingen van de Evaluatiecommissie constateert de Afdeling dat het voorstel slechts een zeer klein onderdeel van een eventueel bulkdataregime behelst. 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

⁹⁶ Voorgesteld artikel 6.

⁹⁷ Voorgesteld artikel 13, eerste lid, onder d.

⁹⁸ CTIVD, Voortgangsrapportage IV: De implementatie van de Wiv 2017 (rapport 69), 5 augustus 2020, p. 12.

⁹⁹ Kamerstukken II 2020/21, 29 924, nr. 203.

¹⁰⁰ Beslissing klacht Bits of Freedom over het handelen van de AIVD en de MIVD, 15 juni 2022, www.ctivd.nl.

¹⁰¹ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, aanbeveling 1–16.

¹⁰² Memorie van toelichting, paragraaf 3.2.6.

soorten bulkdatasets (zoals het onderscheid tussen registerbulkdata en gedragsbulkdata) niet noodzakelijk is.

De Afdeling adviseert in de toelichting nader te motiveren waarom niet wordt aangesloten bij de door de Evaluatiecommissie gedane aanbevelingen en of in dat verband de problematiek van de bulkdatasets niet in zijn geheel moet worden geregeld bij de herziening van de Wiv 2017.

De aanbevelingen van de ECW strekken ertoe te komen tot een geheel nieuw, uniform wettelijk kader voor de verwerking van bulkdatasets. De Afdeling geeft terecht aan dat verlenging van de bewaartermijn onlosmakelijk met de andere aanbevelingen is verbonden. 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. In het aan de Afdeling voorgelegde wetsvoorstel was een artikel (6 oud) opgenomen inzake de mogelijkheid om de bewaartermijn van bulkdatasets in verband met het uitvoeren van een relevantietoets telkens met een jaar te kunnen verlengen. Besloten is om dit artikel uit het wetsvoorstel te lichten, omdat de daarin voorziene verlengingsmogelijkheid niet beperkt dient te blijven tot de bulkdatasets die binnen de reikwijdte van het wetsvoorstel worden verworven maar een bredere toepassing dient te krijgen, namelijk voor de bulkdatasets die met bijzondere bevoegdheden bij de uitvoering van alle aan de AIVD en MIVD door de wetgever opgedragen taken worden verworven. Daartoe zal een nota van wijziging op onderhavig wetsvoorstel worden voorbereid. In deze nota van wijziging zal tevens geregeld worden dat een verleende toestemming voor het real time verzamelen van verkeers- en locatiegegevens (ook wel stomme tap genoemd) wordt onderworpen aan een rechtmatigheidstoets door de TIB.

c. Relevantie en betekenis

De CTIVD heeft eerder het in zijn geheel of grotendeels relevant verklaren van bulkdatasets vanwege het aflopen van de beoordelingstermijn als onrechtmatig gekwalificeerd.¹⁰³ De Afdeling merkt op dat met de voorgestelde regeling het onderscheid tussen het relevantie- en betekenisregime (zie onder punt a) lijkt te worden losgelaten. Zo hoeven de diensten niet meer (bulk)gegevens verkregen door de bijzondere bevoegdheden zo spoedig mogelijk op hun relevantie te beoordelen. De Afdeling begrijpt de regeling zo dat de beoordelingstermijn in beginsel oneindig kan worden verlengd, waarbij elk jaar zal worden bezien of de bulkdatasets voldoende bruikbaar zijn om de beoordelingstermijn met een jaar te verlengen. Daarmee ontbreekt een prikkel om de gegevens zo spoedig mogelijk op hun relevantie te beoordelen. Het knelpunt dat bulkdatasets na anderhalf jaar in zijn geheel of grotendeels als relevant worden beoordeeld, wordt hiermee weliswaar voorkomen, maar wordt tegelijkertijd ook verschoven. In de systematiek van het wetsvoorstel zal immers elk jaar de bruikbaarheid van de gegevens moeten worden beoordeeld, maar onduidelijk blijft op grond van welke criteria op dat moment getoetst moet worden.

