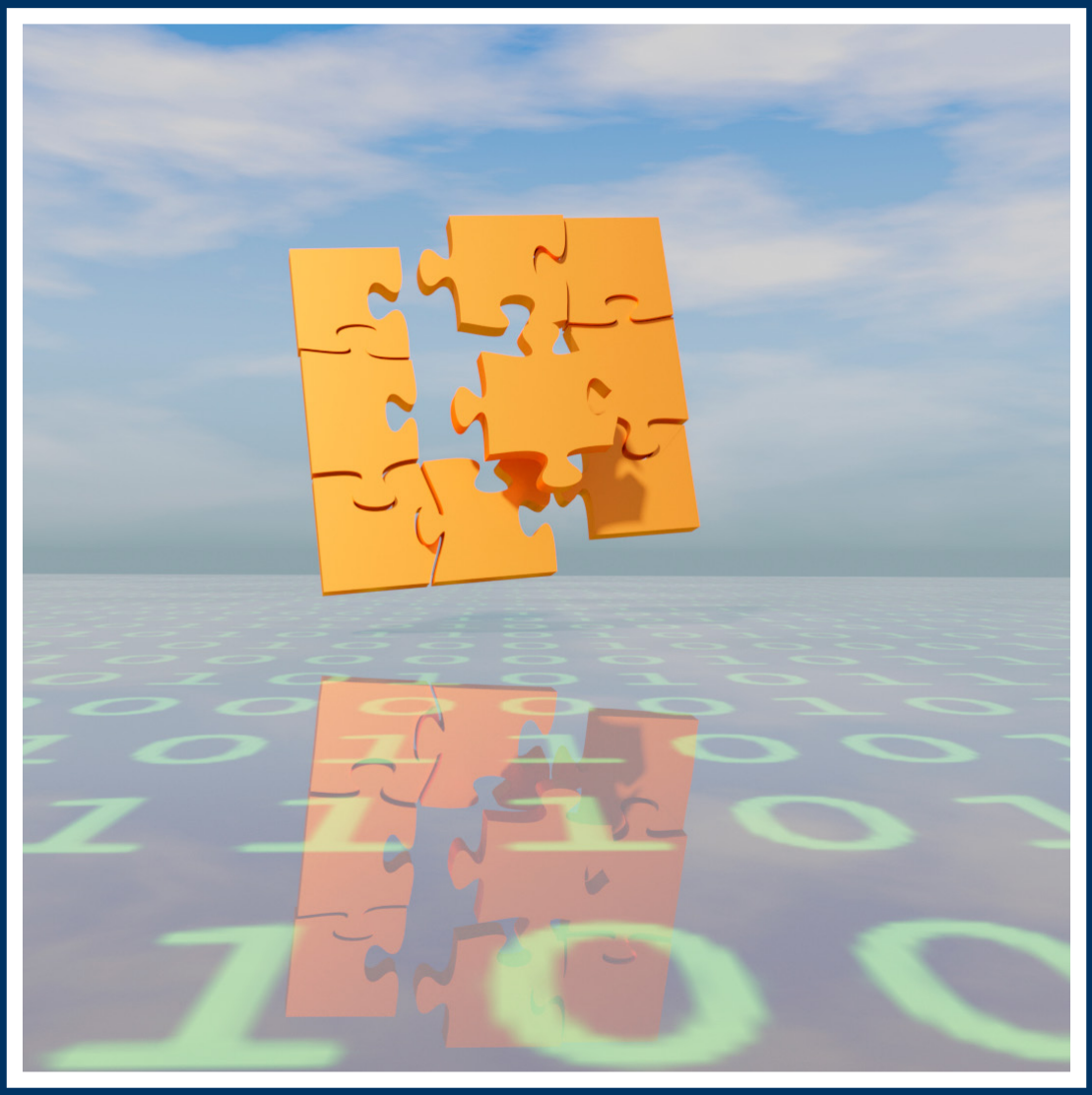
Evaluatie 2020

Wet op de inlichtingen- en veiligheidsdiensten 2017



Evaluatiecommissie Wiv 2017

Voorwoord

De Evaluatiecommissie Wiv 2017 is in mei 2020 ingesteld om de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) te evalueren, twee jaar nadat de wet volledig in werking is getreden. De Evaluatiecommissie heeft als opdracht gekregen zich te buigen over drie centrale vragen: (i) Zijn de doelstellingen van de wet – te weten modernisering van bevoegdheden en versterking van waarborgen – behaald? (ii) Is de wet in de praktijk een werkbaar instrument gebleken voor de taakuitvoering van de diensten? (iii) Zijn er knel- en aandachtspunten in de toepassingspraktijk van de wet?

De evaluatie ziet op een relatief korte periode waarin de wet in de praktijk is toegepast. Ondanks deze beperkte periode is de evaluatie geen eenvoudige klus gebleken. De opdracht heeft betrekking op complexe materie en specialistische wetgeving en omvat bovendien een veelheid aan onderwerpen. Daar komt bij dat de toepassingspraktijk van de wet zich voor een groot deel afspeelt buiten het openbaar toegankelijke domein. De Evaluatiecommissie heeft daarom in de eerste fase van haar onderzoek de tijd genomen om deze toepassingspraktijk te begrijpen en uit te diepen. Dankzij de vele inhoudelijke sessies en gesprekken met betrokken partijen heeft de Evaluatiecommissie een goed beeld gekregen van de toepassing van de wet.

Ondanks de uitbraak van COVID-19 is de Evaluatiecommissie per 1 mei 2020 van start gegaan. De materie leende zich niet (altijd) voor thuiswerken. Zo is de Evaluatiecommissie fysiek bijeengekomen om kennis te nemen van en te spreken over gerubriceerd materiaal. Namens de gehele Evaluatiecommissie spreek ik mijn grote dank uit aan alle gesprekspartners die in deze ingewikkelde periode tijd hebben vrijgemaakt om – vaak in een vrijwel leeg ministerie – met de Evaluatiecommissie te spreken. De Toetsingscommissie Inzet Bevoegdheden (TIB), de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), de diensten en de departementen hebben de Evaluatiecommissie uitvoerig van informatie voorzien. Ook dank ik de externe partijen die de Evaluatiecommissie waardevolle observaties hebben meegegeven, van NGO's tot wetenschappelijk experts en van belangenorganisaties tot maatschappelijke instanties. Daarnaast dank ik het onderzoeksbureau Verdonck, Klooster & Associates (VKA) dat onderzoek heeft gedaan naar de effecten van de wet op het Nederlandse vestigingsklimaat. Mijn dank gaat verder uit naar het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) dat ervoor heeft gezorgd dat wij ons werk geheel in onafhankelijkheid maar altijd goed gefaciliteerd hebben kunnen doen.

Als voorzitter spreek ik mijn dank uit aan het secretariaat van de Evaluatiecommissie voor de toegewijde en betrokken ondersteuning. Tot slot een groot woord van dank aan de leden van de Evaluatiecommissie met wie ik deze uitdagende taak heb kunnen volbrengen. Dankzij de brede samenstelling van de Evaluatiecommissie was er de beschikking over benodigde juridische kennis op verschillende rechtsgebieden, diepgravende technische expertise en waardevolle operationele ervaring. Veel dank aan Theo Bot, Egbert Dommering, Larissa van den Herik, Bart Jacobs, Wim Nagtegaal en Sjoerd Zijlstra. Ieder bracht vanuit eigen expertise en achtergrond een scherpe blik mee. Dat heeft geleid tot soms stevige maar altijd inhoudelijke en waardevolle discussies en bijdragen in een goede sfeer, en tot een rapport met onze gedeelde bevindingen en aanbevelingen.

Renée Jones-Bos, voorzitter

Inhoudsopgave

Belangrijkste bevindingen en conclusies **4**

1 Waarom deze evaluatie, en wat wordt geëvalueerd? **9**
1.1 Aanleiding onderzoek 9
1.2 Onderzoeksopdracht en doelstelling onderzoek 10
1.3 Afbakening 11
1.4 Indeling rapport 12
1.5 Methodologie en verantwoording 12

2 Over de Wiv 2017 **15**
2.1 Totstandkoming van de Wiv 2017 15
2.2 Verschillen tussen de Wiv 2017 en de Wiv 2002 16
2.3 Complexiteit 18
2.4 De reikwijdte van de Wiv 2017 19

3 De Wiv 2017 in een veranderende wereld **21**
3.1 Inleiding 21
3.2 Een veranderende veiligheidssituatie 21
3.3 De Wiv 2017 en privacy 26
3.4 Europese privacyregels en de inlichtingen- en veiligheidsdiensten 31
3.5 Conclusie 36

4 Bulkdata **39**
4.1 Inleiding 39
4.2 Bulkdata in de wet en praktijk 39
4.3 Verwerving van bulkdata 47
4.4 Verwerking bulkdata 53
4.5 Conclusie 66

5 Geautomatiseerde Data-Analyse (GDA) **69**
5.1 Inleiding 69
5.2 GDA in de Wiv 2017 70
5.3 GDA in de praktijk 71
5.4 Voorgestelde oplossing 72
5.5 Handelingswaarborgen GDA+ 75
5.6 Conclusie 77

6 OOG-interceptie **79**
6.1 Inleiding 79
6.2 Introductie van kabelinterceptie 79
6.3 OOG-interceptie in de wet 80
6.4 Implementatie van kabelinterceptie 81
6.5 Knelpunten en aanbevelingen OOG-stelsel 83
6.6 Conclusie 86

7 De hackbevoegdheid 87
7.1 Inleiding 87
7.2 De hackbevoegdheid in de Wiv 2017 87
7.3 De hackbevoegdheid in de praktijk: knelpunten en aanbevelingen 90
7.4 Strategische operaties 96
7.5 Conclusie 97

8 Internationale samenwerking 99
8.1 Inleiding 99
8.2 Internationale en Europese ontwikkelingen 100
8.3 De Wiv 2017 en internationale samenwerking 101
8.4 De waarborg van de wegingsnotities 103
8.5 Nadere waarborgen bij de verstrekking van gegevens aan buitenlandse diensten 105
8.6 Het verlenen en ontvangen van internationale ondersteuning 109
8.7 Multilaterale samenwerking 111
8.8 Conclusie 113

9 Stelsel van toezicht 115
9.1 Inleiding 115
9.2 Inrichting van het toezicht onder de Wiv 2017 116
9.3 De invulling van de ex-ante-toets door de TIB 126
9.4 Samenhang binnen het stelsel van toezicht 133
9.5 Balans in het stelsel 135
9.6 Benoeming en bezetting van TIB en CTIVD 141
9.7 Conclusies en aanbevelingen 145

10 Overige bevindingen 149
10.1 Overgangsrecht 149
10.2 Vestigingsklimaat 150
10.3 Openbaarheid 150
10.4 Administratieve organisatie 151
10.5 Verhouding bewaartermijnen en archiefwet 151

11 Overzicht conclusies en aanbevelingen 153
11.1 Conclusies en aanbevelingen hoofdstuk 4 Bulkdata 153
11.2 Conclusies en aanbevelingen hoofdstuk 5 GDA 154
11.3 Conclusies en aanbevelingen hoofdstuk 6 OOG-interceptie 155
11.4 Conclusies en aanbevelingen hoofdstuk 7 De hackbevoegdheid 155
11.5 Conclusies en aanbevelingen hoofdstuk 8 Internationale samenwerking 156
11.6 Conclusies en aanbevelingen hoofdstuk 9 Stelsel van toezicht 158
11.7 Conclusies en aanbevelingen hoofdstuk 10 Overige bevindingen 160

Bijlagen
Bijlage 1 Samenstelling commissie en secretariaat 163
Bijlage 2 Instellingsregeling 164
Bijlage 3 Afkortingenlijst 172
Bijlage 4 Begrippenlijst 174
Bijlage 5 Jurisprudentieoverzicht 177

Belangrijkste bevindingen en conclusies

Het doel van deze evaluatie is te onderzoeken of de Wiv 2017 datgene heeft gebracht wat de wetgever voor ogen had, namelijk modernisering van de bevoegdheden en versterking van de waarborgen, of de wet in de praktijk een werkbaar instrument is gebleken voor de taakuitvoering van de diensten, en welke knelpunten en aandachtspunten er zijn in de toepassingspraktijk van de wet. In het licht van deze vragen is de Evaluatiecommissie gevraagd zich te buigen over een hele reeks specifieke onderwerpen die zich grofweg laten vatten in de categorieën (i) technische onderwerpen, (ii) internationale samenwerking en (iii) het stelsel van toezicht.

Een belangrijk doel van de Wiv 2017 is modernisering van de bevoegdheden, met name door kabelinterceptie mogelijk te maken. Deze uitbreiding van de bevoegdheden van de diensten heeft in het maatschappelijke debat tot veel kritiek geleid vanwege zorgen in de samenleving over het grootschalig verzamelen van gegevens door de diensten. De Evaluatiecommissie constateert dat de voorbereidingen van de diensten voor kabelinterceptie in volle gang zijn maar dat kabelinterceptie voor het inlichtingenonderzoek, ruim twee jaar na inwerkingtreding van de Wiv 2017, vanwege de technische, juridische en organisatorische complexiteit nog niet heeft plaatsgevonden.

Daarnaast heeft de Wiv 2017 de waarborgen aanzienlijk versterkt. Vooral de introductie van de TIB met toetsing voorafgaand aan de inzet van bijzondere bevoegdheden (ex-ante) is daarbij van betekenis gebleken. Dit heeft geleid tot een betere kwaliteit van de toestemmingsaanvragen. Ook de CTIVD heeft met verve haar dynamische en systeemtoezicht verder uitgebouwd wat heeft bijgedragen aan het op orde brengen van de interne *compliance*-systemen door de diensten in het kader van hun zorgplicht. Het versterkte toezicht speelt een belangrijke rol in de legitimatie van het werk van de diensten. Tegelijkertijd hebben de zwaardere waarborgen ook geleid tot een forse toename van administratieve druk op de diensten. Met name in het begin was er sprake van extra belasting, mede door het ontbreken van een overgangsperiode.

De Evaluatiecommissie stelt vast dat de Wiv 2017 voor een belangrijk deel heeft bereikt wat was beoogd. De diensten missen, na operationalisering van kabelinterceptie, geen essentiële bevoegdheden en de waarborgen op het werk van de diensten zijn versterkt. De Evaluatiecommissie concludeert echter ook dat de wet op punten tekortschiet.

De Wiv 2017 sluit onvoldoende aan op de technologische complexiteit en de dynamiek van de operationele praktijk van de diensten. Daarnaast zijn belangrijke begrippen van de wet niet altijd even consistent, duidelijk en techniekonafhankelijk geformuleerd en afgebakend. In geval van geschillen over die begrippen of over de open normen uit de wet, biedt de wet geen mogelijkheid tot geschilbeslechting. Het ontbreekt de Wiv 2017 verder aan een regeling voor de omgang met bulkdata en aan voldoende uitgewerkte normering van de internationale samenwerking tussen diensten. Ondanks de relatief korte periode dat de wet van kracht is, is het de Evaluatiecommissie gebleken dat deze gebreken knelpunten opleveren in de uitvoering. Deze knelpunten hebben geresulteerd in een aantal patstellingen tussen de diensten en de TIB en CTIVD. De diensten geven aan dat dit tot gevolg heeft dat een klein maar wezenlijk deel van hun onderzoeken momenteel niet kan worden uitgevoerd.

Deze voornaamste bevindingen leiden tot verschillende aanbevelingen die naar de mening van de Evaluatiecommissie nopen tot een wetswijziging. Op het gebied van de meer technische onderwerpen is de belangrijkste aanbeveling van de Evaluatiecommissie om een nieuw regime voor bulkdata te introduceren, waarmee bulkdata met meer waarborgen wordt omkleed. Hierbij moet voor de verwerving van bulkdata eerst de behoefte daaraan worden aangetoond

en geldt voor de daaropvolgende verwerking van bulkdata één regime, ongeacht met welke bevoegdheid de bulkdata is verworven. De Evaluatiecommissie beveelt aan om bij dit regime het instrumentele en verhelderende onderscheid tussen register-bulkdata en gedrag-bulkdata te hanteren. Daarnaast worden voor een aantal technische bevoegdheden aanbevelingen gedaan om operationele knelpunten weg te nemen.

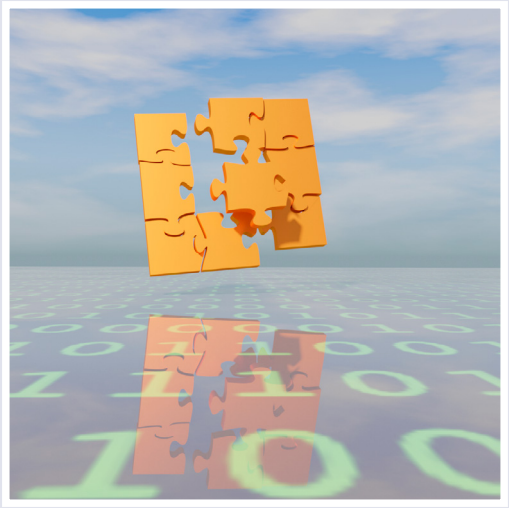
Ten aanzien van internationale samenwerking is de belangrijkste aanbeveling van de Evaluatiecommissie om de normering van deze samenwerking uit te breiden en te versterken in die zin dat die beter wordt geëxpliciteerd en wettelijk verankerd. Hiermee wordt ook de CTIVD meer handvatten geboden bij het toezicht op die samenwerking. Daarnaast wordt aanbevolen om toe te werken naar internationaal toezicht op de internationale samenwerking. Nederland is hierbij uiteraard slechts een van de vele spelers, maar kan wel een voortrekkersrol innemen.

Voor het toezicht geldt dat wat de Evaluatiecommissie betreft het stelsel op hoofdlijnen kan worden gehandhaafd. Wel dient het stelsel te worden gecomplementeerd met een rol voor de bestuursrechter bij de invulling van begrippen en open normen uit de wet. Ook beveelt de Evaluatiecommissie aan om de ex-ante toets te beperken tot de verwerving van gegevens en dit te onderscheiden van de daaropvolgende verwerking van gegevens. Daarmee samenhangend wordt aanbevolen om de statische ex-ante toets te onderscheiden van de dynamische aard van het toezicht tijdens het werk van de diensten, waarbij een goede aansluiting tussen die twee van belang is.

De Evaluatiecommissie is tijdens haar onderzoek gestuit op enige frictie in het systeem. Deze frictie is het gevolg van onvolkomenheden in de wet maar ook van de intensiteit waarmee de diensten, de betrokken ministeries en de toezichthouders met elkaar in deze complexe technische, politieke en sociale omgeving moeten werken. Enige wrijving tussen de toezichthouders en de ondertoezichtgestelden is logisch. De Evaluatiecommissie heeft bemerkt dat er de nodige controverses zijn ontstaan over toepassing van wettelijke bepalingen. Dit sterkt de Evaluatiecommissie in haar aanbeveling om de bestuursrechter een rol te geven. De weg naar de bestuursrechter moet echter wel als uitzondering worden gezien binnen een systeem waarin in eerste instantie moet worden geprobeerd problemen binnen het stelsel zelf op te lossen.

Voor alle aanbevelingen in dit rapport geldt dat deze moeten worden gezien in het licht van de taak van de Evaluatiecommissie: de wet op inhoud en toepassingspraktijk te evalueren en waar nodig voorstellen voor verbeteringen te doen.

Deel I



1 Waarom deze evaluatie, en wat wordt geëvalueerd?

1.1 Aanleiding onderzoek

De Wet op de inlichtingen- en veiligheidsdiensten 2017 (ook: 'de Wiv 2017' of 'de wet') is met een lange voorgeschiedenis op 1 mei 2018 volledig in werking getreden. In de wet zelf is bepaald dat de wet vervolgens binnen vijf jaar wordt geëvalueerd.[1] Tijdens de behandeling van het wetsvoorstel in de Eerste Kamer heeft de toenmalige minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) toegezegd *specifieke* aspecten van de wet binnen deze termijn al na twee jaar te evalueren.[2] Vervolgens heeft het kabinet Rutte III in het regeerakkoord 'Vertrouwen in de toekomst' besloten de *gehele* evaluatie van de Wiv 2017 te vervroegen naar uiterlijk twee jaar na inwerkingtreding van de wet. In het regeerakkoord is ook neergelegd dat de evaluatie wordt uitgevoerd door een onafhankelijke commissie.[3] Op 1 mei 2020 is de Evaluatiecommissie Wiv 2017 met haar werkzaamheden gestart.

Het vroege moment van de evaluatie kan worden geplaatst tegen de achtergrond van de stevige maatschappelijke discussie over de Wiv 2017, met name over de nieuwe bevoegdheid tot kabelinterceptie. Die discussie is begrijpelijk. De wet geeft de Nederlandse inlichtingen- en veiligheidsdiensten (hierna: de diensten) bevoegdheden die grote inbreuk kunnen maken op de privacy van mensen, binnen en buiten Nederland. Het is essentieel dat de diensten zorgvuldig met deze bevoegdheden omgaan en dat de controle op de inzet van deze bevoegdheden adequaat is. Tegelijkertijd wordt de Nederlandse samenleving, en het Nederlandse belang in het buitenland, in toenemende mate geconfronteerd met (veelal digitale) dreigingen. De samenleving verwacht dat de overheid haar daartegen beschermt, en dat mág de samenleving ook verwachten. Dat is immers één van de belangrijkste plichten van de overheid. Maar die overheid moet dan wel wel voldoende op de hoogte zijn van deze dreigingen. In het onderkennen van dreigingen tegen de democratische rechtsorde of de gewichtige belangen van de staat, spelen beide diensten – de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) – een belangrijke rol. Om die dreigingen te kunnen signaleren en hierop te kunnen reageren, moeten zij bevoegdheden inzetten die grote inbreuk kunnen maken op de rechten – vaak de privacy – van mensen. Tegelijkertijd moeten de diensten zich steeds afvragen of een dergelijke inbreuk onder de gegeven omstandigheden gerechtvaardigd is.

Bij de totstandkoming van de wet waren er zorgen over de vraag of met de wet de privacybelangen voldoende zouden worden beschermd. Deze zorgen zijn tweeëneenhalf jaar na inwerkingtreding van de wet niet verdwenen. Met de onthullingen van Snowden[4] over de grootschalige interceptieactiviteiten van de Amerikaanse inlichtingendienst NSA (*National Security Agency*) nog in het geheugen, wordt in het publieke debat nu met name de vraag gesteld of de diensten voldoende zorgvuldig omgaan met grote hoeveelheden gegevens (bulkdata[5]) en of daarvoor voldoende waarborgen aanwezig zijn. Ook is er aandacht voor de samenwerking met buitenlandse diensten en of die samenwerking wel met genoeg waarborgen is omkleed.

---

1 Artikel 167, eerste lid, Wiv 2017.
2 *Handelingen I* 2016/17, 35, nr. 8, p. 4.
3 Bijlage 820238 bij *Kamerstukken II* 2017/18, 34 700, nr. 34, p. 4 (Regeerakkoord 2017-2021 'Vertrouwen in de toekomst').
4 Zie onder meer Greenwald, G. en E. MacAskill. (7 juni 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Beschikbaar via **https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.**
5 Onder bulkdata wordt een omvangrijke verzameling van gegevens verstaan waarvan het merendeel betrekking heeft op personen en/of organisaties die niet in onderzoek zijn van de diensten en dit ook nooit zullen worden. Dit zal verder worden toegelicht in hoofdstuk 4.

1.2 Onderzoeksopdracht en doelstelling onderzoek

Het doel van deze evaluatie is te onderzoeken of de wet datgene heeft gebracht wat de wetgever voor ogen had, of de wet in de praktijk een werkbaar instrument is gebleken voor de taakuitvoering van de diensten, en welke knelpunten en aandachtspunten er zijn in de toepassingspraktijk van de wet. De doelstelling van het onderzoek volgt uit de opdracht aan de Evaluatiecommissie, vastgelegd in het instellingsbesluit.[6] De concrete invulling van deze opdracht is beschreven in een eerdere brief van het kabinet aan de Tweede Kamer.[7]

Daarnaast is een aantal meer specifieke onderwerpen aan de commissie meegegeven, met de opdracht daaraan bijzondere aandacht te besteden. Samengevat gaat het dan om onderwerpen die raken aan (i) de (technische) bevoegdheden van de diensten tot gegevensverwerving en -verwerking en de daaraan verbonden waarborgen, (ii) de bevoegdheden en waarborgen met betrekking tot internationale samenwerking door de diensten, en (iii) het integrale stelsel van toezicht. Onderdeel van de opdracht is ook de vraag wat de effecten van de wet op het Nederlandse vestigingsklimaat zijn, met name voor de ICT-telecommunicatiesector.[8]

Tijdens het onderzoek van de Evaluatiecommissie is het wetsvoorstel tot wijziging van de Wiv 2017 in de Tweede Kamer behandeld. In de loop van deze behandeling zijn door Kamerlid Buitenweg (GroenLinks) twee amendementen ingediend.[9] Deze amendementen hebben betrekking op het delen van ongeëvalueerde gegevens met buitenlandse diensten en het verzamelen van bulkdata via de informantenbevoegdheid. Bij beide amendementen, die zijn verworpen door de Tweede Kamer, heeft de minister van BZK verwezen naar deze evaluatie. Omdat beide amendementen binnen de reikwijdte van de evaluatie vallen, heeft de Evaluatiecommissie deze in het onderzoek betrokken.

Ook hebben er gedurende de onderzoeksperiode van de Evaluatiecommissie ontwikkelingen plaatsgevonden met betrekking tot bepaalde onderwerpen van de evaluatie, met name rondom de omgang met bulkdata. De CTIVD heeft aanbevolen om bulkdatasets te vernietigen als gevolg van een onrechtmatige relevantiebeoordeling.[10] Hierop hebben de betrokken ministers de uitzonderlijke stap genomen om deze aanbeveling niet over te nemen en een tijdelijke bulkregeling vast te stellen over de omgang met bulkdata, die weer tot nieuwe discussie tussen de partijen heeft geleid.[11] Deze ontwikkelingen geven het belang aan van deze vervroegde evaluatie.

---

[6] Regeling instelling Evaluatiecommissie Wiv 2017 van 17 april 2020, *Stcrt.* 21256 (zie bijlage 2 van dit rapport). De opdracht is gegeven door de Minister-President, Minister van Algemene Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie, de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

[7] *Kamerstukken I* 2019/20, 34 588, nr. M (Kamerbrief Evaluatie Wiv 2017).

[8] In het instellingsbesluit (zie bijlage 2) en in de Kamerbrief Evaluatie Wiv 2017 van 12 november 2019 (*Kamerstukken I* 2019/20, 34 588, nr. M) is een heel aantal concrete sub-onderwerpen geformuleerd waaraan de Evaluatiecommissie aandacht dient te besteden.

[9] *Handelingen II* 2019/20, 78, nr. 6 en *Kamerstukken II* 2019/20, 35 242, nr. 8 en nr. 9.

[10] CTIVD. (2020). *Toezichtsrapport 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD.*

[11] *Kamerstukken II* 2019/20, 29 924, nr. 203 (Beleidsreactie CTIVD toezichtsrapporten nr. 70 en 71) en Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 van 5 november 2020, *Stcrt.* 56482.

1.3 Afbakening

De Wiv 2017 bepaalt dat een evaluatie van deze wet een verslag moet zijn van de doeltreffendheid en de effecten van deze wet in de praktijk.[12] De Evaluatiecommissie vat de invulling van deze wetsevaluatie op zoals onder §1.2 besproken. Het onderzoek ziet niet op de vraag of de diensten de wet rechtmatig uitvoeren of anderszins op het functioneren van de diensten.[13] Deze aspecten komen aan de orde in het toezicht door de CTIVD en de toetsing van bijzondere bevoegdheden door de TIB.[14]

Volgens artikel 167, lid 1, Wiv 2017 moet binnen vijf jaar na inwerkingtreding van de wet, en vervolgens telkens na vijf jaar verslag aan de Staten-Generaal worden gedaan over 'de doeltreffendheid en de effecten van deze wet in de praktijk'. Het kabinet heeft besloten om de evaluatie reeds na twee jaar te doen plaatsvinden. Dit is dus een eerste volledige evaluatie van de wet.

In deze evaluatie is gekeken naar de wet als geheel, en naar de veranderingen die de wet heeft gebracht. Volgend uit de opdracht voor de evaluatie is hierbij specifiek ingegaan op het stelsel van toezicht, de (technische) bevoegdheden tot gegevensverwerving en internationale samenwerking. Bij het behandelen van de (technische) bevoegdheden tot gegevensverwerving heeft de Evaluatiecommissie zich gericht op de *bijzondere* bevoegdheden met een sterk technisch karakter. Daar waar relevant heeft de Evaluatiecommissie ook de verwerving van gegevens via *algemene* bevoegdheden betrokken (zie voor uitleg bijzondere en algemene bevoegdheden §2.1). Dit is het geval bij het verwerven en verder verwerken van bulkdata. De algemene bevoegdheden van de diensten zijn zodoende niet op zichzelf onderwerp geweest van onderzoek. Naast de gegevensverwerving is ook aandacht besteed aan de daaropvolgende verwerking van gegevens waar het bulkdata betreft.

In dezelfde periode als waarin deze evaluatie heeft plaatsgevonden, is ook door de Algemene Rekenkamer (AR) een onderzoek uitgevoerd op verzoek van de minister van Defensie (destijds tevens verantwoordelijk voor de AIVD). Dit onderzoek richt zich op de vraag of de Wiv 2017 (incidentele en structurele) effecten heeft op de operationele slagkracht van de diensten. Het onderzoek van de AR richt zich daarmee niet op de wet. Zo zijn de evaluatie van de Wiv 2017 en het onderzoek van de AR verschillend van aard maar liggen zij wel in elkaars verlengde. De voorzitter van Evaluatiecommissie heeft dan ook gedurende de onderzoeken een aantal keer contact gehad met de president van de AR. Daar waar mogelijk en relevant noemt de Evaluatiecommissie de gevolgen van gebreken van de wet voor de taakuitvoering van de diensten. Voor een compleet beeld van de effecten van de wet wordt aangeraden kennis te nemen van beide rapporten. Het rapport van de AR zal naar verwachting enige tijd na aanbieding van dit rapport worden gepubliceerd.

---

[12] Artikel 167, eerste lid, Wiv 2017.

[13] Het functioneren van de diensten zal binnen vijf jaar na inwerkingtreding van de wet (separaat) worden geëvalueerd volgens artikel 167, tweede lid, van de Wiv 2017.

[14] Voor deze aspecten verwijzen we u graag door naar de verschillende voortgangsrapportages en diepteonderzoeken van de CTIVD en de jaarverslagen van TIB, beschikbaar op de websites **www.ctivd.nl/onderzoeken** en **www.tib-ivd.nl/documenten**.

1.4 Indeling rapport

Dit rapport is opgedeeld in drie delen. In het eerste, inleidende deel wordt een achtergrondschets gegeven van de Wiv 2017 en van de totstandkoming van de wet (hoofdstuk 2), gevolgd door een duiding van de context waarin de toepassing van de Wiv 2017 plaatsvindt (hoofdstuk 3).

Het tweede deel omvat de verdiepende hoofdstukken waarin inhoudelijk wordt ingegaan op de drie grote voorliggende thema's, te weten de verschillende technologische vraagstukken, internationale samenwerking en het stelsel van toezicht. Als eerste worden de technologische vraagstukken behandeld. Dit omvat hoofdstukken over de verwerving en verwerking van bulkdata (hoofdstuk 4), geautomatiseerde data-analyse (hoofdstuk 5), de bevoegdheid van onderzoeksopdrachtgerichte interceptie (OOG-interceptie) (hoofdstuk 6) en de hackbevoegdheid (hoofdstuk 7). Vervolgens wordt ingegaan op het thema van internationale samenwerking (hoofdstuk 8). Het verdiepende deel wordt afgesloten met het stelsel van toezicht (hoofdstuk 9). In deze verdiepende hoofdstukken wordt steeds bezien of de wet datgene heeft gebracht wat de wetgever daarmee voor ogen had, of de wet in de praktijk een werkbaar instrument is gebleken voor de taakuitvoering van de diensten en welke knelpunten en aandachtspunten er zijn in de toepassingspraktijk van de wet.[15] Op die punten worden aanbevelingen gedaan. Elk hoofdstuk sluit af met een conclusie van de belangrijkste bevindingen op het desbetreffende onderwerp.

In het derde en afsluitende deel van het rapport wordt een aantal overige bevindingen van de Evaluatiecommissie beschreven die niet zien op een specifiek thema maar op de wet in den brede (hoofdstuk 10) en wordt een overzicht gegeven van alle conclusies en aanbevelingen uit het verdiepende deel van het rapport (hoofdstuk 11).

1.5 Methodologie en verantwoording

De Evaluatiecommissie heeft haar werkzaamheden in de periode mei tot en met december 2020 verricht. Hierbij is zij ondersteund door een secretariaat van zeven personen, inclusief secretariële ondersteuning.

De Evaluatiecommissie heeft haar werk in drie fases opgedeeld; een oriënterende, een verdiepende en een opleverfase. In de oriënterende fase is de Evaluatiecommissie gestart met een aantal inleidende sessies en verkennende gesprekken met de verschillende partijen die direct te maken hebben met de uitvoering van de wet. Dit betreft de leiding van beide diensten, de verantwoordelijke ministers en secretarissen-generaal van BZK en Defensie en de toezichthouders TIB en CTIVD.

In de tweede verdiepende fase heeft de Evaluatiecommissie haar werkzaamheden thematisch onderverdeeld in drie subgroepen die zich richtten op de technologische vraagstukken, de internationale samenwerking en het stelsel van toezicht. In deze verdiepende fase zijn er 33 gesprekken en interviews gevoerd met vertegenwoordigers van:

- De diensten en departementen, waaronder technisch- en juridisch experts;
- De toezichthouders TIB en CTIVD, waaronder zowel de afdeling toezicht als de afdeling klachtbehandeling van de CTIVD en de ICT-unit van de CTIVD;

[15] *Kamerstukken I* 2019/20, 34 588, nr. M (Kamerbrief Evaluatie Wiv 2017).

- De Coördinator Inlichtingen- en Veiligheidsdiensten (Secretaris-Generaal van Algemene Zaken);
- De behoeftestellers van inlichtingenproducten, namelijk het ministerie van Buitenlandse Zaken (plaatsvervangend Directeur-Generaal Politieke Zaken), het ministerie van Justitie- en Veiligheid (Secretaris-Generaal van Justitie en Veiligheid en de Nationaal Coördinator Terrorismebestrijding en Veiligheid), en het ministerie van Defensie (Commandant der Strijdkrachten en plaatsvervangend Commandant der Strijdkrachten);
- Tweede Kamer: De Commissie voor de Inlichtingen- en Veiligheidsdiensten en de Vaste Kamercommissies voor BZK en Defensie;
- De Raad van State;
- De Rechtbank Den Haag;
- De Nationale Ombudsman.

De informatie die door de gesprekspartners met de Evaluatiecommissie is gedeeld, is vertrouwelijk behandeld. Van de gesprekken zijn verslagen gemaakt die aan de geïnterviewde ter verifiering zijn voorgelegd.

De Evaluatiecommissie heeft in deze periode ook voor zover mogelijk alle bedrijven en maatschappelijke organisaties benaderd die via de internetconsultatie bij de totstandkoming van de Wiv 2017 inhoudelijk hebben gereageerd op het wetsvoorstel. Hierop heeft zij van de volgende externe partijen een schriftelijke inbreng en mondelinge toelichting mogen ontvangen:

- Arthur's Legal B.V.;
- Het College voor de Rechten van de Mens;
- Het Nederlands Juristen Comité voor de Mensenrechten;
- De Nederlandse Orde van Advocaten;
- Stichting Bits of Freedom;
- Stichting Free Press Unlimited;
- Stichting Vrijschrift.

Daarnaast zijn de volgende wetenschappelijke experts geraadpleegd:

- Prof. dr. P.H.A.M. Abels;
- Prof. dr. I.T. Cameron;
- Dr. C.W. Hijzen;
- Prof. mr. dr. E.R. Muller;
- Prof. mr. dr. J.J. Oerlemans.

In de laatste fase zijn de bevindingen van de verschillende subgroepen in plenaire sessies behandeld. De opgeleverde observaties, conclusies en aanbevelingen hebben uiteindelijk hun beslag gekregen in dit rapport.

Op basis van artikel 5 van de instellingsregeling had de Evaluatiecommissie de mogelijkheid om ter ondersteuning van haar onderzoek externe deskundigen in te schakelen. Daartoe stond de Evaluatiecommissie een budget ter beschikking. De Evaluatiecommissie heeft in dit verband de effecten van de wet op het Nederlandse vestigingsklimaat laten onderzoeken door Verdonck, Klooster & Associates (VKA). De Evaluatiecommissie spreekt haar waardering uit voor de

gedegen analyse die VKA, in tussentijdse afstemming met het secretariaat, heeft verricht en de inzichtvolle rapportage die daarvan het resultaat is.[16]

Ook heeft de Evaluatiecommissie ten behoeve van het onderzoek vele documenten bestudeerd. Naast de wetsgeschiedenis betreft dit relevante Kamerstukken sinds de inwerkingtreding, toezichtsrapporten en rapportages van de CTIVD, jaarverslagen van de TIB, rechtseenheidsbrieven van de TIB en CTIVD en jaarverslagen van de diensten. Daarnaast heeft de Evaluatiecommissie kennisgenomen van gerubriceerde documenten die hebben bijgedragen aan het begrip van de Evaluatiecommissie van de toepassingspraktijk. Vanwege de openbare aard van dit rapport[17] is de gerubriceerde informatie uit deze documenten niet in dit rapport opgenomen. Alle verslagen van interviews en interne overleggen zijn na afronding van het onderzoek aan de AIVD overgedragen ter archivering.

[16] Het rapport van VKA is, tezamen met het eindrapport van de Evaluatiecommissie, digitaal ter inzage beschikbaar op de website van de rijksoverheid **http://rijksoverheid.nl**.
[17] *Kamerstukken I* 2019/20, 34 588, nr. M (Kamerbrief Evaluatie Wiv 2017).

2 Over de Wiv 2017

2.1 Totstandkoming van de Wiv 2017

Vóór inwerkingtreding van de Wiv 2017 vormde de Wiv 2002 het juridisch kader voor de AIVD en MIVD. In 2013 is de Wiv 2002 geëvalueerd door de commissie Dessens.[18] De belangrijkste conclusie van die commissie was dat de wet aan modernisering toe was vanwege voortschrijdende technische ontwikkelingen, waarbij met name werd gedoeld op de mogelijkheid van kabelinterceptie. Daarbij moest een nieuwe balans komen tussen het effectief kunnen opereren van de diensten en de rechtsstatelijke waarborgen.

Naar aanleiding van het rapport van de commissie Dessens is het kabinet in 2015 met een conceptwetsvoorstel gekomen.[19] Hierin werd onder meer een nieuw stelsel voor ongerichte interceptie (later onderzoeksopdrachtgerichte interceptie genoemd) geïntroduceerd waarmee ook kabelinterceptie mogelijk zou worden. Daarnaast werden enkele voorstellen gedaan ter versterking van de waarborgen, zoals de introductie van het expliciete wettelijke vereiste van wegingsnotities om een zorgvuldige afweging te kunnen maken voordat een samenwerkingsrelatie wordt aangegaan met een buitenlandse dienst. Ook zou de CTIVD zich achteraf moeten buigen over de rechtmatigheid van de inzet van een bijzondere bevoegdheid. Als de CTIVD zou oordelen dat toestemming daarvoor niet had mogen worden verleend, dan zou de betrokken minister die toestemming moeten heroverwegen.

Algemene en bijzondere bevoegdheden

Zowel de Wiv 2002 als de Wiv 2017 hanteren een onderscheid tussen 'bijzondere bevoegdheden' en overige 'algemene bevoegdheden' van de diensten.

Bijzondere bevoegdheden[20] hebben over het algemeen een meer ingrijpend karakter en leiden tot een grotere inbreuk op privacy ten opzichte van algemene bevoegdheden.[21] Een bijzondere bevoegdheid is bijvoorbeeld het observeren en volgen van een persoon (artikel 40) of de hackbevoegdheid (artikel 45). Deze bevoegdheden mogen niet voor alle taken van de diensten worden ingezet, bijvoorbeeld niet voor het verrichten van veiligheidsonderzoeken en het opstellen van dreigings- en risicoanalyses (artikel 28, lid 1).

Algemene bevoegdheden zijn bevoegdheden die wel voor alle taken van de diensten mogen worden ingezet. Het gaat bijvoorbeeld om het raadplegen van een informant (artikel 39).

Voor de meeste bijzondere bevoegdheden bepaalt de Wiv 2017 dat deze alleen mogen worden ingezet met voorafgaande toestemming van de TIB (ex-ante toets). De inzet van zowel de algemene als de bijzondere bevoegdheden staat onder toezicht van de CTIVD, tijdens de uitvoering en achteraf.

---

[18] Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen.*

[19] Consultatieversie van het conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX. (2015). Beschikbaar via **https://www.internetconsultatie.nl/wiv/details**.

[20] Paragraaf 3.2.5 van de Wiv 2017 schetst alle bijzondere bevoegdheden tot gegevensverwerking (inclusief verwerven) van de diensten. Daarnaast bevat hoofdstuk 4 van de Wiv 2017 nog een aantal overige bijzondere bevoegdheden.

[21] *Kamerstukken II* 2016/17, 34 588, nr, 3, p. 60 (Memorie van Toelichting Wiv 2017, hierna: MvT).

Op dit conceptwetsvoorstel werd kritisch gereageerd door onder meer de CTIVD, NGO's en bedrijven in de internetconsultatie en in een *Privacy Impact Assessment* (PIA).[22] Het wetsontwerp is vervolgens grondig aangepast door onder meer de TIB te introduceren, die de toestemming voor de inzet van bepaalde bijzondere bevoegdheden vooraf bindend toetst op rechtmatigheid. Tijdens de wetsbehandeling heeft de regering het wetsvoorstel nog verder aangepast door de zorgplicht die rust op de diensten steviger in te bedden en de waarborgen bij internationale samenwerking te vergroten.

Bij de behandeling van de wet in de Tweede Kamer zijn verschillende amendementen ingediend en moties aangenomen, waaronder de motie-Recourt,[23] waarin was neergelegd dat de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit in de praktijk moeten leiden tot een zo gericht mogelijke inzet van bevoegdheden (het gerichtheidsvereiste). In juli 2017 is de Eerste Kamer akkoord gegaan met het wetsvoorstel zoals het toen voorlag en is de wet in het Staatsblad geplaatst.

Ondertussen was het wetsvoorstel onderwerp geworden van een stevig maatschappelijk debat dat uitmondde in een raadgevend referendum in maart 2018. In reactie op de uitkomst (49,44% tegen, 46,53% voor) zijn door het kabinet aanvullende beleidsregels opgesteld op onder meer het gebied van internationale samenwerking, kabelinterceptie en het gerichtheidsvereiste.[24] Uiteindelijk is de Wiv 2017 zonder overgangsrecht op 1 mei 2018 volledig in werking getreden, samen met deze aanvullende beleidsregels. Het kabinet heeft toen toegezegd een voorstel tot wijziging van de Wiv 2017 in te dienen, om de beleidsregels over internationale samenwerking en het gerichtheidsvereiste in de te wet verankeren.[25] In juli 2019 is dat wetsvoorstel aan de Tweede Kamer gezonden.[26] Hierin is ook de mogelijkheid tot het benoemen van plaatsvervangende leden van de TIB opgenomen. De wetswijziging is in juni 2020 aangenomen door de Tweede Kamer en is op het moment van oplevering van dit rapport nog in behandeling in de Eerste Kamer.

2.2 Verschillen tussen de Wiv 2017 en de Wiv 2002

Met de Wiv 2017 heeft de wetgever beoogd de bevoegdheden van de diensten uit te breiden ten opzichte van de bevoegdheden onder de Wiv 2002. Tegelijkertijd moesten de waarborgen worden versterkt, zodat de bevoegdheden en de waarborgen met elkaar in balans zouden zijn.[27] In hoofdlijnen heeft de Wiv 2017 de volgende veranderingen gebracht:[28]

Uitbreiding bevoegdheden

- De diensten mogen ook 'onderzoeksopdrachtgericht intercepteren' (OOG-interceptie) op de kabel (artikel 48 Wiv). Onder de Wiv 2002 werd dit nog 'ongerichte interceptie' genoemd en mocht dit alleen op niet-kabelgebonden communicatie.
- De medewerkingsverplichting is verruimd; deze verplichting richt zich niet meer alleen tot telecomaanbieders maar tot alle aanbieders van communicatiediensten (artikelen 52 t/m 56).

[22] Bijlage 'Extern advies 9' bij *Kamerstukken II* 2016/17, 35 488, nr. 3 (*Privacy Impact Assessment* Wet op de inlichtingen- en veiligheidsdiensten 20XX).
[23] *Kamerstukken II* 2016/17, 34 588, nr. 66 (motie-Recourt).
[24] Beleidsregels Wiv 2017 van 25 april 2018, *Stcrt.* 24397.
[25] *Kamerstukken II* 2017/18, 34 588, nr. 70.
[26] *Kamerstukken II* 2018/19, 35 242, nrs. 1-3.
[27] *Kamerstukken II* 2016/17, 34 588, nr. 3, hoofdstuk 1 (MvT Wiv 2017).
[28] Zie voor een overzicht van de belangrijkste wijzigingen die de Wiv 2017 heeft meegebracht Dielemans, R. (2018). De Wiv 2002 en Wiv 2017 op enkele hoofdlijnen vergeleken. *Justitiële Verkenningen*, 44(1). p. 68-84.

- De diensten hebben een aanvullende bevoegdheid gekregen tot het verrichten van DNA-onderzoek (artikel 43).

Versterking waarborgen

- De toestemming van de minister voor de inzet van bepaalde bijzondere bevoegdheden[29] wordt *voorafgaand* aan de inzet getoetst op rechtmatigheid door de TIB. Het oordeel van de TIB is bindend (artikel 32). Dit is een aanvulling op het onder de Wiv 2002 al bestaande toezicht van de CTIVD op de de inzet van algemene en bijzondere bevoegdheden door de diensten. Het toezicht van de CTIVD kan zowel tijdens de inzet plaatsvinden als achter en heeft een niet-bindend karakter (dit was zo onder de Wiv 2002 en blijft zo onder de Wiv 2017).
- De CTIVD heeft, naast haar toezichtstaak, de taak voor klachtenbehandeling gekregen waarvoor een aparte afdeling is ingericht die bindende uitspraken kan doen (artikel 114 t/m 124 Wiv 2017).[30]
- Er is toestemming van de rechtbank Den Haag nodig voor de inzet van een bijzondere bevoegdheid jegens journalisten en advocaten (artikel 30 Wiv 2017).[31]
- Het datareductiestelsel is aangescherpt: gegevens verkregen uit de inzet van bijzondere bevoegdheden moeten worden beoordeeld op relevantie (artikel 27 en 48, lid 5).
- De zorgplicht voor een zorgvuldige en rechtmatige gegevensverwerking is uitgebreid door onder meer specifiek te verwijzen naar de kwaliteit van de gehanteerde algoritmen en modellen bij gegevensverwerking (artikel 24).
- Het aantal bevoegdheden waarvoor de minister (in plaats van bijvoorbeeld het hoofd van de betreffende dienst) toestemming moet geven voor de inzet is uitgebreid (zie het kader hieronder). Dit geldt onder meer voor het delen van ongeëvalueerde gegevens met buitenlandse diensten, het binnendringen van een geautomatiseerd werk ('hacken') en het toepassen van geautomatiseerde data-analyse waarbij ook metadata uit OOG-interceptie wordt betrokken.
- Enkele bevoegdheden die onder de Wiv 2002 al bestonden zijn in de Wiv 2017 geëxpliciteerd. Dit geldt onder andere voor geautomatiseerde data-analyse, het binnendringen van een

---

[29] Artikel 32, tweede lid van de Wiv 2017 bepaalt dat de TIB is belast met het toetsen van de rechtmatigheid van de door de betrokken minister verleende toestemming voor de inzet van de volgende bijzondere bevoegdheden: het observeren en volgen indien het inzet van technische middelen in de woning betreft (artikel 40, lid 3), het doorzoeken van besloten plaatsen, het doorzoeken van gesloten voorwerpen, het verrichten van onderzoek aan een voorwerp gericht op het vaststellen van de identiteit indien het doorzoeken van een woning betreft (artikel 42, lid 4), verrichten van DNA-onderzoek gericht op het vaststellen (inclusief verificatie) van de identiteit van personen alsook de verlenging van de termijn voor DNA-onderzoek op het vergaarde celmateriaal (artikel 43, lid 2 en 4), verkennen en binnendringen in geautomatiseerde werken - ook via een derde - en de medewerkingsplicht van derden bij de ontsleuteling (artikel 45, lid 3, 5 en 10), onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers (artikel 47, lid 2), onderzoeksopdrachtgericht onderzoek van communicatie, bekend als OOG-interceptie (artikel 48, lid 2), onderzoek van geïntercepteerde OOG-gegevens ten behoeve van interceptie, bekend als search gericht op interceptie en selectie, bekend als search gericht op selectie (artikel 49, lid 4), selectie van gegevens verkregen uit OOG-interceptie (artikel 50, lid 2), geautomatiseerde data-analyse waarbij OOG-metadata wordt betrokken indien gericht op het identificeren van personen of organisaties (artikel 50, lid 4), medewerkingsplicht van aanbieders van communicatiediensten t.b.v. artikel 47 dan wel artikel 48 (artikel 53, lid 2), medewerkingsplicht tot verstrekking van gegevens van aanbieders van communicatiediensten dan wel aanbieders van opslagdiensten (artikel 54, lid 2) en ten slotte medewerkingsplicht bij ontsleuteling van communicatie als bedoeld in artikel 47 dan wel artikel 48 (artikel 57, lid 2).