De Afdeling adviseerde eerder om de bewaartermijn van bulkdatasets – weliswaar verkregen met OOG-interceptie – substantieel te verkorten, nu zij de kans klein achtte dat het EHRM in het kader van artikel 8 EVRM een termijn van drie jaar voor het bewaren van niet onderzochte bulkgegevens

¹⁰³ CTIVD, Voortgangsrapportage IV: De implementatie van de Wiv 2017 (rapport 69), 5 augustus 2020.

aanvaardbaar zou achten.¹⁰⁴ Zij wijst daarbij ook op jurisprudentie van het EHRM die de wenselijkheid benadrukte van een zo kort mogelijke bewaartermijn die in wet- en regelgeving dient te worden neergelegd.¹⁰⁵

Gelet op de inbreuk op de privacy van personen of organisaties die niet in onderzoek zijn en het feit dat deze ongeëvalueerde bulkdata mogelijk met buitenlandse inlichtingendiensten kan worden gedeeld¹⁰⁶, acht de Afdeling de voorgestelde regeling ontoereikend. Zij acht het noodzakelijk dat de wet met het oog op de beoordeling van het verlengingsverzoek objectieve toetsingscriteria bevat. Dergelijke criteria zijn ook essentieel voor de CTIVD bij de uitoefening van haar toezichtstaak, nu het relevantieregime zoals hiervoor geschetst in beginsel hier niet van toepassing lijkt te zijn.

Daarnaast rijst de vraag in hoeverre het aantal mogelijke verlengingen niet wettelijk gemaximeerd moet worden. Gelet op het recht op bescherming van de persoonlijke levenssfeer en de rechtspraak van het EHRM in dat kader, lijkt dat aangewezen. De toelichting gaat daar niet op in.

De Afdeling adviseert in het licht van het voorgaande het voorstel aan te passen.

Nu artikel 6 (oud) uit het wetsvoorstel is gelicht en het wetsvoorstel niet meer voorziet in de mogelijkheid tot verlenging van de bewaartermijn van met bijzondere bevoegdheden verworven bulkdatasets, is het niet meer opportuun om op hetgeen de Afdeling opmerkt met betrekking tot het opnemen van objectieve toetsingscriteria en een maximering van het aantal mogelijke verlengingen in te gaan. Wel zullen de door de Afdeling gemaakte opmerkingen worden betrokken bij de hiervoor aangekondigde nota van wijziging die nog op het wetsvoorstel zal worden uitgebracht.

9. Technische risico's

De Wiv 2017 bevat in het kader van de beoordeling van de inzet van de hackbevoegdheid een regeling die de diensten ertoe verplicht om vooraf de technische risico's (met inbegrip van gebruik van onbekende kwetsbaarheden) aan te geven. Onder dat wettelijk regime toetst de TIB op dit moment op het risico voor de beschikbaarheid en integriteit van het betrokken geautomatiseerd werk, en op het risico op misbruik door derden. Het laatste is met name van belang bij de inzet van onbekende kwetsbaarheden.¹⁰⁷

In het wetsvoorstel wordt bij het verzoek om toestemming voor het hacken het vereiste om een omschrijving van de technische risico's te geven buiten toepassing gelaten.¹⁰⁸ Volgens de toelichting zou het niet mogelijk zijn voorafgaand aan een toestemmingsperiode te voorspellen welke handelingen precies nodig zijn om met de inzet van het hacken het beoogde doel te bereiken. De eventuele technische risico's, die afhankelijk zijn van veel factoren, zijn daarom ook niet te voorzien, aldus de

¹⁰⁴ Advies van de Afdeling advisering van 21 september 2016 over de Wiv 2017 (W04.16.0097/I), Kamerstukken II 2016/17, 34 588, nr. 4, punt 4f.

¹⁰⁵ EHRM 25 mei 2021 (GK), Big Brother Watch t. Verenigd Koninkrijk, nrs. 58170/13 62322/14 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, paragraaf 405 en 423. Zie ook EHRM 4 december 2015, nr. 47143/06, Roman Zakharov t. Rusland, paragraaf 255.

¹⁰⁶ Artikel 89, tweede lid, Wiv 2017.

¹⁰⁷ Zie uitgebreid TIB, Jaarverslag 2021, bijlage bij Kamerstukken II 2021/22, 29 924, nr. 226, paragraaf 1.1.2.

¹⁰⁸ Voorgesteld artikel 5, eerste lid.

toelichting.¹⁰⁹ De TIB kan de technische risico's volgens het voorstel niet meer expliciet betrekken bij haar toetsing; dit gebeurt slechts bij de generieke proportionaliteitstoets.¹¹⁰ Daar staat tegenover dat ingevolge het voorstel de CTIVD op dit punt bindend toezicht kan uitoefenen.