[30] Onder de Wiv 2002 was de klachtbehandeling belegd bij de Nationale ombudsman, die niet de bevoegdheid had tot het doen van bindende uitspraken.

[31] Onder de Wiv 2002 was dit niet het geval. De onafhankelijke toets op inzet van bijzondere bevoegdheden jegens journalisten was geregeld in de 'Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten' in 15 december 2015 (*Stcrt*. 2015, 46477), als gevolg van de uitspraak van het EHRM (EHRM 22 november 2012, ECLI:CE:ECHR:2012:1122JUD003931506, *(Telegraaf Media Nederland*); NJ 2013/232 m.nt. E.J. Dommering. Deze regeling is met de inwerkingtreding van de Wiv 2017 komen te vervallen.

geautomatiseerd werk via een derde en de criteria voor het aangaan van samenwerkingsrelaties met buitenlandse diensten.

Wat houdt ministeriële toestemming in?

Onder de Wiv 2002 gold al dat voor een aantal bevoegdheden de minister toestemming moest geven voor de inzet. Met de Wiv 2017 is het aantal bevoegdheden waarvoor ministeriële toestemming nodig is, groter geworden. Ministeriële toestemming betekent in de praktijk dat een toestemmingsaanvraag voor de inzet van een bevoegdheid al door diverse personen is gecontroleerd voordat de betrokken minister ernaar kijkt. De doorlooptijd van zo'n aanvraag – van het opstellen van de aanvraag door een medewerker tot en met een beslissing van de minister – varieert van een paar dagen tot enkele weken, afhankelijk van bijvoorbeeld de complexiteit van de aanvraag. De weg naar de minister ziet er als volgt uit:

Een medewerker van de dienst schrijft namens een inlichtingenteam, in overleg met de desbetreffende teamjurist, een toestemmingsaanvraag. Deze aanvraag wordt vervolgens beoordeeld door het hoofd van het inlichtingenteam.[32] Bij akkoord gaat de aanvraag door naar zijn/haar leidinggevende.[33] Als ook diegene akkoord is met de aanvraag, wordt deze voorgelegd aan de afdeling juridische zaken. Deze afdeling controleert de aanvraag op onder meer de juridische kwaliteit en hanteert hierbij vaak het vier-ogenprincipe. Als de afdeling akkoord is, dan wordt de aanvraag voorgelegd aan het diensthoofd (directeur-generaal AIVD resp. directeur MIVD). Het diensthoofd legt de toestemmingsaanvraag tot slot aan de minister voor, in aanwezigheid van de secretaris-generaal. Voor het Ministerie van Defensie geldt dat de aanvraag ook wordt beoordeeld door de Directie Juridische Zaken van het departement en door de adviseurs van de secretaris-generaal en de minister. Bij het Ministerie van BZK wordt de Directie Constitutionele Zaken en Wetgeving (CZW) in specifieke – vaak complexe – gevallen gevraagd om advies.

2.3 Complexiteit

De uitbreiding van bevoegdheden en versterking van de waarborgen zoals beschreven in §2.2 hebben geresulteerd in een omvangrijke wet. Waar de Wiv 2002 bestond uit 106 artikelen, zijn dat er in de nieuwe wet 172 geworden. Dit is bovendien geen makkelijke materie. In de artikelen worden veel specialistische termen genoemd die binnen de wet een eigen betekenis kennen. In de toelichting op de wet worden de artikelen wel nader geduid, maar ook deze omvangrijke toelichting van bijna 300 pagina's is voor de burger doorgaans lastig te volgen. Daarbij geldt ook dat voor bepaalde termen de definitie expliciet in de wet noch toelichting staat. Hiervoor moet de parlementaire geschiedenis worden geraadpleegd. Zowel de complexe aard van de materie als de omvang maken de Wiv 2017 voor de burger een weinig toegankelijke en moeilijk te begrijpen wet.

[32] Teamhoofd bij de AIVD, teamleider bij de MIVD.
[33] Dit is een unithoofd bij de AIVD en een afdelingshoofd bij de MIVD. Zij geven leiding aan verschillende teamhoofden/teamleiders en hun teams.

2.4 De reikwijdte van de Wiv 2017

De Wiv 2017 is een Nederlandse wet die de activiteiten van de Nederlandse diensten reguleert. De Wiv 2017 geldt dus in Nederland in die zin dat zij bijvoorbeeld alleen verplichtingen kan opleggen aan private actoren, zoals aanbieders van communicatiediensten, die onder de Nederlandse rechtsmacht vallen. Met betrekking tot de reikwijdte van de Wiv 2017 valt op dat geen expliciet onderscheid wordt gemaakt tussen de inzet van bevoegdheden ten aanzien van buitenlandse communicatie en binnenlandse communicatie. De Wiv 2017 biedt het juridische kader voor de inzet van bevoegdheden door de diensten, ongeacht waar ter wereld die inzet plaatsvindt en ongeacht de nationaliteit, woonplaats of plaats van verblijf van de burgers die het betreft. De rechtsbeschermingsnormen van de Wiv strekken zich dus niet alleen uit tot de Nederlandse burger, maar tot elk persoon ten aanzien van wie de diensten bevoegdheden inzetten.

Dit is anders dan de wetgeving voor inlichtingen- en veiligheidsdiensten in de meeste andere landen. In veel landen bestaan wel aparte regimes, waarbij voor buitenlandse communicatie en/of buitenlanders in het buitenland minder waarborgen gelden.[34] De Wiv 2017 maakt geen expliciet onderscheid maar verklaart de Wiv 2017 juist algemeen van toepassing op al het handelen van de diensten (artikel 2). Hierdoor creëert de wet een algeheel juridisch kader dat ook geldt voor het handelen van de diensten dat deels in het buitenland plaatsvindt en/of directe en voorzienbare effecten in het buitenland of tegen buitenlanders heeft.[35] Dat de Wiv 2017, inclusief de rechtsbeschermingsnormen, ook van toepassing is op personen in het buitenland hebben de TIB en de CTIVD onderstreept in een brief over journalisten en advocaten in het buitenland.[36] De holistische benadering van de Wiv sluit aan bij de universaliteit van mensenrechten en is internationaal aangemerkt als *best practice*.[37]

De Evaluatiecommissie hecht waarde aan de internationale voorbeeldfunctie van de Wiv 2017 op dit punt. Daarnaast onderstreept de Evaluatiecommissie het rechtstatelijke belang van het uitgangspunt van de Wiv 2017, zoals dat voortvloeit uit het universeel geformuleerde artikel 2, dat bij de uitvoering van de wet privacybescherming en andere waarborgen dienen te gelden ten aanzien van personen, ongeacht waar ter wereld zij zich bevinden. Deze bescherming geldt binnen Nederland zonder onderscheid naar nationaliteit of herkomst en evenzeer voor personen buiten Nederland. Hier wordt in §3.4 en §8.5 verder op ingegaan.

---

[34] In de VS is de *Fourth Amendment* niet van toepassing op buitenlanders buiten de VS. In het VK wordt een onderscheid gemaakt tussen *internal* en *external communication*, waarbij *external communication* is: "*a communication sent or received outside the British Islands*". EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUDO05817013, (*Big Brother Watch)*, r.o. 69-71.

[35] De terminologie van de diensten en de toezichthouders, zoals bijvoorbeeld gebezigd in jaarverslagen, sluit niet altijd volledig bij deze benadering aan. Zo spreekt het AIVD jaarverslag van 2019 over de persoonlijke levenssfeer van 'burgers' in plaats van 'personen'. Zie AIVD. (2019). *Jaarverslag 2019*. p. 22. Zie ook: CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 3.

[36] TIB en CTIVD. (2018). *Rechtsbescherming advocaten en journalisten in het buitenland*. Brief van 31 mei 2018, beschikbaar via **https://www.tib-ivd.nl/documenten/brieven/2018/05/31/rechtsbescherming-advocaten-en-journalisten-in-het-buitenland**.

[37] Wetzling, T en K. Vieth. (2018). Upping the Ante on Bulk Surveillance; An International Compendium of Good Legal Safeguards and Oversight Innovations. *Heinrich Boll Stiftung*. p. 23.

3 De Wiv 2017 in een veranderende wereld

3.1 Inleiding

De Wiv 2017 en de totstandkoming ervan zoals geschetst in hoofdstuk 2 staan niet op zichzelf. Voor een goede evaluatie van een wet is de (internationale) context waarin de wet tot stand is gekomen en waarin zij wordt uitgevoerd belangrijk. Dit geldt zeker voor de Wiv 2017; een wet die is ontstaan en wordt toegepast in een tijd waarin de ontwikkelingen snel gaan. Niet alleen het internationale geopolitieke speelveld verandert, ook de technologische ontwikkelingen staan niet stil. Dit heeft gevolgen voor de taakuitvoering van de diensten. De wetgever wilde met de Wiv 2017 tot modernisering van de wet komen, vooral in het licht van die technologische vooruitgang. Daarnaast is ook het denken over privacyrecht en de bijbehorende jurisprudentie in ontwikkeling en is er een groeiend onbehagen in de samenleving over gegevensverwerking door bedrijven en organisaties.

De toepassing van de wet vindt plaats tegen de achtergrond van deze ontwikkelingen. In dit hoofdstuk wordt deze context geschetst. Hierover bestaat veel relevante literatuur. De Evaluatiecommissie haalt in dit hoofdstuk daarom verschillende rapportages en artikelen aan waarin deze ontwikkelingen worden beschreven, zonder deze ontwikkelingen opnieuw uitgebreid te duiden.

3.2 Een veranderende veiligheidssituatie

3.2.1 Internationale spanningen

In de wereld staan de geopolitieke verhoudingen sterk onder druk als gevolg van de assertievere opstelling van Rusland en China, het veranderend Amerikaans leiderschap en de opkomst van nieuwe spelers. Dit leidt tot nieuwe mondiale spanningen en ontvlambare geopolitieke situaties. De verschuiving van de internationale machtsbalans naar een meer multipolaire orde – ook wel de 'multi-orde wereld'[38] genoemd – brengt grotere onvoorspelbaarheid met zich mee. De spanningen blijven niet beperkt tot het geopolitieke domein. Zo zorgt de positie van China als grootste economie voor geo-economische spanningen tussen de Verenigde Staten en China en wordt in Europa steeds nadrukkelijker gedacht in termen van strategische autonomie en digitale soevereiniteit.[39]

De traditionele internationale samenwerkingsverbanden blijken daardoor minder effectief. Deze samenwerkingsverbanden worden door verschillende landen steeds meer ondergeschikt gemaakt aan het eigen belang. Zo komen, onder meer op militair gebied, internationale normen en regels onder druk te staan, zoals verdragen die zien op conventionele wapenbeheersing en de

[38] Instituut Clingendael. (2017). *Multi-Orde: Strategische Monitor 2017*. p. 13-21.

[39] Adviesraad Internationale Vraagstukken. (2020). *Advies 112: Europese veiligheid: tijd voor nieuwe stappen*. p. 4, 8; Bijlage bij *Kamerstukken II* 2018/19, 30 821, nr. 81, p. 19 (Nationale Veiligheid Strategie 2019); Bijlage bij *Kamerstukken II* 2017/18, 33 694, nr. 12, p. 13-14 (Wereldwijd voor een veilig Nederland - Geïntegreerde Buitenland- en Veiligheidsstrategie 2018 – 2022); Instituut Clingendael (2017). *Multi-Orde: Strategische Monitor 2017*. p. 13-21; Ministerie van Defensie (2020). *Defensievisie 2035*. p. 10-14; Europese Raad. (2020). *Digitale toekomst voor Europa*. Beschikbaar via **https://www.consilium.europa.eu/nl/policies/a-digital-future-for-europe/#**.

non-proliferatie van nucleaire en chemische wapens. Een aantal wapenbeheersingsverdragen is opgezegd of dreigt niet meer verlengd te worden en de nucleaire retoriek wordt harder.[40]

Deze ontwikkelingen leiden ertoe dat niet alleen rekening moet worden gehouden met onvoorspelbare en veranderlijke internationale verhoudingen maar ook met een veelheid aan actoren en de dreigingen die hieruit voortvloeien. Om de Nederlandse samenleving te kunnen blijven beschermen tegen deze dreigingen, moet de Nederlandse overheid op de hoogte te zijn van deze dreigingen om hierop adequaat te kunnen anticiperen.

De diensten en het internationaal recht

Het (heimelijk) vergaren van inlichtingen betreffende andere landen of personen over de eigen landsgrenzen heen wordt niet expliciet gereguleerd door het internationale recht. Toch is het internationale recht relevant voor de diensten. Afhankelijk van de aard en geografische locatie van spionage kunnen verschillende, reeds bestaande, regels van het internationale recht van toepassing zijn.[41] Hierbij kan gedacht worden aan regels betreffende de soevereiniteit van staten en de beginselen van non-interventie en niet-inmenging in de binnenlandse aangelegenheden van andere staten, alsmede het internationale immuniteitenrecht en meer in het bijzonder diplomatieke immuniteit zoals gereguleerd in het Weens Verdrag inzake Diplomatiek Verkeer van 1961. Ondanks het bestaan van deze regels stellen staten en ook internationaal recht-juristen zich vaak gereserveerd op als het gaat om de interactie tussen internationaal recht en spionage. Buchan legt dit in zijn boek over cyberspionage en internationaal recht als volgt uit:

> *"On the one hand, [international lawyers] cannot deny that international legal rules are applicable to intrusive activities such as espionage because to do so would challenge the authority of international law. On the other hand, they are equally unwilling to renounce espionage as a tool of statecraft because they wish to preserve the national security benefits that this practice affords. Ultimately, their only way out of this impasse is to eschew the questions of whether espionage is compatible with international law and proclaim that international law is silent on the subject."* [42]

Het hierboven geschetste dilemma wordt nog groter als het gaat om cyberspionage. De aanvulling van HUMINT met SIGINT heeft de mogelijkheden voor staten om heimelijk inlichtingen te vergaren op zeer significante wijze vergroot, zowel qua schaal en snelheid

---

[40] Instituut Clingendael. (2020). *Strategische Monitor 2019-2020: The writing on the wall*. p. 49-52 en 78-79; Adviesraad Internationale Vraagstukken. (2020). *Advies 112: Europese veiligheid: tijd voor nieuwe stappen.* p. 4, 8; Drent, M. en A. Stoetman. (25 februari 2019). 'Opzegging van het INF-verdrag: Europa aan zet?' *Europa Nu*. Beschikbaar via **https://www.europa-nu.nl/id/vkw7h56951x1/nieuws/opzegging_van_het_inf_verdrag_europa_aan**; Bijlage bij *Kamerstukken II* 2017/18, 33 694, nr. 12, p. 13-14 (Wereldwijd voor een veilig Nederland - Geïntegreerde Buitenland- en Veiligheidsstrategie 2018 – 2022); Ministerie van Defensie (2020). *Defensievisie 2035*. p. 13-14.

[41] Chesterman, S. (2006). The spy who came in from the Cold War: intelligence and international law. *27 Michigan Journal of International Law 1071*. p. 1072; Forcese, C. (2011). Spies without norders: international law and intelligence collection. *5 Journal of National Security Law and Policy 179*, p. 185; Smith, J.H. (2007). Key-Note Address: State Intelligence Gatherine and International Law, *28 Michigan Journal of International Law 543*. p. 544.

[42] Buchan, R. (2019). *Cyberespionage and international law*. Oxford, UK: Hart Publishing, introduction.

als qua intensiteit en diepte.[43] Het internationale recht is echter ook maar beperkt zichtbaar in het reguleren van cyberoperaties die door staten worden uitgevoerd.[44] Specifieke internationale cyberverdragen, zoals de *Budapest Convention on Cybercrime*, beperken zich tot het adresseren van cybercrime en -gedrag van niet-statelijke entiteiten.

Op internationaal niveau bestaat wel overeenstemming dat internationaal recht van toepassing is op cyberspace maar niet over de vraag *hoe* precies.[45] Een groep van onafhankelijke internationale experts heeft het voortouw genomen om tot nadere regelgeving te komen en dit heeft geresulteerd in de *Tallinn Manuals 1.0* (2013) en *2.0* (2017).[46] Deze *Manuals* zijn op zichzelf niet bindend maar Nederland heeft aangegeven dat het een meer inclusieve en gedetailleerde discussie over de toepassing van internationaal recht op cyberoperaties aan de hand van de *Tallinn Manual 2.0 on the international law* ondersteunt.[47]

Nederland heeft een belangrijke voortrekkersrol genomen in de internationale discussie over cyberbeleid, en heeft ook haar visie op de toepasselijkheid van het internationale recht op cyberspace gepubliceerd.[48] Ook onafhankelijke experts blijven bijdragen aan de verdere detaillering van toepasselijk internationaal recht.[49] Desalniettemin bestaan er nog veel vragen en onzekerheden over wat precies toelaatbaar is onder het internationale recht en welke reactie gepast is om '*malicious*' cyberoperaties te voorkomen of te verstoren. Deze vragen kunnen vooral ook een rol spelen bij strategische operaties zoals wordt besproken in §7.4.

De zich ontwikkelende discussies over de inhoud van het internationale recht zijn derhalve ook voor de diensten van belang. Het verdient de aanbeveling om zorg te blijven dragen voor goede inbedding van aandacht voor het internationale recht in de praktijk van de diensten, alsmede voor structuren die coherentie tussen internationale standpunten van Nederland en de praktijk van de diensten waarborgen. Internationaal recht dient daarnaast onderdeel te zijn van de afwegingen die de betrokken ministers maken bij beslissingen om bijzondere bevoegdheden internationaal in te zetten.

---

[43] Ibid.

[44] Zoals ook opgemerkt in de rapporten van Duncan Hollis als OAS Juridical Committee Special Rapporteur.

[45] Report of the Group of Government Experts on Development in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013. Zie ook het rapport uit 2015, UN Doc. A/70/174, 22 July 2015.

[46] Schmitt, M.N. (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press; Schmitt, M.N. (ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, UK: Cambridge University Press.

[47] *Kamerstukken II* 2018/19, 33 694, nr. 56.

[48] Ibid. Zie ook *Kamerstukken II* 2020/21, 33694, nr. 60.

[49] Zie ook 'Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector' (2020). Beschikbaar via **https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea**; en 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research' (2020). Beschikbaar via **https://www.law.ox.ac.uk/news/2020-08-12-second-oxford-statement-international-law-protections-healthcare-sector-during-covid**.

3.2.2 Technologie

De afgelopen periode wordt ook gekenmerkt door snelle ontwikkelingen op het gebied van datatechnologie, AI (kunstmatige intelligentie), autonome systemen, kwantumtechnologie, het cyberdomein en biotechnologie.[50] Deze ontwikkelingen zijn bovendien onderling verbonden waardoor ze elkaar versterken. Tegelijkertijd is een democratisering van technologie te zien, waardoor zeer krachtige technologie op een heel eenvoudige en ook steeds goedkopere wijze door individuen en organisaties kan worden gebruikt.[51] Dit leidt tot veranderingen in het dagelijks gebruik van communicatietechnologie, zowel de manier waarop gecommuniceerd wordt als de aard van de communicatie zelf. Communicatiestromen worden groter, complexer en meer divers. Om deze gegevensstromen te kunnen duiden, zijn steeds meer geavanceerde data-analyse technieken nodig. Dit geldt zeker ook voor het werk van de diensten.

Daarnaast groeit het aantal communicatiekanalen; in 2020 zijn al miljarden *devices*, al dan niet bewust, gekoppeld aan het internet. De verscheidenheid in deze *devices* – en van de kwetsbaarheden daarin – neemt daardoor ook toe: van ijskast tot dataserver en van deurbel tot dijkbewaking. De technologische ontwikkelingen zorgen dus voor een snelle doorontwikkeling van (militaire) systemen en een enorme groei van persoonsgegevens die op het internet en binnen bedrijven en overheden in omloop zijn. De verwachting is bovendien dat deze groei de komende jaren onverminderd doorgaat.

3.2.3 Diffuse dreiging

De genoemde geopolitieke en technologische veranderingen kunnen niet los van elkaar worden gezien en hebben allebei invloed op de veiligheid van Nederland. De Wetenschappelijke Raad voor Regeringsbeleid (WRR) concludeert dat de Nederlandse veiligheidsomgeving is verslechterd.[52] Dankzij de technologische ontwikkelingen kennen conflicten tussen staten steeds vaker – naast meer ontwikkelde conventionele wapens - een digitale component. Met de toename van hybride conflictvoering worden deze conventionele en digitale middelen meer en meer in samenhang ingezet.[53]

De digitale dreiging richting Nederland neemt toe. Deze dreigingen zijn diffuus en dynamisch, waardoor het complex is om de aard en oorsprong te achterhalen. Digitale aanvallen hebben een groeiend bereik en grotere opbrengst, tegen lage kosten en een relatief laag afbreukrisico. Dat maakt deze middelen aantrekkelijk voor staten om in te zetten, onder meer voor heimelijke beïnvloeding (inclusief het verspreiden van desinformatie en het beïnvloeden van verkiezingen), spionage en sabotage. Staten zijn steeds meer bereid tot digitale aanvallen, direct, of via hackersgroepen of *cyberproxies* zoals bedrijven. Deze aanvallen zijn niet alleen gericht op politieke maar ook op economische, militaire en technologische informatie met als doel om de eigen positie te verbeteren. Bovendien geven technologische ontwikkelingen staten de mogelijkheid om met behulp van investeringen in deze technologieën een dominante positie te bemachtigen. Door de

[50] NATO Science & Technology Organization. (2020). *Science & Technology Trends 2020-2040.* p vii.
[51] UK Government Home Office. (2020). *Future Technology Trends in Security.* p. 3.
[52] Wetenschappelijke Raad voor Regeringsbeleid. (2017). *Rapport nr. 98: Veiligheid in een wereld van verbindingen.* p. 176.
[53] Bijlage bij *Kamerstukken II* 2017/18, 33 694, nr. 12, p. 16 (Wereldwijd voor een veilig Nederland - Geïntegreerde Buitenland- en Veiligheidsstrategie 2018 – 2022); Ministerie van Defensie (2020). *Defensievisie 2035.* p. 10-14.

afhankelijkheid van deze technologieën wordt Nederland kwetsbaarder voor digitale spionage en sabotage door kwaadwillende staten.[54]

Naast dreiging vanuit staten spelen ook niet-statelijke actoren een rol. Zo vormt de jihadistische beweging in Nederland een belangrijke factor bij de aanzienlijke terroristische dreiging[55] tegen Nederland. Ook gaat er dreiging uit van niet-statelijke actoren zoals terroristische groeperingen op het gebied van chemische, biologische en nucleaire wapens. Als gevolg van de technologische ontwikkelingen kunnen zij gemakkelijker aan (kennis over) deze wapens komen en voelen zij zich niet of steeds minder gebonden aan internationale afspraken.[56]

Niet alleen de wereld, maar dus ook de aard en herkomst van de dreiging blijven in beweging. De Nationale Veiligheid Strategie[57] uit 2019 stelt vast dat de huidige ontwikkelingen van dreiging vragen om een versterkte en geïntegreerde aanpak door de Nederlandse overheid. De diffuse bedreiging van nationale veiligheid vormt een bedreiging voor het ongestoorde privéleven van de betrokken burgers. De Wiv 2017 moet de diensten bevoegdheden geven om deze dreiging op een adequate manier in kaart te brengen.

3.2.4 Zorgen in de samenleving

Persoonlijke gegevens van burgers worden door veel verschillende bedrijven en organisaties verwerkt voor velerlei doeleinden. Deze gegevens betreffen onder meer financiën, communicatie via mail-, chat- of videodiensten, online aankopen (mogelijk op basis van gepersonaliseerde reclame), slimme apparaten in huis, online muziek- of videodiensten, zoekdiensten, sociale media, *self-tracking* en digitale monitoring in de zorg. Vaak is deze gegevensverwerking niet transparant en is onduidelijk welke verwerkingen werkelijk in het belang van de burger zijn en welke op de achtergrond ook (of vooral) andere belangen dienen. Een sterke informatiepositie kan gebruikt worden voor profilering, *nudging*, sturing en zelfs manipulatie van burgers. Het onbehagen hierover groeit, zoals ook blijkt uit de druk om dominante marktpartijen op te breken. De onthullingen van Edward Snowden[58] over de grootschalige interceptie-activiteiten van de Amerikaanse inlichtingendienst NSA zijn een rol gaan spelen bij dit onbehagen. Naast de hierboven genoemde dreigingen tegen Nederlandse belangen, bestaan ook bedreigingen van de privacy en autonomie van burgers. Het ongemak en verzet hiertegen kwam ook naar voren bij de discussies rondom het raadgevend referendum over de Wiv 2017.