Het voorstel om de eis om vooraf de technische risico's te omschrijven buiten toepassing te laten, is in de praktijk van het hacken vooral van belang als het gaat de inschatting van onbekende kwetsbaarheden. Een kwetsbaarheid is een fout in hard- of software, zoals bijvoorbeeld een fout in de code van software. Als de fout nog onbekend is, en dus niet is «gerepareerd» (gepatcht), kan deze worden gebruikt om te kunnen binnendringen in een geautomatiseerd werk (hacken). Dit is een keuze die in aanloop naar en tijdens de uitvoering van de hackbevoegdheid wordt gemaakt.¹¹¹ Volgens de toelichting is voorafgaand aan de uitvoering van de bevoegdheid veelal niet te voorzien of het daarvoor daadwerkelijk noodzakelijk is een onbekende kwetsbaarheid in te zetten, en is bovendien vaak enige spoed geboden. Met de wijziging hoeft het gebruik van onbekende kwetsbaarheden daarom niet meer te worden beschreven bij toestemmings- of verlengingsaanvragen.¹¹²

De Afdeling onderkent het spanningsveld tussen enerzijds de dynamiek van het hacken en anderzijds de statische ex ante-toetsing door de TIB. Desalniettemin ziet zij, evenals de Evaluatiecommissie, een belangrijke waarborg in het zoveel mogelijk vooraf omschrijven van technische risico's en het gebruik van onbekende kwetsbaarheden. Hacken is een bevoegdheid met mogelijk vergaande gevolgen voor derden, ook in het licht van de verruiming van de bijschrijfmogelijkheid (zie hierna onder punt 10). De Afdeling merkt op 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.

De Afdeling wijst daarbij op het voorstel van de Evaluatiecommissie om te differentiëren in de mate van detail van omschrijving van de technische risico's.¹¹³ Risico's die voorafgaand aan de inzet van de hackbevoegdheid al bekend zijn, kunnen zo worden meegewogen in de proportionaliteits- en subsidiariteitstoetsing door de TIB. Risico's die pas bij de uitvoering naar voren komen, kunnen dan in een later stadium worden onderworpen aan bindende toetsing door de CTIVD. In dit licht acht de Afdeling het noodzakelijk om in het voorstel op te nemen dat redelijkerwijs voorzienbare technische risico's, waaronder redelijkerwijs voorzienbaar gebruik van onbekende kwetsbaarheden, worden beschreven in de toestemmingsaanvraag.

De Afdeling adviseert het voorstel in deze zin aan te passen.

Naar aanleiding van dit advies is in de toelichting verduidelijkt dat in de toestemmingsaanvraag de technische risico's worden vermeld die op het moment van de aanvraag bekend zijn. Met deze aangescherpte formulering wordt onduidelijkheid over wat op welk moment al dan niet

¹⁰⁹ Memorie van toelichting, paragraaf 3.2.4.1.

¹¹⁰ Voorgesteld artikel 13, eerste lid, onder b. Memorie van toelichting, paragraaf 3.2.4.1.

¹¹¹ Memorie van toelichting, paragraaf 3.2.4.2. Zie voor het afwegingskader AIVD, «Beleid AIVD en MIVD over omgang met onbekende kwetsbaarheden», 1 mei 2018, via <https://www.aivd.nl/onderwerpen/onbekende-kwetsbaarheden/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden>.

¹¹² Memorie van toelichting, paragraaf 3.2.4.2.

¹¹³ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88, paragraaf 7.3.3.

redelijkerwijs voorzienbaar is voorkomen. Het gebruik van onbekende kwetsbaarheden hoeft binnen de reikwijdte van dit wetsvoorstel niet meer verplicht te worden beschreven bij toestemmings- of verlengingsaanvragen. In de toelichting is hierover opgenomen dat het gebruik van onbekende kwetsbaarheden één van de onderdelen is die mee worden genomen bij het inschatten van technische risico's. De technische risico's die zich tijdens de uitvoering concreet voordoen zijn onderworpen aan bindend toezicht door de CTIVD. Dit geldt ook voor het gebruik van onbekende kwetsbaarheden. Voor het gebruik van onbekende kwetsbaarheden geldt eveneens dat het voorafgaand aan de uitvoering van de bevoegdheid veelal niet te voorzien is of het daadwerkelijk noodzakelijk is een onbekende kwetsbaarheid in te zetten. Ook bij de inzet van onbekende kwetsbaarheden is vaak enige spoed geboden om gebruik te kunnen maken van een operationele kans en/of snel sporen uit te wissen. De CTIVD kan met bindend toezicht gedurende de gehele uitvoering effectief toezicht houden, aangezien dit toezicht niet gebonden is aan een specifiek moment en doorlopend is.