---

[54] Bijlage bij *Kamerstukken II* 2019/20, 26 643, nr. 695, p. 25 en 31 (Cybersecuritybeeld Nederland 2020); Bijlage bij *Kamerstukken II* 2018/19, 30 821, nr. 81, p. 27 en 31 (Nationale Veiligheid Strategie 2019); Instituut Clingendael. (2020). *Strategische Monitor 2019-2020: The writing on the wall*. p. 22-27; Ministerie van Defensie (2020). *Defensievisie 2035*. p. 13-14; Bijlage bij *Kamerstukken II* 2017/18, 33 694, nr. 12, p. 16, 19-20 (Wereldwijd voor een veilig Nederland - Geïntegreerde Buitenland- en Veiligheidsstrategie 2018 – 2022); AIVD (2019). *Offensief cyberprogramma een ideaal businessmodel voor staten*. p. 4-8; AIVD (2020). *Jaarverslag 2019*. p. 3, 6-7; MIVD (2020). *Jaarverslag 2019*. p. 17-18.

[55] Dreigingsbeeld Terrorisme Nederland 52 stelt het dreigingsniveau op 'aanzienlijk'. Dat wil zeggen dat de kans op een aanslag in Nederland voorstelbaar is. Daarbij moet vooral worden gedacht aan aanslagen van eenlingen of kleine groepen met een jihadistisch motief of uit een andere extremistische hoek. Zie *Kamerstukken II* 2019/20, 29 754, nr. 546, p. 3.

[56] Instituut Clingendael. (2020). *Strategische Monitor 2019-2020: The writing on the wall*. p. 47-48, 123; Bijlage bij *Kamerstukken II* 2017/18, 33 694, nr. 12, p. 21 (Wereldwijd voor een veilig Nederland - Geïntegreerde Buitenland- en Veiligheidsstrategie 2018 – 2022).

[57] De NVS is een driejaarlijkse publicatie die beschrijft wat de nationale veiligheidsbelangen zijn die beschermd moeten worden, hoe die belangen op dit moment worden bedreigd en op welke wijze deze risico's en dreigingen het hoofd wordt geboden. De NVS wordt onder coördinatie en (proces-)regie van de NCTV opgesteld. Bijlage bij *Kamerstukken II* 2018/19, 30 821, nr. 81, p. 19 (Nationale Veiligheid Strategie 2019).

[58] Zie onder meer Greenwald, G. en E. MacAskill. (7 juni 2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Beschikbaar via **https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data**.

De Evaluatiecommissie heeft oog voor dit ongemak. In een wereld waarin grote bedrijven en autocratische leiders dominante posities hebben en waarin het gezag en de geloofwaardigheid van instituties in een democratische samenleving gemakkelijk ondermijnd dreigen te worden, is normering, rechtsbescherming en effectief toezicht essentieel voor het vertrouwen van de burger. Buiten het domein van de nationale veiligheid is de Algemene Verordening Gegevensbescherming (AVG) het leidende kader, met de Autoriteit Persoonsgegevens als toezichthouder. Binnen het domein van de nationale veiligheid wordt het kader gegeven door de Wiv, met de TIB en CTIVD als primaire toezichthouders. Ook het internationaal recht en het Europees recht, en in het bijzonder de mensenrechten, zijn van belang bij de regulering van de diensten. Het moet duidelijk en gegarandeerd zijn dat de diensten enkel werken om de democratische samenleving en haar burgers te beschermen. Dat voor die bescherming onder gecontroleerde omstandigheden de privacy van diezelfde burgers, in het binnen- of buitenland, geschonden wordt, geeft een spanning die inherent is aan het functioneren van de diensten. Alleen met maximale transparantie en voorzienbaarheid van de wet en met effectief toezicht kan een democratie hier mee omgaan. Maar ongemak blijft. Dat zal ook dit rapport niet volledig weg kunnen nemen, al hoopt de Evaluatiecommissie met dit rapport wel bij te dragen aan het verminderen van dit ongemak.

3.3 De Wiv 2017 en privacy

3.3.1 De Wiv als privacywet

De Wiv 2017 regelt de taak, doelstelling en bevoegdheden van de AIVD en MIVD. De diensten mogen deze bevoegdheden alleen inzetten wanneer de inzet voldoet aan de vereisten van proportionaliteit, subsidiariteit en noodzakelijkheid en als de inzet zo gericht mogelijk is (artikel 26). Deze open normen vullen de rechtmatigheidstoets van de inzet van een bevoegdheid in. Een bevoegdheid mag alleen worden ingezet als zij onder de omstandigheden van het geval (waaronder de ernst van de dreiging), mede in vergelijking met andere beschikbare bevoegdheden, voor 'de betrokkene' het minste nadeel oplevert (subsidiariteit). Uitoefening blijft achterwege als deze onevenredig nadeel voor 'de betrokkene' oplevert; de uitoefening moet evenredig zijn aan het beoogde doel (proportionaliteit). De uitoefening moet tenslotte doelgericht zijn, waarbij het verwerven van gegevens die niet noodzakelijk zijn voor het onderzoeken tot een minimum moet worden beperkt (het gerichtheidsvereiste). Doet zich bij de uitoefening een minder belastend alternatief voor, dan wordt de meer belastende uitoefening 'onmiddellijk gestaakt'.

De Wiv 2017 is dus eigenlijk een informatiewet die de bevoegdheden van diensten regelt om inlichtingen te verwerven, deze te interpreteren en te bewaren (of te verwijderen) met betrekking tot organisaties en personen die, kort gezegd, een gevaar zijn voor het voortbestaan van de democratie of een gevaar zijn voor de veiligheid van de staat. In een democratische rechtsstaat mag de overheid immers alleen actief informatie verzamelen, bewerken en opslaan met een adequate wettelijke grondslag en doelbinding. Dit betekent dat het toetsingskader voor de juiste inzet van bevoegdheden ruimer is dan privacy, maar dat ook rekening gehouden moet worden met de belangen van de nationale veiligheid. Bij het verkrijgen van gegevens kunnen inbreuken op eigendomsrechten of op statelijke soevereiniteit plaatsvinden en kunnen ook andere (mensen)rechten en belangen in het geding zijn. Vaak zullen dat vooral privacyrechten zijn en dan dikwijls niet alleen die van de direct betrokken potentiële informatiebron – of het *target* –, maar ook van derden-individuen, zoals bijvoorbeeld bij bulkinterceptie (zie hoofdstuk 4).

Het voorgaande impliceert dat de bescherming van de privacy een belangrijke rol speelt. Dat is ook tot uiting gebracht in een aantal algemene bepalingen die erop ziet hoe de diensten verzamelde gegevens vervolgens moeten verwerken.[59] Zo is er het vereiste van doelbinding (artikel 18, lid 1) en zijn er beperkende voorschriften als het gaat om de verwerking van 'persoonsgegevens' (artikel 19). Verwerking mag slechts plaatsvinden ten aanzien van personen die een ernstig vermoeden oproepen dat zij een bedreiging van de democratische rechtsorde zijn (lid 1 en 2), tenzij "de gegevens van andere personen een onlosmakelijk onderdeel vormen van door de diensten te verwerven gegevensbestanden" (lid 5). Verwerking mag niet plaatsvinden op grond van godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid of seksuele geaardheid (lid 3), tenzij "in aanvulling op de verwerking van andere gegevens, en slechts voor zover voor het doel van de verwerking onvermijdelijk" (lid 4). Ook is er een algemene norm voor het bewaren van gegevens (artikel 20) en gelden er zorgplichtvereisten die onder meer de juistheid en volledigheid van gegevens en de kwaliteit van de gegevensverwerking regelen (artikel 24).

Naast deze algemene bepalingen voor verwerking bepaalt de wet ook dat de gegevens inzake de bron van een journalist en gegevens die betrekking hebben op de vertrouwelijke communicatie tussen advocaat en cliënt alleen mogen worden verzameld en bewaard met toestemming van de rechtbank Den Haag (artikel 30). Daarnaast bevat de wet een aan het privacyrecht ontleende regel die geautomatiseerde beslissingen ten aanzien van personen verbiedt: "het bevorderen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van geautomatiseerde data-analyse is niet toegestaan" (artikel 60, lid 3). Ten aanzien van het verstrekken van persoonsgegevens bepaalt de wet dat dit verboden is wanneer de juistheid van de gegevens redelijkerwijs niet kan worden vastgesteld of als die meer dan tien jaar geleden zijn verwerkt (artikel 68 en 69). Tenslotte voorziet de wet in de 'notificatieplicht' aan degenen die voorwerp van onderzoek zijn (artikel 59) en het inzagerecht (artikel 76 en 80).

Verwerving en verwerking

De Wiv 2017 sluit in haar terminologie aan bij die van de AVG. Zowel de AVG als de Wiv 2017 gebruiken de term 'verwerking' als overkoepelende term voor alles wat er met gegevens wordt gedaan.

Artikel 4, lid 2, van de AVG definieert verwerking als volgt:

> "een *be*werking of een geheel van *be*werkingen (*any operation or set of operations*) met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen (*collecting*), vastleggen (*recording*), ordenen (*organisation*), structureren (*structuring*), opslaan (*storage*), bijwerken of wijzigen (*adaption or alteration)*, opvragen (*retrieval*), raadplegen (*consultation*), gebruiken (*use*), verstrekken door middel van doorzending (*disclosure by transmission*), verspreiden of op andere wijze ter beschikking stellen (*dissemination or otherwise making available*), aligneren of combineren (*alignment or combination*), afschermen, wissen of vernietigen (*restriction, erasure, destruction*)"[60]

[59] Zie paragraaf 3.1 'Algemene bepalingen voor de verwerking van gegevens' van de Wiv 2017.
[60] Verordening (EU) 2016/679.

Artikel 1, onder f, van de Wiv 2017 hanteert voor het verwerken van gegevens een soortgelijke definitie als de AVG en omschrijft 'verwerking' als elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder ook het verzamelen van gegevens. Hoofdstuk 3 van de Wiv 2017 heet ook 'verwerking van gegevens'. In paragraaf 2 van dit hoofdstuk worden regels gesteld voor 'verzamelen' en in de daaropvolgende paragrafen worden andere vormen van 'verwerking' behandeld.

In zowel de Wiv 2017 als de AVG is 'verwerken' dus steeds het verzamelbegrip dat alle vormen handelingen met gegevens omvat, waaronder het verzamelen/verwerven van gegevens. Om toch een onderscheid te kunnen maken tussen het verzamelen/verwerven van gegevens en het daaropvolgende gebruik van de gegevens, wordt in de praktijk door de diensten en de CTIVD gesproken van 'verdere verwerking'. Hiermee worden alle handelingen bedoeld met betrekking tot gegevens nádat deze zijn verworven/verzameld. Ook in de AVG wordt dit geduid als 'verdere verwerking'.[61]

In dit rapport worden voor de leesbaarheid gesproken van 'verwerving' of 'verzameling' voor het verkrijgen van gegevens en van 'verwerking' voor alle daaropvolgende handelingen met de gegevens. Met 'verwerking' wordt hiermee dus specifiek 'verdere verwerking' bedoeld. Het onderscheid tussen verwerving/verzameling en verwerking is van belang voor onder meer de omgang met bulkdata (hoofdstuk 4) en de scheidslijn tussen het ex-ante en ex-post toezicht (hoofdstuk 9). In de desbetreffende hoofdstukken wordt dit nader uitgewerkt.

3.3.2 Het algemene privacyrecht en het dataprotectierecht[62]

Wat is privacy? Ruwweg kunnen daar twee historische lijnen voor worden getrokken, die aan het eind van de 20ste eeuw samenkomen.

De oudste is de persoonlijke levenssfeer die ons afschermt van de (publieke) buitenwereld, de jongste de opslag van persoonsgegevens in databanken. De Amerikaanse boulevardpers zorgde aan het eind van de 19e eeuw in de Verenigde Staten voor het eerste privacyconcept: 'de persoonlijke levenssfeer', beter bekend als '*the right to be let alone*'. De periode 1850-1890 (de tijd van 'krantenmagnaten' Joseph Pulitzer en Ronald Hearst) werd gekenmerkt door een onstuimige groei van de massakranten. Zij vormden een nieuwe industrie die begerig was naar 'verhalen' uit het privéleven. De informatietechnologie die hierbij centraal stond was de met telelenzen de privésfeer binnendringende fotografie en afluisterapparatuur. Schending van privacy werd daardoor een nieuw maatschappelijk fenomeen. In reactie op deze ontwikkeling formuleerden de rechtsgeleerden Warren en Brandeis het nieuwe recht om 'alleen gelaten te worden'.[63]

In de periode dat het Europees Hof voor de Rechten van de Mens (EHRM) het in artikel 8 van het Europese Verdrag voor de Rechten van de Mens en de fundamentele vrijheden (EVRM) beschermde privacyrecht begon uit te bouwen tot een algemeen recht dat de persoonlijke levenssfeer (een recht om alleen gelaten te worden) beschermt, vond in Europa een andere, parallelle ontwikkeling plaats, die van de vorming van publieke en commerciële databanken.

[61] Zie o.a. artikel 5, lid 1, onder b, en artikel 6, lid 4, onder a, van de Algemene Verordening Gegevensbescherming.
[62] In dit stuk is gebruik gemaakt van Dommering, E.J. (2019). *De Europese informatierechtsorde*. Amsterdam: DeLex. p. 208-209, p. 269 en p. 300 e.v.
[63] Warren, S. en L. Brandeis. (1890). The Right to Privacy. *4 Harvard Law Review*, 193. p. 196.

De informatietechnologie die hier de sleutel vormt is de computer, van meet af aan een potentiële databank waarin persoonsgegevens kunnen worden opgeslagen en gecombineerd. Het Duitse Constitutionele Hof erkende begin jaren tachtig van de vorige eeuw een op de menselijke waardigheid gebaseerd 'recht op informationele zelfbestemming'. Het Duitse Hof stelde:

> "Iedereen die er niet zeker van kan zijn dat gegevens over maatschappelijk afwijkend gedrag voor langere tijd worden geregistreerd en kunnen worden gebruikt op een manier waarvan hij niets weet, zal proberen om dat gedrag niet te vertonen. Dat is in strijd met de elementaire functie van zelfbeschikking in een democratische samenleving waarin de burgers de mogelijkheid moeten hebben om deel te nemen aan het maatschappelijke en politieke leven zonder risico te lopen op een voor hem ondoorzichtige manier te worden geregistreerd."[64]

Kort daarvoor had de Raad van Europa een verdrag voor dataprotectie vastgesteld.[65] In Nederland leidde de ophef rond de volkstelling van 1971 tot de instelling van de commissie Koopmans. Deze commissie legde de grondslag voor de Wet Persoonsregistratie, de voorloper van de Wet Bescherming Persoonsgegevens (Wbp) en de Europese AVG.

Dat recht van informationele zelfbeschikking gaat over beperking van macht, aanvankelijk alleen die van de overheid, later ook die van commerciële en 'welzijn' machten. Het is dus in zoverre een 'omgekeerd' recht ten opzichte van het recht om alleen gelaten te worden. Het laatste gaat om afscherming van de persoonlijke levenssfeer, het eerste om uit de handen van de macht te blijven, althans het gebruik van persoonsgegevens in de sfeer van de macht aan regels te binden. Het zou zich daardoor al snel ontwikkelen tot een recht dat de overheid en commerciële machten controleert op het juist en proportioneel verzamelen, gebruiken en bewaren van persoonsgegevens. In de rechtsliteratuur is er daardoor al snel een aanhoudende discussie ontstaan of dit recht op bescherming van persoonsgegevens (ook wel: 'dataprotectierecht') eigenlijk wel een privacyrecht was en of het wel ging over 'zelfbeschikking'. Bij de parlementaire behandeling van de Wbp verwierp de regering dit Duitse concept van zelfbeschikking. Het zag het recht meer als een middel tot institutionele controle (informatie-, inzage- en correctierecht). Bij de latere discussie een dergelijk recht in de Grondwet op te nemen werd het afgewezen, "omdat de balans tussen de bescherming van de persoonlijke levenssfeer en het belang van de Nederlandse rechtsorde bij het vastleggen van persoonsgegevens"[66] zou worden verstoord.

De inhoud van dat 'zelfbeschikkingsrecht' heeft eerst gestalte gekregen in het Dataprotectieverdrag 108 van de Raad van Europa en de EG dataprotectierichtlijnen, in Nederland geïmplementeerd in de Wbp. De EU leidde een nieuw hoofdstuk in met een afzonderlijk recht op dataprotectie in artikel 8 van het EU Handvest, en, per eind mei 2018 in de AVG, die de beginselen van de dataprotectierichtlijnen verder uitwerken en tot een Europese wet verheffen.[67]

Het klassieke privacyrecht en het dataprotectierecht blijven aan elkaar verbonden omdat het uitgangspunt nog steeds is dat er een individu is die zijn rechten 'dicht bij' (de onmiddellijke privé-levenssfeer) of als datasubject 'op afstand' (opname in databestanden van derden) uitoefent. De kern van de rechten van dat datasubject wordt gevormd door het toestemmingsrecht voor het gebruik of de eisen voor het bestaan van een rechtvaardigingsgrond voor gebruik zonder toestemming. In alle gevallen mag de verwerking alleen plaatsvinden voor bepaalde

[64] BVerfG 15 december 1983, NJW 1984, (*Volkszählungsurteil),* p. 419.
[65] Conventie 108, d.d. 28 januari 1981.
[66] *Kamerstukken II*, 1999/2000, 27460, nr. 2.
[67] Verordening (EU) 2016/679, Uitvoeringswet AVG (Stb. 2018, 144).

gerechtvaardigde doeleinden (de zogenaamde doelbinding van artikel 6, lid 3, AVG), en moet er een inzage- en correctierecht zijn (artikel 15 en 16 AVG). Het hele systeem van opslag en verwerking moet transparant zijn. Toestemming, doelbinding, inzage- en correctierecht, transparantie zijn de kernrechten. Toezicht op naleving van die rechten door overheden en marktpartijen door een specifieke marktautoriteit met steeds verdergaande bevoegdheden is daarvan het sluitstuk. In Nederland is dat de ontwikkeling van de Registratiekamer tot de Autoriteit Persoonsgegevens.

In de 21ste eeuw is een kentering te bespeuren omdat publieke en commerciële databanken, waar persoonsgegevens van individuen zijn opgenomen, zo talrijk en omvangrijk zijn dat het individu niet meer in staat is zijn rechten uit te oefenen. Dit klinkt door in een recente beslissing van het Duitse Constitutionele Hof waarin het een aangepaste formulering van het zelfbeschikkingsrecht geeft:

> "De garantie van dit fundamentele zelfbeschikkingsrecht wordt in het bijzonder verwezenlijkt wanneer de ontplooiing van de persoonlijkheid door de overheidsautoriteiten wordt bedreigd die persoonsgegevens gebruiken en combineren op een manier die de betrokken persoon niet kan waarnemen of controleren. De reikwijdte van het recht op zelfbeschikking is niet beperkt tot gevoelige informatie. Gelet op de huidige mogelijkheden om gegevens te bewerken en te combineren is ieder persoonsgegeven even belangrijk." [68]

Het persoonsgegevensrecht is voor de naleving van de normen die uit het zelfbeschikkingsrecht voortvloeien in belangrijke mate afhankelijk geworden van een daartoe door de overheid aangestelde autoriteit of van het initiatief van een organisatie voor het algemeen en collectief belang. De eerste kan bestuurlijke sancties opleggen, de tweede kan via acties bij de rechter handhaving afdwingen.[69]

In het recht van de diensten is het systeem van controle afwijkend geregeld, maar even wezenlijk voor de bescherming van de rechten van de burger. Evaluatie van de Wiv 2017 betekent dan ook in belangrijke mate evaluatie van het toezicht op de bescherming van de rechten van de burger (zie hoofdstuk 9).

3.3.3 Big data

Deze rechten moeten in een samenleving van *big data*[70] anders worden ingevuld. Het doelbindingsbeginsel is niet verdwenen, maar is bij omvangrijke verzamelingen van gegevens in zijn algemeenheid minder eenduidig omdat soms pas in een later stadium van bewerking het gebruiksdoel kan worden vastgesteld.[71] De nadruk komt daardoor meer te liggen op de zorgvuldigheidsnormen die bij de verwerking ná verwerving in acht moeten worden genomen: in de aard van de gerichtheid van de selectie, de toegepaste analyse, de toegang tot de data, de bewaar-

---

[68] In de beslissing die aan de basis stond van EHRM 30 januari 2020, ECLI:CE:ECHR:2020:0130JUD005000112, (*Breyer)*; Nederlandse Jurisprudentie (NJ) 2020, Aflevering 51/52, met annotatie van E.J. Dommering).

[69] Bijvoorbeeld de uitspraak van de Rechtbank Den Haag, 5 februari2020,ECLI:NL:RBDHA:2020:865, (*SyRI)*; NJ 2020, nr. 386, Aflevering 45, p. 6768-6795.

[70] De term duikt omstreeks 2011 in de discussie op en stond toen voor de drie 'v''s: volume, velocity, variety, zie M.A.A. Oostveen, *Protecting individuals against negative impact of big data: the potential and limitations of the privacy and data protection law approach*, Amsterdam, dissertatie Universiteit van Amsterdam 24 juli 2017.

[71] Merel Koning, *The purpose and limitations of purpose limitation*, dissertatie Radboud universiteit Nijmegen d.d. 23 september 2020.

termijnen en de veiligheid en betrouwbaarheid van de gebruikte systemen. Hierin worden duidelijke fasen onderscheiden.[72] Voor bulkdata wordt dit nader uitgewerkt in §4.3.

Daarbij moet ook de verzameling en de aard van de persoonsgegevens nader worden gespecificeerd. In *big data* bevinden zich persoonsgegevens die niet het doel van het verzamelen zijn, dat soms bij verdere analyse kunnen worden, maar meestal niet. Soms zijn het onvolledige gegevens die pas na analyse in combinatie met andere gegevens 'persoonsgegevens' worden. Dit ligt al besloten in de definitie die al in artikel 2 van richtlijn 95/46 stond dat een persoonsgegeven slaat op een 'geïdentificeerde' of een 'identificeerbare' natuurlijke persoon.[73] Verder wordt de aard van de persoonsgegevens belangrijker omdat niet ieder persoonsgegeven iets of evenveel over het privéleven zegt. Die trend tekent zich duidelijk in de jurisprudentie af. Een onderscheid moet worden gemaakt tussen, wat genoemd kan worden, oriënterende of identificerende gegevens die een te identificeren persoon in verband brengen met het gebruik van een te identificeren communicatie apparaat (bijvoorbeeld een smartphone), zonder dat deze verder iets onthullen over het privéleven van de betrokkene. Een voorbeeld daarvan zijn recente uitspraken van Europese rechters over het opslaan van gegevens op SIM-kaarten.[74] Het aanleggen van deze gegevensverzameling wordt weliswaar aangemerkt als een verwerkingshandeling waarop in beginsel de beschermingsregels van toepassing zijn, maar daaraan worden minder zware eisen gesteld dan bij persoonsgegevens die meer onthullen over iemands privéleven (in het gegeven voorbeeld van de telefoon: waar en met wie iemand belt of de inhoud van die communicatie zelf). Dit sluit aan bij het - voor de analyse van bulkinterceptie in dit rapport geïntroduceerde onderscheid - tussen verzamelingen persoonsgegevens die aangemerkt kunnen worden als 'registergegevens' en die gezien moeten worden als 'gedragsgegevens'. Daarop wordt in §4.2.3 nader ingegaan.

3.4 Europese privacyregels en de inlichtingen- en veiligheidsdiensten

3.4.1 Toezicht

In §3.3 kwam het Europese recht ter sprake omdat dit een grote rol heeft gespeeld en speelt bij de ontwikkeling van het privacyrecht. In deze paragraaf wordt dieper ingegaan op de rol van het Europese recht in relatie tot de inlichtingen- en veiligheidsdiensten. Voor een goed begrip daarvan staat de Evaluatiecommissie in onderstaand kader eerst stil bij de vraag hoe dat recht precies invloed heeft op de Nederlandse rechtsorde.

Europees recht en de diensten

Het recht van de Raad van Europa (waarvan het EVRM het basisverdrag is) en het in de vorige paragraaf genoemde Dataverdrag 108 (een gespecialiseerd verdrag) zijn regionaal internationaal recht. Het verdrag is door bijna alle landen in Europa geratificeerd en goedgekeurd. De fundamentele rechten die het toekent aan de burgers in de verdragsstaten

[72] Nader uitgewerkt in de M.A.A. Oostveen, *Protecting individuals against negative impact of big data: the potential and limitations of the privacy and data protection law approach*, Amsterdam, dissertatie Universiteit van Amsterdam 24 juli 2017.

[73] HvJEU 19 oktober 2016, ECLI:EU:C:2016:779, (*Breyer*); NJ 2017, aflevering 392; HvJEU 29 juli 2019, ECLI:EU:C:2019:629, (*Facebook ID);* NJ, aflevering 97.

[74] HvJEU 2 oktober 2018, ECLI:EU:C:2018:788, (*Ministerio Fiscal*); NJ 2020, nr 232 en EHRM 30 januari 2020, (*Breyer)*; NJ 2020, Aflevering 51/52, met annotatie van E.J. Dommering).

zijn rechten waar de burgers een rechtstreeks beroep op doen. De Nederlandse Grondwet bepaalt in artikel 94 dat dit soort internationale verdragsrechten bij voorrang boven het nationale recht worden toegepast. Zo heeft het een grote rol gespeeld bij de ontwikkeling van de grondrechtelijke bescherming in Nederland. Als de hoogste nationale rechter een toepassing aan het EVRM heeft gegeven in relatie tot het nationale recht, kan aan het EHRM een beslissing worden gevraagd of de nationale rechter een juiste toepassing heeft gegeven. Dit Hof beoordeelt dan of een beperking die binnen het nationale recht door de nationale rechter werd geaccepteerd, voldoet aan de beperkingsdoeleinden die het verdrag kent en of de beperking die binnen zo'n doel aan het recht is opgelegd 'noodzakelijk is in een democratische samenleving'. De hoogste nationale rechters kunnen sinds 1 augustus 2018 ook prejudicieel een vraag aan het EHRM voorleggen.

In dat kader heeft het EHRM een rechtspraak ontwikkeld die toetst of de beperkingen die op het recht van privacy en het rechterlijk toezicht worden gemaakt in het belang van de nationale veiligheid en het goed functioneren van de inlichtingen- en veiligheidsdiensten in een democratische samenleving noodzakelijk is. Deze discussie keert terug in hoofdstuk 4 over bulkdata en hoofdstuk 9 over toezicht naar aanleiding van het Dataprotectieverdrag 108+.

De werking van het EU-recht is anders. De lidstaten van de EU-landen hebben op basis van het Verdrag betreffende de Europese Unie (EU-Verdrag) en het Verdrag betreffende de werking van de Europese Unie (VwEU) een Europese rechtsorde vastgesteld die rechtstreeks (via verordeningen) of na omzetting (richtlijnen) de inhoud van het interne nationale recht mede bepaalt. Daarnaast hebben de EU-staten in 2000 een Handvest voor de grondrechten van de EU vastgesteld. Dat betekent dat de nationale rechter die op basis van EU-recht intern beslissingen neemt ook moet kijken of dat in overeenstemming is met het EU-Handvest. Er is een EU-rechter, het Hof van Justitie van de Europese Unie (HvJEU), dat anders functioneert dan het EHRM. Zodra bij een nationale rechter een vraag van uitleg van het EU-recht rijst, worden daarover prejudiciële vragen aan dat Hof gesteld dat daarover in laatste instantie beslissingen neemt. Sinds het Handvest functioneert dit Hof ook als Europees Constitutioneel Hof doordat het EU-recht dat niet verenigbaar is met het Handvest onverbindend wordt verklaard. Dat heeft het Hof bijvoorbeeld gedaan in een aantal zaken die in deze paragraaf wordt besproken.

Dat EU-Handvest staat niet geheel los van het EVRM. Artikel 52, lid 3, van het Handvest bepaalt dat de rechten in het Handvest die overeenstemmen met het EVRM op dezelfde manier moeten worden uitgelegd als dat door het EHRM gebeurt (die volgens artikel 6, lid 3, van het EU-Verdrag deel uitmaken van de rechtsbeginselen van de EU). Het HvJEU en het EHRM stemmen op dit vlak hun rechtspraak dus steeds meer op elkaar af. Daarnaast bepaalt datzelfde artikel 52, lid 3, dat het Handvest ook meer bescherming kan bieden dan het EVRM, hetgeen bij privacy het geval is, omdat het in artikel 8 (artikel 15, VwEU) een recht op bescherming van persoonsgegevens kent, een expliciete regel die in artikel 8 van het EVRM ontbreekt. Dat heeft tot gevolg gehad dat de rechtspraak die het HvJEU over persoonsgegevens heeft ontwikkeld, indirect weer de verdere uitbouw heeft beïnvloed van de bescherming die het EVRM biedt.

De relatie tussen het EU-recht, het HvJEU en de nationale wetten die zien op de bevoegdheden van de inlichtingen- en veiligheidsdiensten is anders dan die van het EHRM. De EU-verdragen bepalen dat de lidstaten bevoegd blijven maatregelen te nemen in het belang van hun nationale veiligheid. Artikel 15, lid 1, van de richtlijn voor privacy en elektronische communicaties (richtlijn 2002/58/EG) kent aan de lidstaten de bevoegdheid toe om maatregelen in het belang van de nationale veiligheid te nemen die noodzakelijk, geschikt en proportioneel zijn. De artikelen 2, lid 2, en 23 AVG maken ook een uitzondering. Het HvJEU heeft aan die bepalingen die hier en in hoofdstuk 4 verder worden besproken in 2020 beslissingen gegeven die kunnen betekenen dat op dit gebied het EU-recht ook van belang wordt. Het ging om de uitleg van de nationale veiligheidsexceptie in artikel 15 van richtlijn 2002/58. Denkbaar is ook dat het Hof dat in de toekomst in het kader van artikel 23 AVG zal doen.

Ook ten aanzien van de activiteiten zoals gegevensverwerving en gegevensverwerking van de diensten heeft het EHRM belangrijke jurisprudentie ontwikkeld. Oude wetgeving in Europa voldeed vaak niet aan de eisen die het EHRM stelde. De waarborgen die rechten van burgers moesten beschermen, waren vaak niet voldoende verankerd in de nationale wetgeving. Een belangrijke waarborg voor de rechtsbescherming van burgers betreft het onafhankelijk toezicht, vooraf, tijdens en achteraf, op de werkzaamheden van de inlichtingen- en veiligheidsdiensten. Het EHRM in Straatsburg liet zich hier in de zaak *S. en Marper*[75] als volgt over uit:

> *"The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention (...), paragraph 47 above). The domestic law must also afford adequate guarantees that retained personal data are efficiently protected from misuse and abuse (see Article 7 of the Data Protection Convention - paragraph 47 above)."*

In latere uitspraken heeft het Hof in Straatsburg de noodzaak van effectief onafhankelijk toezicht op het werk van de diensten benadrukt zodat het plaatsvervangend kan optreden voor het gebrek aan mogelijkheden voor individuele actie.[76] Voor de eisen die aan dit toezicht moeten worden gesteld, verwijst het EHRM in de *Centrum för Rättvisa*-zaak naar het rapport van de Venetië-commissie[77]:

> *"According to the report, the two most significant safeguards were the authorisation process (of collection and access) and the oversight process. It was clear from the Court's case-law that the latter must be performed by an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation*

[75] EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204, *(S and Marper*).

[76] EHRM 4 december 2015, ECLI:CE:ECHR: 2015:1204JUD004714306,(*Roman Zakharov*); NJ 2017, 185; EHRM 6 juni 2016, ECHR:2016:0112JUD003713814, (*Szabó en Vissy)*; EHRM 19 juni 2018, ECLI:CE:ECHR:2018:061 9JUD003525208, (*Centrum för Rättvisa*); EHRM 13 september 2018, (*Big Brother Watch).*

[77] De commissie van de Raad van Europa die kwaliteitseisen voor de rechtsstaat ontwikkelt. De laatste versie van dit rapport is van 2015: https://rm.coe.int/16806daadb.

stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the Foreign Intelligence Surveillance Court. However, it noted that despite the existence of judicial authorisation, the lack of independent oversight of the court's conditions was problematic. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention. In this regard, a general complaints procedure to an independent oversight body could compensate for non-notification."[78]

Het EHRM kijkt dus naar het toezichtsysteem in zijn geheel. De doorslaggevende elementen voor *effectief* toezicht zijn: voorafgaand toezicht bij inzet van de bevoegdheden, onafhankelijkheid van de toezichthouder (te vergelijken met de rechterlijke macht), en toezicht op de uitvoering van de bevoegdheden. De verwachting is dat het Hof deze lijn zal doorzetten in de uitspraken van de *Grand Chamber* in de *Centrum för Rättvisa* en *Big Brother Watch* zaken die in 2021 zijn te verwachten. Zoals in §9.2 uiteen wordt gezet is de Evaluatiecommissie van oordeel dat het Nederlandse toezicht weliswaar kan worden verbeterd, maar aan de thans geldende Europese maatstaven voldoet.

3.4.2 Verwerking persoonsgegevens

Het EHRM heeft in een aantal zaken die betrekking had op politie- en opsporingsregisters proportionaliteitsnormen ontwikkeld, vergelijkbaar met degenen die gelden voor verzameling en verdere verwerking van persoonsgegevens in het algemeen. Kort gezegd komt dit neer op regels die zien op de aard van de delicten waarvoor een verdenking bestaat, de categorieën van personen die mogen worden 'gevolgd', de tijdsduur dat ze mogen worden gevolgd, regels voor opslag, toegang en onderzoek van verzamelde gegevens, de transparantie van de regels, en regels omtrent de duur van de opslag.[79] Deze zes basisbeginselen zijn ook van belang voor de gegevensverwerking van de diensten. De in de vorige paragraaf genoemde beslissingen (thans aanhangig bij de *Grand Chamber*) gingen over bulkinterceptie door diensten (zie §4.3.1).

Zoals in het kader is uiteengezet, ligt de vraag of het EU-recht van toepassing is in het domein van de nationale veiligheid gecompliceerder, omdat zij rijst in het kader van de uitleg van het Unierecht. Het gaat steeds over de uitleg van Unierecht, in relatie tot de bevoegdheid van de lidstaten om hun nationale veiligheid zelf te regelen. Zij is al enige malen aan de orde geweest en werd voor het eerst opgeworpen in de bekende 'dataretentie'-zaken. De eerste zaak werd aangespannen in Ierland door de privacy-actiegroep *Digital Rights Ireland* en betrof de rechtsgeldigheid van de zogenaamde Dataretentierichtlijn (2006/24/EG).[80] De Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie was een lex specialis ten opzichte van de uit 1995 stammende algemene Privacyrichtlijn 95/46/EG, die in 2018 is vervangen door de AVG. Artikel 5, lid 3, van deze richtlijn stelde dat opslag van 'communicatie- en verkeersgegevens' kan plaatsvinden met toestemming van de betrokkenen als "opslag het uitsluitende doel heeft de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien

[78] EHRM 19 juni 2018, (*Centrum för Rättvisa*), r.o. 70 en 71.

[79] Het gaat hier om een lange reeks beslissingen, voornamelijk in de strafrechtelijke sfeer. Ten aanzien van een grootschalige inzameling en opslag is vooral van belang de beslissing inzake Liberty; EHRM 1 juli 2008, CE:ECHR:2008:0701JUD005824300, (*Liberty)*; NJ 2010, nr. 324.

[80] HvJEU 8 april 2014, ECLI:EU:C:2014:238, (*Digital Rights Ireland*); HvJEU 6 oktober 2015, ECLI:EU:C:2015:650 (*Schrems*); HvJEU 21 december 2016, ECLI:EU:C:2016:970, (*Tele2 Sverige*) en de gevoegde zaak (*Secretary of State)*; NJ 2017, 186, alle met annotatie van E.J. Dommering.

noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiesamenleving deze dienst kan leveren". Deze beperkte 'functionele' toestemming, nodig om de geïndividualiseerde dienst te kunnen leveren en factureren, kende in artikel 15, lid 1, een uitzondering. Deze liet het de lidstaten toe liet verdergaande beperkingen (dus langere opslag dan functioneel noodzakelijk) bij wet te regelen, "indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale belangen, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van elektronische communicatiesystemen". Aangezien de EU vreesde dat deze uitzondering tot te veel uiteenlopende nationale regelingen zou leiden, werd de Dataretentierichtlijn opgesteld, die deze uitzondering binnen een bepaalde bandbreedte (de lidstaten konden kiezen uit een termijn van een half tot twee jaar) harmoniseerde. *Digital Rights* beklaagde zich vervolgens bij de Ierse Data-Autoriteit dat de Dataretentierichtlijn onvoldoende rechtswaarborgen bevatte om deze verdergaande uitzondering te rechtvaardigen. Dit kwam neer op een klacht dat de Dataretentierichtlijn in strijd was met de artikelen 7, 8 en 11 van het Handvest. Het HvJEU kwam hier tot de conclusie dat de richtlijn in strijd was met de artikelen 7 en 8 omdat zij onvoldoende rechtswaarborgen bevatte en verklaarde deze richtlijn daarom nietig. De EU-Commissie heeft geen nieuwe dataretentierichtlijn vastgesteld en ook Nederland heeft afgezien van een voortzetting van de dataretentieregeling in gewijzigde vorm. Dit leidde tot nieuwe zaken. Met name in de Tele2 zaak[81] was aan de orde in hoeverre de beperking van de toepasselijkheid van EU-recht in het gebied van nationale veiligheid ook de gelding van de EU-regels voor privacy beperkte.

Pas in 2020 kwam deze vraag in de volle breedte aan de orde in de zaken *Privacy International* en de gevoegde zaken *La Quadrature du Net en anderen/ Ordre des barreaux francophones et germanophone en anderen*. Met name in de laatste zaken werden vergaande beslissingen gegeven over retentie, bulkinterceptie en geautomatiseerde data-analyse door telecomproviders in opdracht van inlichtingen- en veiligheidsdiensten.[82] In deze zaken ging het in de eerste plaats om de betekenis van de algemene richtlijn over privacy met betrekking tot elektronische communicatie (EG 2002/58). In overweging 11 van de considerans van de richtlijn (herhaald in de artikelen 1, lid 3, en 15 daarvan) verklaart deze de richtlijn niet van toepassing in zaken betreffende nationale veiligheid. Het HvJEU legt de uitzondering beperkt uit en formuleert een aantal proportionaliteitsregels die betrekking hebben op de activiteiten. Het Hof acht de doorzend- en retentieverplichtingen die de diensten aan telecommunicatieondernemingen kunnen opleggen te vergaand, gelet ook op de aard van de persoonsgegevens die zich in de bulkdataset bevonden. Het Hof erkent wel dat tussen de aard van die gegevens een onderscheid moet worden gemaakt. Het formuleert een set proportionaliteitsregels en toezichtregels waaraan deze specifieke vorm van toezicht moest voldoen. Een en ander zal in §9.2 verder besproken worden.

3.4.2 Internationale uitwisseling van persoonsgegevens

In de hiervoor besproken ontwikkeling van het EU-recht speelde ook de internationale uitwisseling van persoonsgegevens, waarvoor de EU de zogenaamde '*safe harbour*'-agreement met de Verenigde Staten had gesloten. Dit agreement beoogde dat alleen kon worden uitgewisseld als er een gelijkwaardig systeem van bescherming was. In de zaak Schrems achtte het Hof de getroffen voorziening ontoereikend.[83] In een tweede zaak, eveneens aangespannen door de

[81] HvJEU 21 december 2016, ECLI:EU:C:2016:970, (*Tele2 Sverige*) en de gevoegde zaak (*Secretary of State).*
[82] HvJEU 6 oktober 2020, ECLI:EU:C:2020:790, (*Privacy International*); HvJEU 6 oktober 2020, ECLI:EU:C:2020:929, *(Quadrature du Net and others*).
[83] HvJEU 6 oktober 2015, (*Schrems*); NJ 2016, 446 en 447.

Oostenrijker Schrems, achtte het HvJEU de onder de AVG getroffen regeling ook onvoldoende omdat het systeem van rechtsbescherming in de VS ontoereikend is. Op grond van de *Patriot Act* zouden Amerikaanse diensten onbeperkt toegang kunnen krijgen tot uitgewisselde persoonsgegevens.[84] Nu internationale uitwisseling van gegevens essentieel is voor het werk van de inlichtingen- en veiligheidsdiensten zijn deze uitspraken voor de evaluatie van het daarvoor gehanteerde systeem van waarborgen wezenlijk. Dit wordt in §8.2 verder uitgewerkt.

3.5 Conclusie

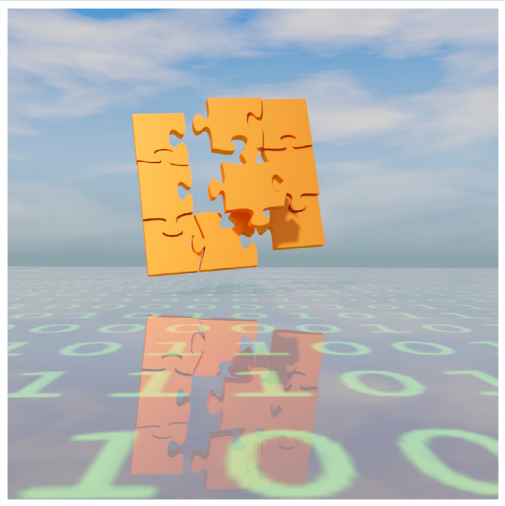
De totstandkoming en de toepassing van de Wiv 2017 staan niet op zichzelf. In dit hoofdstuk is in grote lijnen de relevante context van de wet geschetst. De oplopende geopolitieke spanningen en snelle technologische ontwikkelingen zorgen voor een toenemende diffuse en dynamische digitale dreiging. Tegelijkertijd groeit in de samenleving het onbehagen over niet transparante gegevensverwerking door bedrijven en instanties. Voor het vertrouwen in het werk van de diensten is normering, rechtsbescherming en effectief toezicht dan ook essentieel.

Daarnaast is de Europese jurisprudentie over privacy en gegevensverwerking een belangrijk onderdeel van de context van de Wiv 2017. Zo wordt in de jurisprudentie de aard van persoonsgegevens steeds belangrijker omdat niet ieder persoonsgegeven iets of evenveel over het privéleven zegt. Ook de geschetste Europeesrechtelijke ontwikkeling, voor een deel van na de inwerkingtreding van de Wiv 2017, is relevant voor deze wetsevaluatie. Ondanks dat het te vroeg is voor een volledige duiding van de betekenis van de meest recente uitspraken, geven die wel aan dat zij voor de juridische normering van het handelen van de diensten van wezenlijke betekenis zullen blijven. Op ieder relevant aspect daarvan zal daarom in de deelhoofdstukken nader worden ingegaan.

Alle in dit hoofdstuk beschreven ontwikkelingen laten het belang zien van het werk van de diensten en hun verstrekkende maar noodzakelijke bevoegdheden, als ook het belang van normering, rechtsbescherming en effectief toezicht op hun handelen. Dit vormt het centrale thema in dit rapport en de hierop volgende verdiepende hoofdstukken.

[84] HvJEU 16 juli 2020, ECLI:EU:C:2020:559, (*Schrems II*).

Deel II



4 Bulkdata

4.1 Inleiding

Een belangrijk doel van de Wiv 2017 is om de bevoegdheden waarover de diensten beschikken te moderniseren en tegelijkertijd de waarborgen met deze modernisering in balans te brengen. In de hoofdstukken 4 tot en met 7 wordt onderzocht of de wet op het gebied van de technische bevoegdheden tot verwerving en verwerking van gegevens in balans is, of er bij de uitvoering sprake is van knelpunten en zo ja, hoe deze knelpunten op te lossen.

In dit hoofdstuk wordt gekeken naar het verwerven en verwerken van het type gegevens dat in de praktijk 'bulkdata' wordt genoemd. Allereerst zullen het begrip bulkdata, de wettelijke bepalingen over bulkdata en het gebruik van deze gegevens in de praktijk worden toegelicht. Vervolgens wordt ingegaan op de *verwerving* van bulkdata, de huidige knelpunten en de daaruit volgende aanbevelingen. Tenslotte worden ook de knelpunten en aanbevelingen ten aanzien van de *verwerking* van bulkdata behandeld. Hierbij betrekt de Evaluatiecommissie ook het datareductiestelsel, inclusief de relevantiebeoordeling van bulkdata.

4.2 Bulkdata in de wet en praktijk

4.2.1 Wat is bulkdata

De technologische ontwikkelingen leiden tot een enorme groei van gegevensstromen en het aantal communicatiekanalen. Dit resulteert in grotere en complexere hoeveelheden gegevens (zie ook §3.2). Deze grote verzamelingen van gegevens worden bulkdata genoemd. Bulkdata is een omvangrijke verzameling van gegevens waarvan het merendeel betrekking heeft op personen en/of organisaties die niet in onderzoek zijn van de diensten en dit ook nooit zullen worden.[85] Bulkdata kenmerkt zich dus enerzijds door grootte en anderzijds door het type gegeven in de bulkdata. Het begrip bulkdata is daarmee niet gerelateerd aan *de wijze van verwerving* maar aan *de aard en omvang* van de gegevens zelf. Er wordt ook wel gesproken van 'bulkdatasets', waarmee specifieke, nader omlijnde verzamelingen van bulkdata wordt bedoeld. Het verzamelen en verwerken van bulkdata brengt een inbreuk op de privacy met zich mee. Met het verwerven van bulkdata komen namelijk gegevens van personen in de systemen van de diensten zonder dat er een hen betreffende reden is. Daarmee is het gevoeliger dan het *gericht* verzamelen van gegevens van een specifiek *target*.

Met bulkdatasets worden niet zogenaamde 'technische referentiesets' bedoeld. Deze technische referentiesets bevatten wel heel veel gegevens maar géén persoonsgegevens. Daarmee vallen ze niet binnen de definitie van bulkdata. Denk hierbij bijvoorbeeld aan zendmastgegevens van een mobiel telecommunicatienetwerk, of aan technische karakteristieken van een militair radarsysteem.

[85] Definitie gehanteerd in CTIVD toezichtsrapport nr. 70, zie: CTIVD. (2020). *Toezichtsrapport 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. Deze definitie wordt ook door de AIVD en MIVD gehanteerd. Deze definitie komt voor een belangrijk deel overeen met de gehanteerde definitie van de US National Academy of Sciences, zie: US National Academy of Sciences. (2015). *Bulk collection of signals intelligence: technical options*. The National Academies Press: Washington, D.C., **https://www.nap.edu/read/19414/chapter/1**.

4.2.2 Gebruik van bulkdata

De diensten verrichten hun onderzoekstaken in het belang van de nationale veiligheid.[86] Bulkdata is daarbij essentieel. Niet alleen de diensten en betrokken ministers geven dit aan, ook de CTIVD ziet dit zo.[87] De Evaluatiecommissie heeft van de diensten meerdere voorbeelden van het gebruik van bulkdata gekregen. De hierna opgenomen selectie van niet-gerubriceerde voorbeelden illustreert het gebruik van bulkdata voor de taakuitvoering van de diensten.[88] De Evaluatiecommissie is tot de conclusie gekomen dat zowel het verwerven en verwerken van bulkdata beter moet worden geregeld in de wet.

Voorbeelden gebruik van bulkdata

Onderzoek naar ISIS[89]

Bulkdatasets die de diensten verwerven, hebben in veel gevallen inlichtingenwaarde voor onderzoeken die betrekking hebben op dreigingen vanuit het buitenland, bijvoorbeeld bij het in kaart brengen van de locaties (en daarmee: de trajecten) van uitreizigers. In dat kader hebben de diensten onderzoek gedaan met behulp van een verworven bulkdataset met daarin onder andere locatie-metadata. Hierdoor hebben de diensten kunnen zien dat uitreizigers zich in een specifiek (toenmalig) ISIS-gebied in Syrië bevonden. Dit was een belangrijke schakel om te kunnen vaststellen dat deze personen zich hadden aangesloten bij ISIS. Zonder de locatie-metadata verkregen uit deze bulkdataset was dit niet mogelijk geweest. Over een aantal van deze uitreizigers is een ambtsbericht uitgebracht aan de Immigratie- en Naturalisatiedienst.

Bescherming van Nederlandse militairen[90]

In Afghanistan maken de diensten gebruik van bulkdatasets ter bescherming van Nederlandse militairen (*force protection*). Hiermee kan de dreiging tegen Nederlandse militairen en coalitiepartners worden onderkend (*threat to the force*). Deze bulkdataset geeft de MIVD bijvoorbeeld inzicht in de locaties en de bewegingen van (potentiële) tegenstanders in het missiegebied. Daarmee helpt de bulkdata ook bij het onderzoeken of het doel van de militaire missie wordt bedreigd (*threat to the mission*).