Waar het opnemen van de beschrijving van technische risico's in de aanvraag voor toestemming onder de Wiv 2017 een apart wettelijk vereiste is vervalt dit onder de Tijdelijke Wet. Het vermelden in de toestemmingsaanvraag van de op het moment van de aanvraag bekende technische risico's vindt immers plaats in het licht van de in de aanvraag te verantwoorden proportionaliteitstoets. Het laten vervallen van het wettelijk vereiste, dat voor meerdere uitleg vatbaar is, strekt ertoe om te benadrukken dat volstaan kan worden met hetgeen in de aanvraag in het kader van de proportionaliteitstoets is gesteld.

10. Verruiming van de bijschrijfmogelijkheid

a. Verschillende vormen

Bijschrijven houdt in dat toestemming voor de inzet van een bevoegdheid ook geldt voor een ander geautomatiseerd werk, nummer of technisch kenmerk dat een target gebruikt. Er hoeft daarvoor dan geen aparte toestemmingsprocedure te worden gevolgd. Het voorstel voorziet in uitbreiding van de bijschrijfmogelijkheden op drie onderdelen:

- i. In het kader van de hackbevoegdheid: het bijschrijven van andere geautomatiseerde werken die door het target of een derde in gebruik zijn;¹¹⁴*
- ii. In het kader van gericht tappen: het bijschrijven van andere nummers of technische kenmerken die door een persoon of organisatie in gebruik worden genomen;¹¹⁵*
- iii. In het kader van het opvragen van gegevens bij aanbieders van telecommunicatie- en opslagdiensten: het aan de hand van andere nummers of technische kenmerken opvragen van gegevens, of het opvragen van gegevens bij andere aanbieders.¹¹⁶*

De derde bijschrijfmogelijkheid is geheel nieuw. Volgens de Evaluatiecommissie is een bijschrijfmogelijkheid in het kader van het opvragen van gegevens minder indringend dan bijvoorbeeld bijschrijven in het kader van de hackbevoegdheid, doordat in het eerstgenoemde geval aanbieders vooraf worden geïnformeerd en er niet heimelijk wordt binnenge-

¹¹⁴ Voorgesteld artikel 5, tweede lid, en artikel 45, achtste lid, Wiv 2017.

¹¹⁵ Voorgesteld artikel 10, en artikel 47, zevende lid, Wiv 2017. Onder een tap valt een telefoontap, een internettap of een microfoon.

¹¹⁶ Voorgesteld artikel 11, en artikel 54 Wiv 2017.

drongen.¹¹⁷ Ook de TIB ziet het ontbreken van de bijschrijfmogelijkheid als een hiaat in de wet.¹¹⁸

In dit licht acht de Afdeling het opnemen van deze nieuwe bijschrijfmogelijkheid gerechtvaardigd.¹¹⁹ De eerste en tweede bijschrijfmogelijkheden zijn daarentegen herformuleringen van de al bestaande bijschrijfmogelijkheden in de Wiv 2017. De Afdeling gaat daar in punt b op in.

b. Exclusiviteitsvereiste

In de Wiv 2017 wordt gesproken over toestemming die wordt verleend voor het binnendringen van geautomatiseerde werken, of het ontvangen of opnemen van telecommunicatie via nummers of technische kenmerken van een persoon of organisatie. In het kader van de hackbevoegdheid gaat het bij de reeds bestaande bijschrijfmogelijkheid om een target die gebruik gaat maken van een ander (aan hem toebehorend) geautomatiseerd werk, dat in de plaats treedt van het eerste geautomatiseerde werk of waar hij aanvullend gebruik van maakt. Ook ziet de bestaande bijschrijfmogelijkheid in het kader van de hackbevoegdheid op het hacken via het geautomatiseerde werk van een derde (een partij die geen target is van de diensten). Ook hier gaat het om werken die in de plaats treden van of een aanvulling zijn op het geautomatiseerde werk waar oorspronkelijk toestemming voor is verleend.¹²⁰