Ook worden aan de hand van bulkdatasets netwerken van personen gevonden die verantwoordelijk zijn voor de ontwikkeling en verspreiding van *Improvised Explosive Devices* (IED's). IED's vormen een concrete bedreiging voor Nederlandse militairen in missiegebied. Met behulp van de bulkdatasets identificeert de MIVD hoe het netwerk functioneert, is opgebouwd en wordt aangestuurd (*command & control*) en welke personen binnen

---

[86] Wiv 2017, artikel 8 en 10.

[87] *Kamerstukken II* 2019/20, 29 924, nr. 203 (Beleidsreactie CTIVD-rapporten nr. 70 en 71); CTIVD. (2020). *Toezichtsrapport 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. p. 3, 13, 22-23.

[88] In dit kader verwijst de Evaluatiecommissie ook graag naar het rapport van dhr. D. Anderson over de Investigatory Powers Bill van het Verenigd Koninkrijk en in het bijzonder Annex 8 t/m 11 waarin tientallen Britse *case studies* worden besproken. Hierin wordt expliciet gemotiveerd waar bulkdata noodzakelijk is. Zie: Anderson, D. (2016). *Report of the Bulk Powers Review*. Independent Reviewer of Terrorism Legislation, **https://www.gov.uk/government/publications/investigatory-powers-bill-bulk-powers-review**.

[89] Bron: Schriftelijke bijdrage van de AIVD en MIVD aan de Evaluatiecommissie.

[90] Ibidem.

het netwerk anderen opleiden om IED's te maken. Met deze inzichten kan de dreiging die uitgaat van IED's in missiegebied, zowel voor de Nederlandse militairen als de internationale partners, worden verminderd. Zo wordt rechtstreeks bijgedragen aan de bescherming van de Nederlandse militairen.

OPCW[91]

Nederland heeft als gastland van diverse internationale organisaties een bijzondere verantwoordelijkheid. Een zorgelijke ontwikkeling die de diensten onderkennen, is de ondermijning van de integriteit van internationale organisaties door statelijke actoren. Op 13 april 2018 heeft de MIVD een cyberoperatie van de Russische militaire inlichtingendienst GRU verstoord die zich richtte op het hacken van de Organisatie voor het Verbod op Chemische Wapens (verder: OPCW) in Den Haag. De MIVD wist dat vier inlichtingenofficieren zich door Nederland verplaatsten en was ervan op de hoogte dat zij met een auto geparkeerd stonden op een parkeerterrein naast het hoofdkantoor van de OPCW. De Russische inlichtingenofficieren vormden op dat moment een directe dreiging tegen de digitale communicatienetwerken van de OPCW. Mede dankzij de analyse van bulkdata kon snel en effectief worden opgetreden. Hoewel voor het onderkennen van deze dreiging tegen de OPCW gebruik is gemaakt van een combinatie van diverse informatiebronnen, was deze onderkenning niet mogelijk geweest zonder het gebruik van gegevens uit bulkdatasets.

Luchtaanvallen Syrië[92]

De OPCW deed onderzoek naar luchtaanvallen in Syrië in 2017. Bij deze aanvallen is zeer waarschijnlijk gebruik gemaakt van het chemische strijdmiddel sarin. Uit openbare bronnen bleek dat een van deze luchtaanvallen werd uitgevoerd door een militair vliegtuig vanaf de Syrische vliegbasis Shayrat. Door het analyseren van een bulkdataset hebben de diensten kunnen vaststellen welke personen zich rondom en op deze vliegbasis bevonden op het moment dat de luchtaanvallen werden voorbereid en uitgevoerd. De analyse van deze set door de diensten was doorslaggevend voor het aanwijzen van een vijftal sleutelfiguren in het Syrische chemische wapenprogramma. Bovendien vormde het een belangrijk puzzelstuk voor het internationaal onderzoek van de Syrische gifgasaanvallen. Zonder de bulkdataset had deze waardevolle bijdrage niet geleverd kunnen worden.

Gebruik registers van Nederlandse medeoverheden[93]

De diensten maken ook gebruik van register-bulkdata van Nederlandse medeoverheden zoals de Basisregistratie Personen (BRP). De BRP bevat persoonsgegevens van Nederlandse ingezetenen en van personen die Nederland hebben verlaten. De AIVD gebruikt deze gegevens bijvoorbeeld bij het uitbrengen van een ambtsbericht over een persoon, om de naam en geboortedatum van een persoon te kunnen onderbouwen. Op deze wijze is voor de ontvanger, bijvoorbeeld het Openbaar Ministerie, direct te verifiëren over wie een ambtsbericht gaat.

[91] Ibidem.
[92] Ibidem.
[93] Ibidem.

Gebruik passagiersgegevens bij terrorisme-onderzoek[94]
De diensten krijgen soms een melding binnen dat een bepaald persoon mogelijk een jihadist is. Het is van belang om een dergelijke melding goed te onderzoeken, zowel om deze uit te sluiten alsook om deze als basis te gebruiken voor verder onderzoek. Passagiersgegevens kunnen bij het duiden van zo'n melding als bron worden gebruikt. Door middel van deze bulkdata kunnen bijvoorbeeld historische vliegbewegingen van een persoon in kaart worden gebracht waarmee een inschatting gemaakt kan worden of verder onderzoek noodzakelijk is of dat de melding kan worden ontkracht. Passagiersgegevens worden ook gebruikt om meer informatie over bekende *targets* te achterhalen.

Het gebruik van bulkdata is een noodzakelijke component van de methoden en technieken die de diensten gebruiken bij onderzoek naar enerzijds concrete dreigingen en *targets* en anderzijds naar nieuwe of 'verborgen' dreigingen, waarbij de uiteindelijke *targets* nog niet bekend zijn. In de bovengenoemde voorbeelden komt dat vooral naar voren in het voorbeeld 'Bescherming van Nederlandse militairen'. Daarin wordt niet alleen onderzoek gedaan naar de gekende *targets* maar juist ook naar eventuele nieuwe *targets* of wat de gekende *targets* precies van plan zijn. Daarnaast laat het voorbeeld van de luchtaanvallen in Syrië de noodzaak van bulkdata zien voor reconstructie van belangrijke gebeurtenissen.

4.2.3 De Wiv 2017 en bulkdata

In de praktijk kan bulkdata worden verworven met zowel algemene als bijzondere bevoegdheden. Zo worden passagiersgegevens[95] verkregen via de algemene informantenbevoegdheid en worden andere bulkdatasets weer verworven via de hackbevoegdheid (artikel 45). Bij de totstandkoming van de Wiv 2017 is er met name veel maatschappelijke aandacht geweest voor de nieuwe bijzondere bevoegdheid tot OOG-interceptie op de kabel. Met die bevoegdheid wordt bulkdata verworven.[96] In de Wiv 2017 is ervoor gekozen om deze bevoegdheid te koppelen aan de hoogste waarborgen, te weten toestemming van de minister met rechtmatigheidstoets door de TIB voor zowel verwerving (artikel 48 en 49, lid 1) als verwerking (artikel 49, lid 2, en 50). Die hoge waarborgen worden op zijn plaats geacht, gelet op de inbreuk op de rechten van betrokkenen door de verwerving. Maar voor bulkdatasets die met andere bevoegdheden worden verworven, gelden weer andere ('lagere') waarborgen voor de verwerving en de verwerking.

Opvallend is dat in de systematiek van de Wiv 2017 de waarborgen dus niet volgen uit de aard en omvang van de gegevens, maar afhangen van de bevoegdheid waarmee die gegevens worden verworven. Dit leidt tot inconsistentie omdat vergelijkbare gegevens via verschillende bevoegdheden kunnen worden verworven. De Evaluatiecommissie ziet hierin een ernstig gebrek aan voorzienbaarheid en uniformiteit.

---

[94] CTIVD. (2020). *Toezichtsrapport 71 over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD*. p. 18.

[95] *Advance Passenger Information (API)*, zie ook: CTIVD. (2020). *Toezichtsrapport 71 over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD*.

[96] Ook met de bevoegdheid tot OOG-interceptie van niet-kabelgebonden communicatie zoals satellietverkeer wordt bulkdata verworven. Dit was al mogelijk onder de Wiv 2002. Dat geldt ook voor hacken.

4.2.4 Bulkdata in de praktijk

Er bestaan in de praktijk diverse soorten bulkdata. Per bulkdataset, of zelfs binnen een bulkdataset, kan de aard van de gegevens die daarin zitten verschillen. Het kan gaan om identificerende gegevens zoals telefoonnummers, of om gedragsgegevens die meer onthullen over iemands privéleven zoals met wie, waar en op welk moment dit telefoonnummer in contact heeft gestaan. Grofweg kan binnen bulkdata een onderscheid worden gemaakt tussen *register*-bulkdata en *gedrag*-bulkdata.[97] Dit onderscheid is conceptueel verhelderend en praktisch nuttig, onder meer bij de relevantiebeoordeling van bulkdata (zie §4.4.5). Dit onderscheid sluit bovendien aan op de in §3.3 geschetste ontwikkelingen in jurisprudentie waarbij gekeken wordt naar de aard van een persoonsgegeven en de mate waarin dit gegeven inzicht verschaft in iemands privéleven, ofwel identificerende gegevens en gegevens die inzicht geven in gedragingen.

Register-bulkdata

Onder register-bulkdata wordt bulkdata verstaan die bestaat uit identificerende kenmerken. Het gaat hierbij om feitelijke, relatief stabiele kenmerken die beschrijven wie of wat je bent. Denk hierbij bijvoorbeeld aan postcodes, geboortedata en paspoortnummers. Deze kenmerken worden ook wel 'attributen' genoemd.

Andere voorbeelden van *register*-bulkdata zijn een verzameling van e-mailadressen, een bulkregister van een telecommunicatie-aanbieder met abonneegegevens of basisregistraties van de overheid zoals het Handelsregister van de Kamer van Koophandel (KvK) of het kentekenregister (Basisregistratie Voertuigen).

Gedrag-bulkdata

Onder gedrag-bulkdata wordt bulkdata verstaan die niet enkel uit identificerende *kenmerken* maar óók uit gedragsgegevens bestaat. Met gedragsgegevens wordt gedoeld op meer tijdsgebonden informatie over gebeurtenissen die inzicht geven in bijvoorbeeld gedragingen van personen: niet wat je *bent*, maar wat je *doet*.

Gedacht kan worden aan passagiersgegevens waaruit blijkt waar iemand op welke tijd heen vliegt[98] of telefonieverkeersgegevens waaruit onder meer kan worden opgemaakt wie met wie heeft gebeld.

De diensten maken gebruik van zowel register- als gedrag-bulkdata. Omdat er veel verschillende soorten bulkdatasets zijn, kunnen bulkdata op veel verschillende manieren behulpzaam zijn bij de taakuitoefening van de diensten. Met name uit de combinatie van verschillende bulkdatasets kan waardevolle informatie voortkomen. De voorbeelden uit §4.2.2 laten de meerwaarde en ook de noodzakelijkheid zien van gedrag-bulkdata met locatiegegevens en communicatiegegevens.

---

[97] Het zuiverst zou zijn om te spreken van 'register-bulkdata' en 'niet-registerbulkdata'. Voorstelbaar is immers dat gegevens niet vallen onder de definitie van register-bulkdata, maar ook niet precies vallen onder de definitie van gedrag-bulkdata. In dit rapport wordt voor de leesbaarheid en inzichtelijkheid toch steeds gesproken van enerzijds register-bulkdata en anderzijds gedrag-bulkdata.

[98] Zie ook: CTIVD. (2020). *Toezichtsrapport 71 over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD.*

Vanuit het subsidiariteitsprincipe geldt dat gegevens met de minst ingrijpende bevoegdheid moeten worden verworven. Soms zijn die lichtere middelen niet beschikbaar of is de inzet ervan niet mogelijk. In de praktijk hebben de diensten in het buitenland minder beschikking over lichtere middelen. Voor gedrag-bulkdata geldt dan ook dat deze in beginsel niet in Nederland en specifiek over Nederlandse burgers en ingezetenen wordt verworven als er ook een lichter middel bestaat om de benodigde gegevens te verzamelen.

Daarnaast maken de diensten ook gebruik van register-bulkdata. Dit zijn bijvoorbeeld overheidsregisters zoals het register van de KvK, het kentekenregister van de RDW en de Basisregistratie Personen (BRP) (zie §4.3.1). De diensten hebben deze register-bulkdata van andere overheidsorganen nodig om het beeld van personen in onderzoek zo volledig mogelijk te maken. Naast deze Nederlandse register-bulkdata bestaan er ook buitenlandse register-bulkdatasets. Denk daarbij aan een digitaal telefoonboek van een stad in een ander land. Hierbij kan van tevoren nooit worden gezegd welke gegevens van personen of organisaties uit de bulkdata wel en welke gegevens niet zullen worden gebruikt; van een telefoonboek kan vooraf ook niet worden aangeven of slechts de telefoonnummers van personen met de beginletters A t/m H van de achternaam gebruikt zullen worden.

Hierdoor ontstaat in de praktijk een dilemma. Hoe kan enerzijds de operationele waarde van een bulkdataset behouden blijven en anderzijds de inbreuk op de privacy van die vele personen die niet in onderzoek zijn worden geminimaliseerd? Hier wordt in §4.3.3 verder op ingegaan.

Europese jurisprudentie over bulkinterceptie

In §3.4 kwamen de uitspraken van het EHRM en het HvJEU die gerelateerd zijn aan bulkinterceptie reeds ter sprake. Het gaat bij het EHRM om de *Big Brother Watch* zaak en bij het HvJEU om de zaken *Quadrature du Net/Ordre des barreaux francophones et germanophone* en *Privacy International*. De relevantie, de gevolgen voor deze zaken op bulkinterceptie en de conclusie worden hieronder per zaak beschreven. Kortgezegd is de conclusie dat het in dit hoofdstuk geschetste systeem kan voldoen aan de eisen die het EHRM stelt en dat de uitspraken van het HvJEU alleen van toepassing zijn bij de uitleg van EU-recht, dat bij de Wiv 2017 niet rechtstreeks van toepassing is.

Het EHRM

Big Brother Watch[99]

Het ging in deze zaak, die een uitvloeisel was van de onthullingen van Snowden, om de toegang die een onderdeel van de Britse inlichtingendienst (GCHQ) had tot de onderzeese glasvezelkabels waarover grote hoeveelheden internetcommunicatiegegevens werden getransporteerd (in het arrest aangeduid als '*bulk interceptions of communications*'). De wettelijke basis daarvoor was de *Regulation of Investigatory Powers Act* (RIPA). Dit alles vond plaats in het kader van een samenwerking met de Amerikaanse inlichtingendiensten. RIPA voorzag in regels voor de interceptie in verband met zware criminaliteit en nationale veiligheid. Een speciaal probleem bij de toepassing van deze regels was of het om commu-

[99] EHRM 13 september 2018, (*Big Brother Watch*).

nicatie ging die moesten worden beschouwd als intern of extern ten opzichte van het Verenigd Koninkrijk. De klacht bij de nationale instanties werd onder meer aanhangig gemaakt door journalisten die stelden dat deze vorm van interceptie hun bronbescherming srecht in gevaar zou kunnen brengen. In nationale instantie werd op de klachten beslist door het *Investigatory Powers Tribunal* (IPT).

In zijn beslissing over de vraag of de RIPA een wettelijke regeling is die voldoet aan de eisen die artikel 8 EVRM stelt, recapituleert en benadrukt het EHRM de zes waarborgeisen die het voor strafrechtelijk onderzoek en vorming van (persoons)gegevensbestanden heeft ontwikkeld: 1) de aard van de verdenkingen, 2) categorieën van personen die mogen worden 'gevolgd', 3) de tijdsduur dat ze mogen worden gevolgd, 4) regels voor opslag, toegang en onderzoek van verzamelde gegevens, 5) de transparantie van de regels en 6) regels omtrent de duur van de opslag. De eerste twee zien specifiek op het strafrecht dat op zoek is naar potentiële daders en zijn daardoor niet zonder meer van toepassing.

In overweging 314 erkent het EHRM nadrukkelijk dat bulkinterceptie een geoorloofd middel kan zijn, waarbij het een update geeft van zijn oudere beslissingen:

> *"Although (...) these cases are now more than ten years old, given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime), advancements in technology which have made it easier for terrorists and criminals to evade detection on the Internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation."*[100]

Daar voegt het in overweging 316 aan toe:

> *"However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasized this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications."*[101]

Conclusie EHRM

Het Britse wettelijke systeem voldeed volgens het Hof niet geheel aan de zes waarborgcriteria die het had ontwikkeld en in aangepaste vorm op bulkdataverzamelingen heeft toegepast. Dit ziet op de specifieke Britse situatie. Het systeem van waarborgen dat in dit hoofdstuk wordt voorgesteld, spoort met de zes basisbeginselen die het Hof heeft geformuleerd. De beperking van het doel komt tot uitdrukking in een nieuwe procedure om de bulkbehoefte vast te stellen, en de noodzaak een onderscheid te maken tussen register- en

[100] EHRM 13 september 2018, *(Big Brother Watch)*, r.o. 314.
[101] EHRM 13 september 2018, *(Big Brother Watch)*, r.o. 316.

gedrag-bulkdata. De andere eisen vinden hun vertaling in de hier beschreven onderzoeksprocedure en voorschriften voor de toegang tot en het bewaren van bulkdata.

De *Big Brother Watch* zaak is thans nog aanhangig bij de *Grand Chamber* van het EHRM, die naar verwachting binnen afzienbare termijn uitspraak zal doen. Het is de verwachting van de Evaluatiecommissie dat die uitspraak in lijn zal zijn met het hier verdedigde standpunt.

Het HvJEU

Ook de EU-rechter heeft zich recentelijk over het verzamelen en onderzoeken van bulkdata uitgelaten. Het gaat om de in §3.4.2 besproken zaken *Quadrature du Net e.a./Ordre des barreaux francophones et germanophone e.a. en Privacy International.* Deze zaken gingen over de reikwijdte van de EU-privacy en elektronische communicatierichtlijn (2002/58/EG) ten opzichte van de nationale veiligheid van de lidstaten. Het draait om artikel 15 van de richtlijn dat toelaat dat de aard van de retentierechten en verplichtingen die de telecommunicatieondernemingen onder de artikelen 5, 6, 8 en 9 hebben in het belang van de nationale veiligheid aangepast kunnen worden, mits dat noodzakelijk is en de maatregelen aan de eisen van proportionaliteit voldoen. In beide gevallen ging het om nationale wetgeving (Britse, Belgische en Franse) met betrekking tot inlichtingen- en veiligheidsdiensten die vergaande retentieverplichtingen aan de telecommunicatieondernemingen konden opleggen zodat diensten toegang konden krijgen tot door de providers aan te houden bulkbestanden. Een beroep op de bescherming van de nationale veiligheid geeft, volgens het Hof, lidstaten geen vrijbrief om Europese wet- en regelgeving buiten beschouwing te laten:

> *"the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law"*[102]

Het Hof overweegt echter ook:

> *"where the Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is not covered by Directive 2002/58, but by national law only, with the result that the measures in question must comply with, inter alia, national constitutional law and the requirements of the ECHR."*[103]

Het Hof van Justitie benadrukt in deze uitspraken dat de activiteiten zoals retentie van bulkgegevens door telecomaanbieders in opdracht van de inlichtingen- en veiligheidsdiensten binnen het bereik van de Europese privacy- en elektronische communicatierichtlijn[104] vallen. Dit betekent dat bij een eventuele verplichting tot medewerking de

[102] HvJEU 6 oktober 2020, (*Privacy International*), r.o. 44; HvJEU 6 oktober 2020, (*Quadrature du Net and others)*, r.o. 99.
[103] HvJEU 6 oktober 2020, (*Privacy International*), r.o. 48.
[104] Richtlijn (EU) 2002/58.

toestemming hiertoe getoetst moet zijn door een onafhankelijk orgaan of rechterlijke instantie. Deze toets moet bindend zijn. Er moet sprake zijn een tijdgebondenheid ten aanzien van de uitvoering én getoetst moet worden op het bestaan van de dreiging en de noodzakelijkheid van de inzet.

De eisen die het Hof stelt, vertonen gelijkenis met de '*six minimum requirements*' van het EHRM. Het Hof acht het inzetten van deze bevoegdheid wel gerechtvaardigd, maar stelt daaraan, anders dan het EHRM in de hierboven geanalyseerde beslissing, de eis dat er sprake moet zijn van een onmiddellijke en dadelijke terroristische dreiging.

Conclusie HvJEU
De eisen die het Hof stelt aan de door diensten aan telecommunicatieondernemingen opgelegde verplichtingen gaan verder dan de eisen die de Wiv voor de diensten kent. Deze rechtspraak ziet echter op uitleg van de EU-richtlijnen, en is, zoals het Hof uitdrukkelijk vaststelt, niet van toepassing op wetgeving als de Wiv. De Nederlandse diensten verzamelen, bewerken en bewaren zelf de bulkbestanden. Dat de diensten bepaalde verrichtingen uitvoeren met medeweten en medewerking van providers (zoals bijvoorbeeld het inrichten van een accesslocatie ten behoeve van kabelinterceptie art. 53) is geen verwerking in de zin van de EU-privacy regelgeving, ook niet onder artikel 23 van de AVG. Het gaat hierbij niet om een *activiteit* van de telecomaanbieder, maar van de diensten zelf. De uitleg van de Wiv is niet een vraag van gemeenschapsrecht die aan het HvJEU kan worden voorgelegd, zodat een toetsing aan het EVRM en de zes basisbeginselen die het EHRM heeft ontwikkeld meer voor de hand ligt. In dit hoofdstuk van het Evaluatierapport zijn voor het verwerken van bulkbestanden proportionaliteitsregels neergelegd die beogen aan die criteria te voldoen. In hoofdstuk 9 over toezicht is hetzelfde nagestreefd.

4.3 Verwerving van bulkdata

4.3.1 Voorzienbaarheid verwerving bulkdata

De Wiv 2017 spreekt niet over bulkverwerving. De wet geeft de diensten de mogelijkheid om gegevens te verwerven, ongeacht of het gaat om bulkdata of niet. Dat maakt dat niet voor iedereen duidelijk is dat de diensten bulkdata mogen verwerven. De gevoeligheid van bulkverwerving vereist een explicitering.

Het gebrek aan voorzienbaarheid geldt met name voor het verwerven van bulkdata via een informant (artikel 39). Met deze bevoegdheid mogen de diensten zich wenden tot "bestuursorganen, ambtenaren en voorts eenieder die geacht wordt de benodigde gegevens te kunnen verstrekken" (artikel 39, lid 1). In de praktijk worden op basis van deze informantenbevoegdheid door de Koninklijke Marechaussee (KMar) passagiersgegevens aan de AIVD verstrekt. Deze bulkdata wordt daarbij structureel als geautomatiseerd bestand aan de AIVD gegeven en de AIVD slaat deze bulkdata op.[105] Op basis van de taakstelling van de diensten is het goed uitlegbaar dat de diensten deze bulkdata van andere Nederlandse medeoverheden gebruiken. Voor de

[105] Zie ook: CTIVD. (2020). *Toezichtsrapport 71 over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD.*

passagiersgegevens is dit ook rechtmatig bevonden door de CTIVD.[106] Deze mogelijkheid volgt alleen niet duidelijk uit artikel 39 of de toelichting hierop.[107]

Daarnaast is de informantenbevoegdheid niet de enige manier waarop de diensten aan bulkdata van Nederlandse medeoverheden kunnen komen. Artikel 94 verplicht de KMar, de politie en de Belastingdienst om desgevraagd gegevens te verstrekken. Toch wordt de verstrekking aan de diensten vaak gedaan op basis van artikel 39. Dit heeft te maken met de mogelijkheid om bij de informantenbevoegdheid (artikel 39) de gevraagde gegevens als geautomatiseerd bestand te ontvangen. Artikel 94 kent deze mogelijkheid niet. Overigens is medewerking bij de informantenbevoegdheid dan weer vrijwillig, terwijl verstrekking onder artikel 94 verplicht is.[108]

Een eenduidige en voorzienbare grondslag voor het verwerven van bulkdata van Nederlandse medeoverheden ontbreekt nu. De Evaluatiecommissie vindt dat die er wel zou moeten zijn en doet daartoe in §4.3.4 een aanbeveling.

4.3.2 Uniformiteit bij verwerving bulkdata

Dat bulkverwerving niet voorkomt in de bepalingen in de Wiv 2017 heeft niet alleen effect op de voorzienbaarheid, maar ook op de uniformiteit van waarborgen bij deze verwerving. Als bulkdata wordt verworven via OOG-interceptie of de hackbevoegdheid, dan moet de betrokken minister daarvoor toestemming geven, met de toets door de TIB op de rechtmatigheid van die toestemming. Maar als bulkdata op andere wijze wordt verworven dan geldt deze waarborg niet.

Dat verschil is wel te verklaren als er alleen wordt gekeken naar de verstrekkendheid van de bevoegdheid. Het vragen van gegevens op basis van vrijwilligheid aan personen/organisaties (informantenbevoegdheid) is minder ingrijpend dan het ongezien inbreken in de systemen van personen of organisaties. Maar het verschil is niet goed te verklaren als wordt gekeken naar de *aard en omvang* van de gegevens. In beide gevallen wordt bulkdata verworven, wat betekent dat er inbreuk wordt gemaakt op de privacy van mensen die niet het onderwerp van onderzoek van de diensten zijn of zullen worden. De Evaluatiecommissie vindt een aanvullende waarborg hier nodig en zal daarop in §4.3.4 terugkomen.

4.3.3 Het gerichtheidsvereiste en bulkverwerving

Bij de inzet van bevoegdheden – ook voor het verwerven van bulkdatasets – moeten de diensten voldoen aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit (artikel 26) en het gerichtheidsvereiste.[109] Deze vereisten worden door de TIB betrokken in haar rechtmatigheidstoets.

De vraag is hoe in dat licht het gerichtheidsvereiste bij bulkverwerving moet worden ingevuld. De toelichting op het in de Eerste Kamer aanhangige wijzigingsvoorstel van de Wiv 2017 vult het gerichtheidsvereiste als volgt in: “De diensten doen wat redelijkerwijze in hun vermogen ligt om reeds bij verwerving van gegevens de niet voor het onderzoek noodzakelijke gegevens

[106] De CTIVD noemt in toezichtsrapport nr. 71 dat passagiersgegevens bijvoorbeeld kunnen worden gebruikt om historische vliegbewegingen in kaart te brengen of ter raadpleging na een melding dat iemand een mogelijke jihadist is (p. 18).

[107] In de MvT wordt bij de informantenbevoegdheid bijvoorbeeld alleen gesproken over de CT Infobox en de toegang in dat kader tot daarvoor in aanmerking komende gegevens bij de aangesloten partners. Zie: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 56-59 (MvT Wiv 2017).

[108] Zie hierover het toetsingskader bijlage I bij het CTIVD-rapport nr. 71: CTIVD. (2020). *Toezichtsrapport 71 over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD.*

[109] Het gerichtheidsvereiste vloeit voort uit motie-Recourt *Kamerstukken II* 2016/17, 34 588, nr. 66.

tot een minimum te beperken en motiveren dit in hun aanvraag tot de inzet van een bevoegdheid."[110] Dit gebeurt door de gegevens zoveel mogelijk af te bakenen; geografisch, naar tijdstip, naar soort data/type verkeer, naar object/*target* of naar gedraging.[111] Hierbij moet volgens de regering rekening worden gehouden met zaken zoals de inlichtingencontext van het zoeken naar ongekende dreiging en de reële technische mogelijkheden.[112] In de toelichting op het wijzigingsvoorstel wordt niet gesproken over de specifieke invulling van het gerichtheidsvereiste bij bulkverwerving.

Bij bulkverwerving is de doelbinding in het algemeen minder eenduidig omdat soms pas bij de verwerking specifieke gebruiksdoelen kunnen worden vastgesteld (zie §3.3.3). Bij inlichtingenonderzoek is van tevoren niet altijd bekend welke personen en/of organisaties en dus welke specifieke gegevens uit bulkdata precies van belang zullen zijn. De Evaluatiecommissie constateert dat daarom vaak juist de *volledigheid* met betrekking tot de personen/organisaties van een bulkdataset van groot belang is bij verwerving. Het eisen van een (te) scherpe afbakening veronderstelt volgens de Evaluatiecommissie dat de verwerving gericht is op *gekende* dreiging met *gekende targets*. Bulkverwerving is echter juist (vaak) gericht op het verkrijgen van een informatiepositie bij een dreiging waarvan de *targets* nog niet of maar deels bekend zijn (*target discovery*).

Toch moeten de diensten ook bulkdata volgens de wet zo gericht mogelijk verwerven. De toelichting bevat, ook in de hangende wetswijziging, te weinig aanknopingspunten voor een adequate toepassing van dit criterium bij bulkverwerving. Uit CTIVD-rapporten maakt de Evaluatiecommissie op dat gerichtheid bij bulkverwerving op verschillende manieren kan worden beoordeeld en sterk afhangt van het gebruikte middel. Zo schrijft de CTIVD dat bij OOG-interceptie een groot gedeelte van de gerichtheid al gelegen is in het feit dat bij er bij de technische inzet heel veel gegevens *niet* worden geïntercepteerd.[113] Allereerst wordt er gekozen voor een bepaalde 'communicatiedrager' zoals een kabel of satelliet. Bij kabel wordt dan een specifieke *fiber* uitgekozen en binnen die *fiber* weer specifieke communicatiestromen. Bij etherverkeer worden specifieke frequenties gekozen en daarbinnen de communicatiestromen die van belang zijn. Vervolgens wordt gefilterd door bepaalde (gedrags)gegevens wél of juist niet door te laten (positieve en negatieve filtering). Bij inzet van de hackbevoegdheid wordt de gerichtheid weer anders ingericht. Hierbij is het niet de keuze voor een bepaalde *fiber* maar de keuze voor een bepaald geautomatiseerd werk en daarbinnen de keuze voor een bepaalde gegevensverzameling. Het is nodig dat de toelichting op de wet meer ingaat op de verschillende manieren waarop het gerichtheidsvereiste bij bulkverwerking moet worden ingevuld. In de volgende paragraaf worden hiervoor aanbevelingen gedaan.

[110] *Kamerstukken* II 2018/19, 35 242, nr. 3, p. 5 (MvT wijziging Wiv 2017).
[111] Ibidem.
[112] Ibidem.
[113] CTIVD. (2019). *Toezichtsrapport 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD.*

4.3.4 Aanbevelingen bulkverwerving

4.3.4.1 Voorzienbaarheid: introductie bulkparagraaf in de wet

De Evaluatiecommissie vindt dat in de wet een aparte paragraaf over bulkdata moet worden opgenomen. In de toelichting op deze paragraaf moet duidelijkheid worden geboden over de verschillende reeds bestaande bevoegdheden die de diensten kunnen inzetten om bulk te verwerven.[114] Hiermee wordt de voorzienbaarheid voor het publiek vergroot. Het verdient bovendien de aanbeveling in de toelichting op deze bulkparagraaf – voor zover mogelijk in het openbare domein – in te gaan op het operationele belang en de noodzakelijkheid van bulkdata voor de diensten alsook de bijbehorende maatregelen.[115]

> **Aanbeveling 1**
>
> Neem in de wet een bulkparagraaf op.

Ten behoeve van de voorzienbaarheid beveelt de Evaluatiecommissie daarnaast aan om één expliciete en eenduidige grondslag te hanteren voor het verkrijgen van bulkdata van Nederlandse medeoverheden. Dit gebeurt nu aan de hand van zowel artikel 39 als 94. De onduidelijke verhouding en overlap tussen deze twee artikelen moet worden weggenomen.

> **Aanbeveling 2**
>
> Kom tot één grondslag voor het verkrijgen van gegevens (inclusief bulkdata) van Nederlandse medeoverheden.

4.3.4.2 Uniformiteit: introductie aantonen bulkbehoefte

Naast meer voorzienbaarheid moet er ook meer uniformiteit worden aangebracht bij bulkverwerving. De Evaluatiecommissie begrijpt dat de waarborgen voor de verschillende manieren van bulkverwerving zijn afgestemd op de vraag hoe ingrijpend de bevoegdheid is waarmee de bulkdata wordt verworven. Tegelijkertijd is een extra waarborg op zijn plaats voor alle gevallen waarin de diensten willen overgaan tot het verwerven van bulkdata, onafhankelijk van welke bevoegdheid wordt gebruikt.

De toestemmingsprocedure voor bulkverwerving dient te worden uitgebreid met een extra stap voorafgaand aan de toestemmingsaanvraag voor de inzet van een bevoegdheid. In deze extra stap gaat het om het aantonen van de bulkbehoefte. Daarbij motiveert de dienst de noodzakelijkheid van bulkverwerving voor de inlichtingenbehoefte: Is bulkdata noodzakelijk voor een of meer onderzoeksopdrachten? Hierbij moet ook worden aangegeven om wat voor soort bulkdata

---

[114] Oratie J.J. Oerlemans. Zie: Oerlemans, J.J. (November 2020). *Grenzen stellen aan de datahonger*. Beschikbaar via **https://www.uu.nl/sites/default/files/UU%20oratietekst%20Jan-Jaap%20Oerlemans%2016%2011%202020.pdf**.

[115] In dit kader verwijst de Evaluatiecommissie ook graag naar het rapport van dhr. D. Anderson over de *Investigatory Powers Bill* van het Verenigd Koninkrijk en in het bijzonder Annex 8 t/m 11 waarin tientallen Britse *case studies* worden besproken. Hierin wordt expliciet worden gemotiveerd waar bulkdata noodzakelijk is. Zie: Anderson, D. (2016). *Report of the Bulk Powers Review*. Independent Reviewer of Terrorism Legislation.

het gaat, zoals register-bulkdata of gedrag-bulkdata. De bulkbehoefte wordt voorgelegd aan het diensthoofd en vervolgens aan de betrokken minister. Pas als de minister akkoord is met de behoefte, vervolgen de diensten de gebruikelijke procedure voor de daadwerkelijke verwerving. Dit betekent dat als het gaat om een bijzondere bevoegdheid zoals OOG-interceptie of de hack-bevoegdheid, hiervoor aanvullend nog een toestemmingsverzoek aan de betrokken minister wordt voorgelegd en deze toestemming wordt getoetst door de TIB (zie §2.2).

Met de introductie van het aantonen van de bulkbehoefte wordt niet de *bevoegdheid tot verwerving* centraal gesteld, maar wordt recht gedaan aan de *aard van de beoogde gegevens*. Hierdoor wordt de noodzaak tot verwerving van een bulkdataset losgekoppeld van het technische middel waarmee dit wordt verworven. Dit is een operationele beslissing die door de betrokken minister wordt genomen. Het gaat dus niet om een toestemming voor de inzet van een bijzondere bevoegdheid die door de TIB op rechtmatigheid wordt getoetst.

De Evaluatiecommissie streeft met de introductie van de bulkbehoefte naar meer uniformiteit in de bulkverwerving door niet de verwervende bevoegdheid maar de aard van de beoogde data centraal te stellen. Met deze extra stap wordt gedeeltelijk tegemoetgekomen aan de (verworpen) motie van het Kamerlid Buitenweg (GroenLinks).[116] In deze motie werd voorgesteld het toestemmingsniveau voor het verzamelen van bulkdata via de informantenbevoegdheid op ministerieel niveau te beleggen. Met de introductie van de bulkbehoefte krijgt de minister bij bulkverwerving altijd een rol: niet alleen wanneer dit via de inzet van bijzondere bevoegdheden gebeurt (dat was al zo), maar ook bij bulkverwerving via algemene bevoegdheden zoals de informanten-bevoegdheid. Tegelijkertijd blijft – ná toestemming van de minister op de bulkbehoefte – de huidige toestemmingsprocedure voor bevoegdheden (dus ook voor de informantenbevoegdheid) gelijk. De introductie van de bulkbehoefte leidt tot een betere motivering van de noodzakelijkheid van bulkverwerving. Daarmee kan de TIB die ook beter betrekken bij het toetsen van de inzet van de bijzondere bevoegdheid.

Voor bulkdata die door buitenlandse diensten aan de Nederlandse diensten wordt verstrekt, geldt ook dat de bulkbehoefte eerst moet worden aangetoond. Wanneer een verstrekking van een buitenlandse dienst, maar bijvoorbeeld ook van een informant, niet voorzien was door de diensten, geldt dat *achteraf* alsnog de bulkbehoefte moet worden aangetoond. Pas ná toestemming van de minister kan de desbetreffende bulkdata worden gebruikt voor het inlichtingenproces (zie §8.6).

Dit betekent een meer uniforme benadering van bulkverwerving. Ook dwingt deze nieuwe stap tot een explicietere afweging van de noodzaak tot bulkverwerving door het aantonen van de bulkbehoefte, in plaats van de weging direct te richten op de noodzakelijkheid, proportionaliteit, subsidiariteit en gerichtheid van de inzet van een technisch middel. Dit leidt tot een verhoging van de waarborgen op de verwerving van bulk.

Aanbeveling 3

Voeg een stap aan het toestemmingsproces toe waarbij de bulkbehoefte voorafgaand aan het inzetverzoek ter toestemming wordt voorgelegd aan de minister.

[116] *Kamerstukken II* 2019/20, 35 242, nr. 8

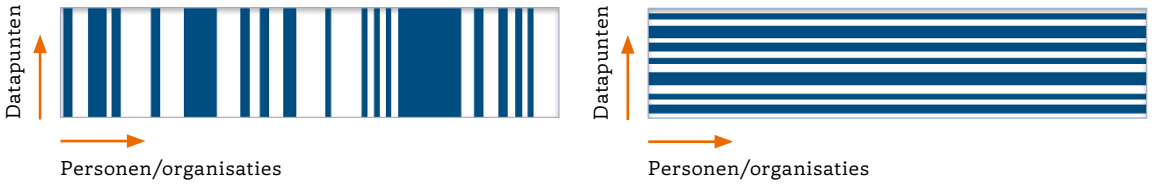
4.3.4.3 Op bulk toegespitste invulling gerichtheid

Het is bij bulkverwerving niet altijd haalbaar om de te verwerven gegevens (voldoende) van tevoren toe te spitsen op bepaalde *targets* of op een bepaalde locatie. Tegelijkertijd is gerichtheid een belangrijke waarborg. De vraag is wat een passende invulling is van het gerichtheidsvereiste bij bulk. Hierbij is het nuttig om onderscheid te maken tussen register-bulkdata en gedrag-bulkdata.

De Evaluatiecommissie beveelt aan de mate van gerichtheid bij bulkverwerving niet alleen te relateren aan het aantal personen en/of organisaties. Gerichtheid bij bulk kan grofweg op twee manieren worden benaderd: door het aantal verschillende personen/organisaties in de bulkdataset te reduceren, of door de hoeveelheid gegevens per persoon/organisatie in de bulkdataset te reduceren ('datapunten'). In de praktijk kunnen deze twee manieren elkaar aanvullen. Het is van belang dat beide manieren in de wet uiteen worden gezet.

Vanwege het belang van volledigheid van bepaalde bulkdatasets, met name register-bulk, beveelt de Evaluatiecommissie aan om daar de gerichtheid vooral in te vullen door de hoeveelheid gegevens per persoon, de datapunten, te reduceren. Dit betekent dat de *volledigheid* van de bulkdata met betrekking op het aantal personen en/of organisaties in stand blijft, maar dat de *omvang* van de bulkdataset wordt verkleind. Denk voor register-bulk bijvoorbeeld aan de RDW waarin informatie over de milieuprestaties van een voertuig wellicht niet worden bewaard, maar de koppeling van voertuig en eigenaar wel. Bij gedrag-bulkdata kunnen beide manieren van reductie worden gebruikt, eventueel in combinatie. Zo kan bij verwerving van gedrag-bulkdata worden gereduceerd door alleen gegevens van een bepaald gebied binnen te halen (reductie van aantal personen/organisaties). Ook kan gedrag-bulkdata worden gereduceerd door datapunten zoals het type telefoonabonnement dat iemand heeft niet mee te nemen. Omdat gedrag-bulkdata per definitie minder eenvormig van aard is, zal bij de beoordeling van de gerichtheid meer maatwerk moeten worden toegepast.

Onderscheid tussen reductie op personen/organisaties en reductie op datapunten



Hierbij is van belang dat de datapunten niet altijd op voorhand kunnen worden geïdentificeerd. Soms is het bovendien technisch niet mogelijk om bij verwerving bepaalde datapunten van andere datapunten te scheiden. Het is dus voorstelbaar dat de diensten breder verwerven en vervolgens bepaalde datapunten bewaren en de rest vernietigen. Dit is overeenkomstig het '*select while you collect*' principe.[117] De keuze welke datapunten relevant zijn is dynamisch. Dit hangt niet alleen af van de bulkdataset en het onderzoek waarvoor deze wordt verworven, maar bijvoorbeeld ook van de fase waarin dit onderzoek zich bevindt. Nieuwe inzichten die gedurende het onderzoek worden opgedaan kunnen leiden tot een andere keuze voor datapunten. Datapunten die niet langer waardevol zijn voor het onderzoek worden dan niet langer verworven. De Evaluatiecommissie ziet dat het daarom moeilijk kan zijn om de keuze voor

[117] Jacobs, B. (2016). Select while you collect – Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten. *Nederlands Juristenblad*, 4, p. 256-261.

bepaalde datapunten van tevoren vast te leggen. Hier is in de ogen van de Evaluatiecommissie een belangrijke rol weggelegd voor het dynamisch toezicht van de CTIVD (zie §9.3).

De invulling van het gerichtheidsvereiste aan de hand van het onderscheid tussen aantallen personen en/of organisaties enerzijds en aantal datapunten anderzijds kan onder het huidige wettelijk kader al worden gehanteerd. In de toelichting op de nieuw te introduceren bulk-paragraaf moet deze interpretatie van het gerichtheidsvereiste voor bulkverwerving worden uitgewerkt en geïllustreerd. Daarnaast moet deze invulling van het gerichtheidsvereiste ook bij de toelichting op artikel 26 worden opgenomen.

Aanbeveling 4

Neem in de wet op dat het gerichtheidscriterium bij de verwerving van bulkdata kan worden ingevuld aan de hand van zowel het terugbrengen van aantallen personen en/of organisaties als het terugbrengen van het aantal te verwerven datapunten.

4.4 Verwerking bulkdata

4.4.1 Uniformiteit bij verwerking

De Wiv 2017 kent alleen bepalingen met betrekking tot bulkdata in het kader van OOG-interceptie. Deze bepalingen zijn opgenomen in navolging van aanbevelingen van de commissie Dessens. Daarmee zijn ook nieuwe waarborgen geïntroduceerd.[118] Deze waarborgen zien niet alleen op de verwerving maar ook op de daaropvolgende *verwerking* van de geïntercepteerde bulkdata. Hiermee gelden er voor de omgang met bulkdata uit OOG-interceptie dus extra waarborgen, in aanvulling op de algemene bepalingen voor gegevensverwerking. Op overige bulkdata (niet verkregen met OOG-interceptie) zijn enkel de algemene bepalingen van verwerking van gegevens van toepassing, waaronder dat de verwerking van gegevens alleen plaatsvindt voor zover deze noodzakelijk is voor een goede taakuitvoering (artikel 18).

Uit de wet volgen drie waarborgen voor de verwerking van bulkdata uit OOG-interceptie:

1. Waarborg op **handeling**: wat mag met bulkdata worden gedaan?
2. Waarborg op **toegang**: wie mag er bij de bulkdata?
3. Waarborg op **tijd**: hoe lang mag bulkdata worden bewaard?

Voor bulkdata verkregen uit andere bevoegdheden dan OOG-interceptie geldt dit 'OOG-verwerkingsregime' met extra waarborgen niet. Dit zorgt voor een gebrek aan uniformiteit en daardoor voor een ongewenst verschil in waarborgen bij de omgang van bulkdata. Ook zorgt het voor onnodige complexiteit in de systemen van de diensten. De Evaluatiecommissie vindt dat dit anders moet. Hiertoe worden in §4.5.5 aanbevelingen gedaan. De waarborgen bij OOG-interceptie worden hierbij als uitgangspunt genomen en verbreed.

[118] *Kamerstukken II* 2014/15, 33 820, nr. 4 (Kabinetsstandpunt advies commissie Dessens).

4.4.2 Bulkdata en huidige handelingswaarborgen

Het eerste type waarborg ziet op handeling: Wat mogen de diensten met bulkdata doen? In het huidige OOG-verwerkingsregime mogen de diensten niet zomaar met bulkdata uit OOG-interceptie aan de slag. Handelingen met betrekking tot deze bulkdata worden in artikel 49 en artikel 50 van waarborgen voorzien.

Artikel 50 regelt het gebruik van bulkdata uit OOG-interceptie voor het inlichtingenonderzoek. In artikel 50, lid 1, wordt de mogelijkheid tot het selecteren[119] van de geïntercepteerde gegevens geregeld. Deze selectie heeft als doel om de inhoud van de gegevens beschikbaar te maken voor het inlichtingenonderzoek. Pas ná selectie aan de hand van bepaalde criteria wordt de inhoud van de gegevens toegankelijk.[120] IP-verkeer wordt zo bijvoorbeeld pas beschikbaar nadat het is geselecteerd aan de hand van bijvoorbeeld een IP-adres. Voor deze selectiebevoegdheid geldt toestemming van de betrokken minister, getoetst door de TIB. Voor metadata uit OOG-interceptie bepaalt artikel 50, lid 2, dat het toepassen van geautomatiseerde data-analyse (GDA) op deze metadata, indien gericht op het identificeren van personen of organisaties, aan toestemming van de betrokken minister en een toets door de TIB onderhevig is. Metadata hoeft dus niet geselecteerd te worden, maar voor GDA-handelingen op OOG-metadata gelden zo wel extra waarborgen. [121]

Artikel 49, lid 1, biedt daarnaast de mogelijkheid aan een beperkte groep daartoe aangewezen functionarissen om de geïntercepteerde bulk te onderzoeken met als doel de interceptie te optimaliseren ('*search* gericht op interceptie').[122] Daarnaast mag op grond van artikel 49, lid 2, de bulkdata worden doorzocht om de reeds beschreven selectie van deze bulk te optimaliseren, door onder meer potentiële selectiecriteria te verifiëren en nieuwe potentiële *targets* te identificeren ('*search* gericht op selectie').[123] Voor deze beide vormen van '*searchen*' is toestemming nodig van de betrokken minister, die wordt getoetst door de TIB.

Bulkdata verkregen via andere bevoegdheden, zoals de hackbevoegdheid, kent deze handelingswaarborgen niet. Voor deze bulkdata gelden alleen de algemene bepalingen voor gegevensverwerking. Zo hoeven gegevens uit deze bulkdata verkregen uit de hackbevoegdheid niet

---

[119] De term 'selecteren' moet in dit rapport worden gelezen als 'selectie' in de context van de Wiv 2017. Dit wijkt dus af van hoe het begrip 'selectie' doorgaans wordt gebruikt wat tot verwarring kan leiden.

[120] Zie voor verdere toelichting: AIVD. *Onderzoeksopdracht gerichte interceptie (OOG)*. Webpagina beschikbaar via **https://www.aivd.nl/onderwerpen/onderzoeksopdrachtgerichte-interceptie-oog**; CTIVD. (2019). *Toezichtsrapport 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD*; CTIVD. (2019). *Toezichtsrapport 64 over de inzet van de bijzondere bevoegdheid tot selectie door de AIVD en de MIVD*.

[121] Zie hoofdstuk 5.

[122] De MvT Wiv 2017 duidt deze search gericht op interceptie bevoegdheid als volgt: 'Deze vorm van search is primair gericht op de optimalisatie van de interceptie, waarbij vooral naar de aard van het verkeer wordt gekeken. Wordt datgene geïntercepteerd wat beoogd wordt? […] Search gericht op interceptie ziet dan ook vooral op de technische kenmerken en de aard van de communicatie, zoals protocollen, frequenties, taal maar ook de kwaliteit van de intercepties.' Zie: *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 104 (Mvt Wiv 2017).

[123] De MvT Wiv 2017 onderscheidt twee situaties bij de inzet van *search op selectie* bevoegdheid: 'Allereerst het vaststellen van en verifiëren van selectiecriteria in relatie tot personen en organisaties die door de diensten worden onderzocht. […] in de opbrengst van de geïntercepteerde telecommunicatie [kan] op zoek worden gegaan naar selectiecriteria die […] voor het onderzoek van de diensten naar die personen of organisatie relevante gegevens kunnen opleveren. […] De tweede situatie […] betreft het in relatie tot lopende onderzoeken van de dienst identificeren van personen of organisaties welke in aanmerking komen voor onderzoek door een dienst. […] In deze situatie wordt aan de hand van gegevens uit lopende onderzoeken, zoals de identiteit van personen of organisaties die reeds in onderzoek staan of andersoortige gegevens (zoals telefoonnummers, IP-adressen, e-mailadressen e.d.), bezien of aan de hand van de opbrengst van de geïntercepteerde telecommunicatie daaraan personen of organisaties zijn te koppelen die mogelijk voor onderzoek door de dienst in aanmerking komen.' Zie: *Kamerstukken II* 2016/17, 34588, nr. 3, p. 106 (MvT Wiv 2017).

eerst via de bijzondere selectiebevoegdheid geselecteerd te worden. Met andere woorden: de handelingswaarborgen zijn gekoppeld aan het middel waarmee bulkdata wordt verworven en niet aan de aard van de gegevens. Dit zorgt ervoor dat bulkdata uit OOG-interceptie met meer waarborgen is omkleed dan bulkdata die via een andere bijzondere bevoegdheid is verworven. Dat vindt de Evaluatiecommissie een onterecht verschil.