In het kader van tappen gaat het bij de reeds bestaande bijschrijfmogelijkheid om nummers en technische kenmerken die toebehoren aan de desbetreffende persoon of organisatie die na de toestemmingsverlening bekend worden. Als het target gebruik maakt van een nummer of technisch kenmerk dat aan een andere persoon of organisatie toebehoort, dient hiervoor wel toestemming te worden verkregen. Dit geldt ook voor bijschrijven in het kader van de hackbevoegdheid: voor nieuwe derden moet opnieuw toestemming worden verkregen.¹²¹

De TIB legt deze bijschrijfmogelijkheden in de Wiv 2017 zo uit dat sprake moet zijn van apparaten die exclusief aan die persoon of organisatie toebehoren. Dat wil zeggen, als een geautomatiseerd werk uitsluitend wordt gebruikt door het target of de derde waarop de toestemmingsaanvraag zag, dan mag dit werk worden bijgeschreven.¹²² De regering acht dit problematisch omdat cyberactoren vaak gebruik maken van een gedeelde infrastructuur, zodat bijschrijven, gegeven deze uitleg, vrijwel onmogelijk wordt.¹²³ Er is dan immers geen sprake van exclusief gebruik.

De Evaluatiecommissie aarzelt bij het exclusiviteitsvereiste in het licht van technologische ontwikkelingen.¹²⁴ Zij beveelt de wetgever aan om een werkbare uitleg te geven wanneer een geautomatiseerd werk «in gebruik is» van een actor. Tegelijkertijd benadrukt zij het belang van de toetsing

¹¹⁷ Artikel 54 Wiv 2017. Zie hier rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 7.3.6.

¹¹⁸ Memorie van toelichting, paragraaf 3.5 en rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 7.3.6.

¹¹⁹ Memorie van toelichting, paragraaf 3.5.

¹²⁰ Kamerstukken II 2016/17, 34 588, nr. 3, p. 81 (MvT Wiv 2017).

¹²¹ Kamerstukken II 2016/17, 34 588, nr. 3, p. 81 en 88 (MvT Wiv 2017). Zie ook rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, p. 90.

¹²² Zie rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 7.3.5.

¹²³ Memorie van toelichting, paragraaf 3.2.5.

¹²⁴ De Evaluatiecommissie noemt als voorbeeld het gebruik van virtuele computers op gedeelde servers. Deze virtuele computers kunnen qua functionaliteit in exclusief gebruik zijn, maar draaien op een infrastructuur die in bezit is van een andere partij (rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken 2020/21, 34 588, nr. 88, paragraaf 7.3.5).

van de TIB op aanvragen die zien op nieuwe derden. De Evaluatiecommissie moedigt de diensten in dat kader voorts aan om zo nodig interne procedures te verkorten en gebruik te maken van de spoedprocedure.¹²⁵ In de toelichting blijven deze aanbevelingen grotendeels onbesproken. De toelichting verduidelijkt wel dat «in gebruik zijn» inhoudt dat geen sprake hoeft te zijn van exclusief gebruik, maar operationaliseert deze term verder niet. De toelichting gaat verder op de mogelijkheid van een spoedprocedure niet in.

De herformulering («in gebruik is») in het voorstel maakt duidelijk dat niet is vereist dat sprake is van exclusief gebruik om te kunnen bijschrijven, zo stelt de toelichting. Dit geldt voor alle drie de bijschrijfmogelijkheden. Dit betekent dat ingevolge het voorstel geautomatiseerde werken die naast de actor ook door anderen worden gebruikt, ook kunnen worden bijgeschreven.¹²⁶ Als de Afdeling het goed ziet, zouden door dit voorstel sneller nieuwe derden bijgeschreven kunnen worden als het target wisselt van infrastructuur die wordt gedeeld met of in bezit is van derden omdat toestemming in die gevallen niet meer is vereist.

De Afdeling heeft eerder geadviseerd om bij het binnendringen van geautomatiseerde werken van een derde een afweging te maken van de technische risico's. Dat zou betekenen dat steeds opnieuw om toestemming zou moeten worden gevraagd.¹²⁷ De Afdeling ziet de nadelen van het steeds opnieuw vragen van toestemming; de voorgestelde verruiming van de bijschrijfmogelijkheid in het kader van het hacken en tappen is ingegeven door het operationele belang om het zicht op targets niet te verliezen. Niettemin vraagt de Afdeling zich af of het volgen van de spoedprocedure hier niet ook uit operationeel oogpunt tot voldoende resultaat kan leiden. 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 zij op dat gebruikmaking van de spoedprocedure de voorkeur heeft.

De Afdeling adviseert de toelichting aan te vullen omtrent de mogelijkheid van gebruikmaking van de spoedprocedure om de problematiek rondom het exclusiviteitsvereiste te ondervangen, en zo nodig het voorstel aan te passen.

De spoedprocedure ex artikel 37 Wiv 2017 is niet de geëigende oplossing voor de problematiek die met dit wetsvoorstel wordt geadresseerd. De spoedprocedure is bedoeld voor onvoorziene en uitzonderlijke situaties, waarbij onverwijld spoed de toepassing van de reguliere procedure niet toelaat. Dat veronderstelt wel dat de reguliere procedure al wel in de bevoegdheid tot bijschrijving voorziet. Als dat niet het geval is, biedt de spoedprocedure ook geen soelaas. Het gaat er hier dan ook juist om de mogelijkheid tot bijschrijving tot een onderdeel van het reguliere proces te maken. In onderzoeken naar landen met offensief cyberprogramma is operationele snelheid en wendbaarheid juist in de reguliere procedure gewenst.

¹²⁵ Rapport Evaluatiecommissie Wiv 2017, bijlage bij Kamerstukken II 2020/21, 34 588, nr. 88, paragraaf 7.3.4.

¹²⁶ Memorie van toelichting, paragraaf 3.2.5.

¹²⁷ Advies van de Afdeling advisering van 21 september 2016 over de Wiv 2017 (W04.16.0097/I), Kamerstukken II 2016/17, 34 588, nr. 4, punt 9.

11. Artikelsgewijze toelichting

De Afdeling merkt op dat de artikelsgewijze toelichting bij het voorstel grotendeels ontbreekt. De reden hiervoor is dat het algemeen deel van de toelichting al veel aspecten uitvoerig uiteenzet. Niettemin, en met name met betrekking tot de in het voorstel neergelegde bevoegdheden, wordt een nauwkeurige juridische omschrijving daarvan per afzonderlijke bepaling gemist. Gelet op de verhouding tot de Wiv 2017 en de complexiteit van de materie is aanvulling van de artikelsgewijze toelichting dan ook op zijn plaats zodat per bevoegdheid en per bepaling kan worden gezien hoe dit in het grotere geheel past. Dat maakt het zo ook eenvoudiger bij de brede herziening (en eventueel andere toekomstige wijzigingen) van de Wiv 2017 te zien waarom een bepaalde bevoegdheid is opgenomen en wat dit juridisch betekent.¹²⁸ Aanvulling van de artikelsgewijze toelichting is dan ook geen herhaling van wat al in het algemeen deel is opgenomen, maar expliciteert de juridische betekenis van de voorgestelde bevoegdheden in een meer op de concrete bepalingen toegespitste wijze.

De Afdeling adviseert in de artikelsgewijze toelichting de in het voorstel opgenomen bevoegdheden toe te lichten.

Aan dit advies van de Afdeling is gevolg gegeven.

12. De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

De Afdeling adviseerde in voorgesteld artikel 7 (thans vernummerd tot artikel 6), vijfde en zesde lid, «juncto tweede» schrappen en in het zesde lid, «derde lid» te wijzigen in «tweede lid».

Deze door de Afdeling geadviseerde redactionele wijzigingen zijn doorgevoerd.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

*De vice-president van de Raad van State
Th.C. de Graaf*

Tot slot is van de gelegenheid gebruik gemaakt om het opschrift in overeenstemming met Aanwijzing 4.2, tweede lid, van de Aanwijzingen voor de Regelgeving te brengen alsmede het wetsvoorstel aan te vullen met een bepaling (artikel 15 nieuw) waarbij artikel 145 Wiv 2017 van overeenkomstige toepassing wordt verklaard op besluiten die op grond van de wet worden genomen. In artikel 145 Wiv 2017 wordt – kort gezegd – de Algemene wet bestuursrecht niet van toepassing verklaard op de operationele besluitvorming van de diensten.

Ik verzoek U, mede namens mijn ambtgenoot van Defensie, het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
H.G.J. Bruins Slot

¹²⁸ Zie ook advies van de Afdeling advisering van de Raad van State van 21 september 2016 over de Wiv 2017 (W04.16.0097/I), Kamerstukken II 2016/17, 34 588, nr. 4, punt 10. Zie ook Ar 4.48.