Ten slotte wordt ten aanzien van het delen van bulkdata met buitenlandse inlichtingen- en veiligheidsdiensten in de wet niets specifieks geregeld. Dit geldt voor zowel bulkdata verkregen met OOG-interceptie als met andere bevoegdheden. Uiteraard gelden bij het delen van bulkdata de wettelijke regelingen voor internationale samenwerking (zie hoofdstuk 8). Hierbij wordt echter niet specifiek gesproken over het delen van bulkdata. Gezien de aard van de gegevens is dit opvallend. In §4.4.5 zal hier nader op in worden gegaan.

4.4.3 Bulkdata en huidige toegangswaarborgen

De tweede waarborg in het huidige OOG-stelsel bij verwerking van bulkdata verkregen uit OOG-interceptie ziet op toegang: Wie mag er bij de bulkdata? Medewerkers uit het inlichtingenproces die onderzoek doen en die beschikken over een specifieke autorisatie voor deze OOG-gegevens hebben alleen toegang tot de geselecteerde inhoud van gegevens. Niet alle medewerkers hebben die autorisatie; dit hangt ervan af of de OOG-gegevens nodig zijn voor het onderzoek van de medeweker. Voor metadata uit OOG-interceptie geldt dat deze wel rechtstreeks toegankelijk is voor het inlichtingenproces. Zoals gezegd hoeft metadata namelijk niet geselecteerd te worden. Het huidige stelsel kent dus geen aanvullende toegangswaarborgen voor OOG-metadata. Er gelden alleen handelingswaarborgen: het betrekken van metadata bij GDA.

Voor de *search*-bevoegdheden hebben bepaalde medewerkers toegang tot de geïntercepteerde bulkdata (artikel 49, lid 5). Dit geldt alleen voor een beperkte groep functionarissen die daarvoor speciaal wordt aangewezen door de betrokken minister of (indien gemandateerd) hoofd van de dienst. Dit wordt 'functiescheiding' genoemd. Als deze functionarissen bijvoorbeeld een interessant nieuw selectiekenmerk identificeren, dan mogen de resultaten niet zonder meer door het relevante inlichtingenteam worden gezien. Dit kan pas nadat deze resultaten zijn geselecteerd met de inzet van de selectiebevoegdheid.

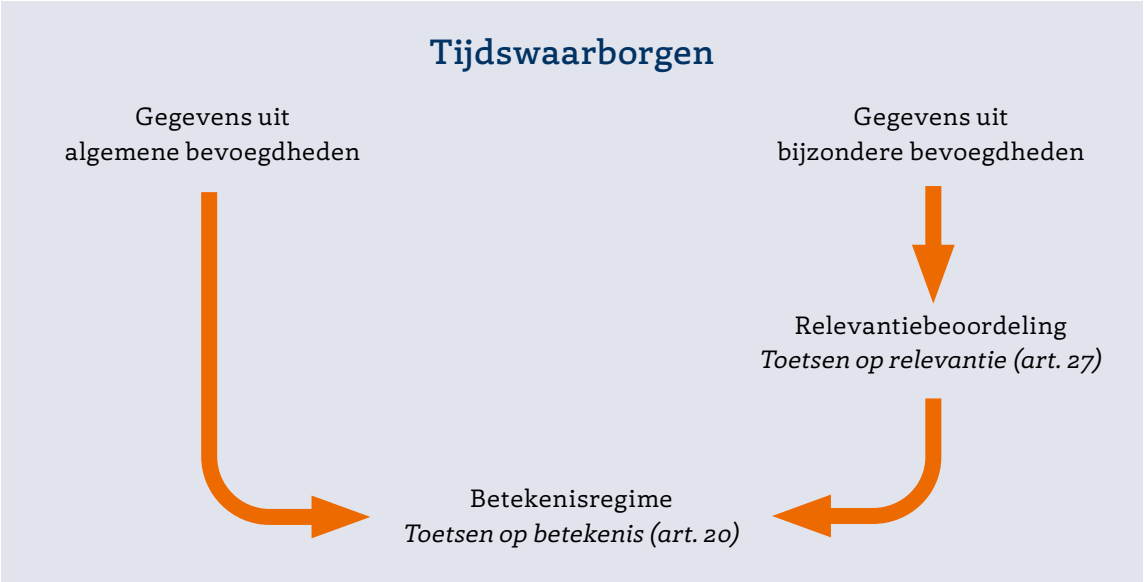
In de praktijk worden voor deze verschillen in toegang de termen 'binnenbak' en 'buitenbak' gebruikt. De buitenbak is de denkbeeldige bak waarin de OOG-data – na filtering – terecht komt. Deze bak is niet toegankelijk voor medewerkers uit het inlichtingenproces, enkel voor technisch beheer en data-analyse (waaronder *searchen*). De binnenbak bevat de gegevens die wél toegankelijk zijn voor het inlichtingenproces, mits de medewerker is geautoriseerd. Voor OOG-data is dit de metadata en de geselecteerde inhoud.

Voor de toegang tot overige bulkdata (verkregen uit andere bevoegdheden) gelden er geen specifieke wettelijk vastgelegde toegangswaarborgen. Dan zijn enkel de minder specifieke algemene bepalingen van toepassing. Ook dit vindt de Evaluatiecommissie een onterecht verschil.

4.4.4 Bulkdata en huidige tijdswaarborgen

Het derde type waarborg in het huidige OOG-verwerkingsregime op bulkdata verkregen uit OOG-interceptie is de waarborg op tijd: Hoe lang mag bulkdata worden bewaard? Met de Wiv 2017 is de verplichting geïntroduceerd om gegevens verkregen uit bijzondere bevoegdheden zo spoedig mogelijk op hun relevantie te beoordelen (artikel 27). Het gaat hierbij om relevantie voor het onderzoek waarvoor de gegevens initieel zijn verworven, óf voor enig ander lopend

onderzoek[124] van de diensten. Deze beoordeling moet binnen één jaar plaatsvinden, met de mogelijkheid deze termijn eenmalig met een half jaar te verlengen (maximaal anderhalf jaar). Gegevens die als niet-relevant worden beoordeeld, moeten worden vernietigd. Gegevens die wél als relevant zijn beoordeeld, komen in het zogenaamde 'betekenisregime'. Dit houdt in dat de gegevens worden verwijderd als deze, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren (art. 20). Hierbij is geen specifieke termijn gesteld waarbinnen de betekenis moet worden getoetst.



De verplichting tot het beoordelen op relevantie geldt voor alle gegevens verkregen via bijzondere bevoegdheden. Daarmee geldt het dus ook voor bulkdata, bijvoorbeeld verkregen via een hack. Voor gegevens (en dus ook bulkdata) verkregen uit OOG-interceptie geldt echter een andere termijn voor deze relevantiebeoordeling (artikel 48, lid 5 en 6). Hiermee wordt een onderscheid geïntroduceerd op basis van techniek, terwijl techniekonafhankelijkheid juist een belangrijk doel van de Wiv 2017 was. Bij gegevens uit etherinterceptie geldt dat de relevantie niet binnen één jaar, maar binnen drie jaar moet worden beoordeeld. Voor gegevens uit kabelinterceptie geldt een termijn van één jaar, die vervolgens twee keer met een jaar kan worden verlengd (in totaal dus ook maximaal drie jaar). De reden voor de langere beoordelingstermijn is uitgebreid beschreven in de toelichting op de Wiv 2017. Het komt er in het kort op neer dat OOG-gegevens van belang zijn voor historisch onderzoek om nog onbekende *targets* en ongekende dreigingen te kunnen onderkennen. Dergelijke onderzoeken vergen tijd.

Waar voor bulkdata uit OOG-interceptie dus een beoordelingstermijn van maximaal drie jaar geldt, en voor bulkdata uit overige bijzondere bevoegdheden een termijn van maximaal anderhalf jaar, bestaat er wettelijk geen verplichting tot het op relevantie beoordelen van gegevens (inclusief bulkdata) uit algemene bevoegdheden. Deze gegevens komen direct in het betekenisregime. Dit geldt nu bijvoorbeeld voor bulkdata verkregen met de informantenbevoegdheid zoals de passagiersgegevens. Opnieuw geldt dat de waarborgen afhankelijk zijn van het middel waarmee bulkdata is verworven. Ook voor de tijdswaarborgen voor bulkdata resulteert dit in

[124] Het gaat hierbij om onderzoek vallend onder de a- en d-taak van de AIVD (artikel 8, lid 2) en onder de a-, c- en e- taak van de MIVD (artikel 10, lid 2).

een gebrek aan uniformiteit en daardoor een onwenselijk en tamelijk willekeurig verschil in waarborgen.

De relevantiebeoordeling van bulkdata uit bijzondere bevoegdheden is onderwerp van discussie geworden tussen de betrokken ministers en de CTIVD. Deze discussie draait in essentie om de vraag op welke wijze deze relevantiebeoordeling dient plaats te vinden. Deze discussie is in de ogen van de Evaluatiecommissie het gevolg van het ontbreken van een definitie in de wet van de term 'relevantie'. De wet geeft een intuïtief kader door het begrip relevantie in verband te brengen met zaken zoals de dreiging[125] en onderzoeksopdrachten.[126] In de wetgeschiedenis wordt gesteld dat het draait om een inhoudelijke toets waarbij gekeken moet worden of gegevens bijdragen aan het onderzoek. Dit kan ook in negatieve zin door bijvoorbeeld hypotheses te ontkrachten.[127] Hoe inhoudelijk deze toets moet plaatsvinden, wordt niet gespecificeerd. De Evaluatiecommissie is van mening dat de wet hiervoor (meer) aanknopingspunten moet bieden.

Relevantiebeoordeling van bulkdata

De CTIVD concludeerde in november 2019 dat het vereiste om bulkdata binnen maximaal anderhalf jaar op relevantie te beoordelen in de praktijk niet goed uitvoerbaar is.[128] De toezichthouder gaf aan dat de AIVD er niet in was geslaagd om de bulkdata tijdig inhoudelijk op relevantie te beoordelen. Naast het (gedeeltelijk) vernietigen van een aantal bulkdatasets, had de AIVD ook een substantieel deel van de bulkdatasets als 'relevant' aangemerkt. Dit achtte de CTIVD onrechtmatig, omdat deze bulkdata voor het overgrote deel betrekking had op organisaties en/of personen die geen onderwerp zijn van onderzoek van de diensten en dat ook nooit zullen worden (dus: bulkdatasets). In haar recente toezichtrapport over bulkhacks specificeerde de CTIVD dit door te stellen dat gegevens die niet gerelateerd zijn aan *targets* van de diensten, niet relevant zijn voor de taakuitvoering.[129]

De toezichthouder benoemde wel dat de bulkdata nog gedeeltelijk noodzakelijk kan zijn voor de taakuitvoering van de diensten en dat integrale vernietiging tot operationele risico's zou kunnen leiden. De wet biedt echter geen ruimte om evident niet-relevante gegevens als relevant aan te merken, aldus de CTIVD. Zodoende resulteerde dit in de aanbeveling om de betreffende bulkdatasets terstond te vernietigen.[130]

[125] "Er is geen sprake van het bewaren van data van personen en organisaties die niet relevant zijn in het kader van de dreiging." *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 7 (MvT Wiv 2017).
[126] "Doorlopende vernietiging van niet-relevant materiaal: Bij het onderzoek van de diensten in fase 2 en 3 van het interceptiestelsel (artikel 49 en 50 van de wet) kan worden vastgesteld dat bepaalde geïntercepteerde gegevens op generlei wijze gerelateerd zijn aan onderzoeksopdrachten. Deze gegevens worden dan vernietigd." *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 111 (MvT Wiv 2017).
[127] *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 32 (Nota naar aanleiding van het Verslag Wiv 2017).
[128] CTIVD. (2019). *CTIVD nr. 66, Voortgangsrapportage III over de invoering van de Wiv 2017*. p. 9-10.
[129] Juridisch kader behorende bij CTIVD toezichtrapport nr. 70, zie: CTIVD. (2020). *Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. p. 19.
[130] Ibidem. p. 24-25.

In reactie op het onrechtmatigheidsoordeel van de CTIVD schreven de betrokken ministers aan de Tweede Kamer: "De CTIVD acht een relevantiebeoordeling van deze bulkdatasets op het door de diensten gekozen abstractieniveau echter onrechtmatig"[131]. Met andere woorden, er heeft een relevantiebeoordeling plaatsgevonden, maar deze heeft de CTIVD onrechtmatig bevonden omdat deze niet gedetailleerd genoeg was, aldus de ministers. Het onrechtmatigheidsoordeel van de CTIVD wordt door de betrokken ministers niet gedeeld.[132] In reactie op de aanbeveling van de CTIVD om de bulkdatasets te vernietigen, geven de ministers aan dat beoordeling op relevantie een open norm is en dat de wijze waarop de diensten hieraan invulling hebben gegeven past binnen het huidige wettelijk kader. De ministers schrijven dan ook aan de Kamer dat zij niet zullen overgaan tot vernietiging van de bulkdatasets, temeer omdat dit als onverantwoord wordt gezien "gelet op het operationele belang van deze sets", zo stellen zij.[133]

Alle partijen verwijzen in deze vastgelopen discussie vervolgens naar de Evaluatiecommissie. Het is niet aan de Evaluatiecommissie om uitspraken te doen over de (on)rechtmatigheid van het als relevant aanmerken van onderhavige concrete bulkdatasets. Wel besteedt de Evaluatiecommissie aandacht aan de vraag wat een zinvolle invulling is van het wettelijke vereiste van relevantiebeoordeling van bulkdata (zie §4.4.5.3).

De discussie over het al dan niet (on)rechtmatig aanmerken van bulkdata als relevant heeft niet alleen gevolgen voor het bewaren van deze gegevens. De relevantiebeoordeling is ook gekoppeld aan het wettelijke onderscheid tussen geëvalueerde en ongeëvalueerde gegevens. De wet gebruikt dit onderscheid in de context van het verstrekken van gegevens aan buitenlandse diensten.[134] Bij het verstrekken van ongeëvalueerde gegevens is 'niet bekend wat de inhoud daarvan is'[135] en geldt zodoende de zwaardere waarborg van ministeriële toestemming (artikel 89, lid 2). De wet geeft echter geen definitie van (on)geëvalueerde gegevens. Uit de wetsgeschiedenis volgt dat een gegeven als 'ongeëvalueerd' moet worden beschouwd als dit gegeven nog niet op relevantie voor de taakuitvoering is beoordeeld.[136] Hiermee wordt de discussie rondom relevantiebeoordeling van bulkdata ook van belang voor het delen van bulkdata. Of deze bulkdata wel of niet op relevantie is beoordeeld, heeft directe invloed op het benodigde toestemmingsniveau voor het delen van deze bulkdata. De CTIVD heeft aangegeven dat deze relevantiebeoordeling wel voldoende specifiek moet zijn, zodat de diensten de risico's van het delen van die gegevens in kunnen schatten.[137] Hierop hebben de betrokken ministers gereageerd dat ook een meer abstracte relevantiebeoordeling resulteert in 'geëvalueerde' gegevens, "zolang er voldoende zicht is op de aard en inhoud van de gegevens in relatie tot een onderzoek van de dienst".[138] In de volgende paragraaf wordt nader ingegaan op deze discussie.

[131] *Kamerstukken II* 2019/20, 34 588, nr. 85, p.2 (Beleidsreactie CTIVD voortgangsrapportage III).
[132] *Kamerstukken II* 2019/20, 34 588, nr. 87, p.2 (Beleidsreactie CTIVD voortgangsrapportage IV).
[133] *Kamerstukken II* 2020/21, 29 924, nr. 203, p.3 (Beleidsreactie CTIVD rapporten nr. 70 en 71).
[134] Wiv 2017, artikel 64, lid 1 en 3, en artikel 89, lid 2.
[135] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 239 (MvT Wiv 2017).
[136] *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 18 (Nota naar aanleiding van het Verslag Wiv 2017).
[137] CTIVD. (2019). *Toezichtsrapport 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD*. p. 11.
[138] *Kamerstukken II* 2020/21, 29 924, nr. 193, p.2-3 (Beleidsreactie CTIVD rapport nr. 65).

4.4.5 Aanbevelingen bulkverwerking

Uit voorgaande paragrafen blijkt dat de Wiv 2017 niet voorziet in een uniform stelsel voor verwerking van bulkdata. De verschillende type waarborgen (handeling, toegang en tijd) zijn gekoppeld aan het *middel* in plaats van aan de *aard* van de gegevens. Onlangs hebben de betrokken ministers aanvullende beleidsregels vastgesteld om de verdere verwerking van bulkdata uit andere bevoegdheden dan OOG-interceptie met meer waarborgen te omkleden. Dit gebeurde naar aanleiding van aanbevelingen van de CTIVD.[139] Deze tijdelijke bulkregeling brengt een aanscherping van de praktijk binnen de kaders van de huidige wet. De ministers hebben bij de aankondiging hiervan aangegeven dat het gaat om tijdelijke maatregelen in afwachting van de resultaten van het onderzoek van de Evaluatiecommissie. In onderstaand kader wordt deze tijdelijke bulkregeling op hoofdlijnen toegelicht. In §9.5.2 wordt nader ingegaan op de grondslag voor deze regeling.

Tijdelijke bulkregeling

De tijdelijke bulkregeling[140] heeft betrekking op de verdere verwerking van alle bulkdata waar de diensten over beschikken, ongeacht met welke bevoegdheid de bulkdata is verkregen. De enige uitzondering hierop is bulkdata uit OOG-interceptie. Daarvoor heeft de wet immers al een apart stelsel opgetuigd.

Voordat een bulkdataset verder wordt verwerkt, wordt deze beoordeeld op de mate waarin de bulkdataset inzicht geeft in bepaalde aspecten van privéleven en de mate waarin de set voor eenieder toegankelijk is. Aan de hand van deze beoordeling wordt het toegangsregime bepaald, te weten: standaard toegang, beperkte toegang of strikt beperkte toegang. De betrokken minister stelt dit vast. Hoe hoger de mate van inbreuk en hoe kleiner de toegankelijkheid, des te strenger is het toegangsregime. Dit wordt in de regeling verder uitgewerkt.

Daarnaast stelt de regeling dat voor het verstrekken van bulkdata aan een buitenlandse dienst, altijd een akkoord van de betrokken minister nodig is. De CTIVD wordt hier dan van op de hoogte gesteld. In de Wiv 2017 geldt ministeriële toestemming en meldplicht aan de CTIVD alleen bij 'ongeëvalueerde' gegevens.

Op het gebied van de tijdswaarborgen stelt de regeling alleen aanvullende eisen voor het toetsen van bulkdata op betekenis, niet voor de relevantiebeoordeling. De regeling bepaalt dat bulkdata binnen één tot drie jaar (afhankelijk van het toegangsregime) periodiek op betekenis moet worden getoetst.

De Evaluatiecommissie ziet met de CTIVD en de betrokken ministers en diensten ook de noodzaak van extra waarborgen voor de verwerking van bulkdata, zeker gezien de gevoelige aard van bulkdata en de inbreuk op privacy. Hierbij is het van belang dat er één uniform verwerkingsregime komt voor alle bulkdata. Daarvoor doet de Evaluatiecommissie een voorstel. In dat voorstel, dat wettelijk moet worden vastgelegd, staan de waarborgen voor de verwerking van bulkdata los van de bevoegdheid waarmee de bulkdata is verkregen. Ook bulkdata verkregen

[139] *Kamerstukken II* 2019/20, 29 924, nr. 203 (Beleidsreactie CTIVD rapporten nr. 70 en 71).
[140] Regeling van 5 november 2020, *Stcrt.* 2020, 56482.

van buitenlandse inlichtingen- en veiligheidsdiensten moet onder dit bulkverwerkingsregime worden geschaard (zie §8.6).

Aanbeveling 5

Leg een uniform verwerkingsregime voor alle bulkdata in de wet vast.

Dit nieuwe uniforme bulkverwerkingsregime moet worden gebaseerd op het huidige verwerkingsregime voor gegevens verkregen uit OOG-interceptie. Daarmee kenmerkt het nieuwe regime zich door drie onafhankelijke waarborgen: waarborgen op handeling, toegang en tijd. De aanbevolen inrichting van dit bulkverwerkingsregime wordt hieronder per waarborg uitgewerkt. Dit voorgestelde bulkverwerkingsregime zorgt voor uniformiteit, striktere waarborgen en een verduidelijking van bepaalde wettelijke begrippen.

4.4.5.1 Handelingswaarborgen nieuw bulkverwerkingsregime

Het nieuwe bulkverwerkingsregime heeft betrekking op alle bulkdata die de diensten in huis hebben; van bulkdata verkregen uit OOG-interceptie tot bulkdata verkregen via een informant of van een buitenlandse dienst. Medewerkers van de diensten mogen deze bulkdata niet zomaar gebruiken. Hiervoor gelden handelingswaarborgen.

Allereerst mogen gegevens uit de bulkdata pas worden gebruikt in het inlichtingenproces nádat deze gegevens zijn geselecteerd. Deze systematiek is gebaseerd op de selectiebevoegdheid binnen het huidige OOG-stelsel. Deze bestaande bevoegdheid ziet op de selectie van inhoud en niet op metadata. Voor metadata heeft de wet een andere waarborg ingesteld (GDA, zie hoofdstuk 5). De Evaluatiecommissie acht het verschil in waarborgen tussen het gebruik van inhoud enerzijds en het gebruik van metadata anderzijds echter niet langer zinvol. Dit verschil is het gevolg van de gedachte dat het kennisnemen en gebruiken van inhoud als meer inbreukmakend kan worden gezien. In het licht van de technologische en privacy ontwikkelingen beschreven in hoofdstuk 3, is deze gedachte steeds minder valide. De Evaluatiecommissie beveelt daarom aan om het onderscheid tussen inhoud en metadata los te laten in het wettelijk kader. Álle bulkdata moet daarmee worden geselecteerd voordat deze gebruikt kan worden in het inlichtingenonderzoek. Dit behoeft een wettelijke wijziging van de huidige selectiebevoegdheid in artikel 50, lid 1, onder a.

Onderscheid tussen inhoud en metadata

Het onderscheid tussen inhoud en metadata komt neer op het onderscheid tussen de communicatie zelf (inhoud) en gegevens over deze communicatie (metadata). Het onderscheid werd gemaakt met het idee dat de inhoud gevoeliger is dan de metadata. In de Wiv 2017 is metadata dan ook met minder waarborgen omkleed dan inhoud. Vanuit juridisch oogpunt is het onderscheid tussen inhoud en metadata ter discussie geraakt. Ook met metadata kan een zware inbreuk worden gemaakt op privacy omdat metadata inzicht kan geven in locaties en gedragingen van personen.[141] Het gaat om informatie die het mogelijk maakt de 'wie, waar, wanneer en hoe' van communicatie te kennen.

[141] EHRM 13 september 2018, (*Big Brother Watch*);HvJEU 6 oktober 2020, (*Privacy International*) r.o. 71.

Vanuit technisch oogpunt is het verschil tussen inhoud en metadata ook steeds problematischer geworden. Dit heeft vooral te maken met het gebruik van internet als drager van communicatie. Waar bij telefonie de metadata en de inhoud technisch onafhankelijk van elkaar worden verwerkt, oorspronkelijk over verschillende kanalen, is bij het internet alle communicatie over één protocol: het *internet protocol* (IP). Communicatie via IP is opgebouwd uit verschillende communicatielagen. In de praktijk wordt boven op een bepaalde communicatie laag weer een nieuw communicatie protocol geïmplementeerd. Dit leidt er toe dat het onderscheid tussen inhoud en metadata vanuit een technisch oogpunt in toenemende mate afhankelijk is van de context.

Dit is bijvoorbeeld goed te zien bij webverkeer. Een URL is lang als metadata beschouwd (het zei tenslotte alleen maar iets over welke webpagina werd bezocht, vergelijkbaar met een telefoonnummer van vroeger). Nu blijken zoekmachines in die URL ook de gebruikte zoektermen op te nemen. Die zoektermen zijn inhoud van communicatie, maar worden verstuurd als onderdeel van de URL. Ook bij *cookies* is het onderscheid lastig. *Cookies* zijn parameters die worden meegestuurd bij het openen van webpagina's. Soms bevatten die hele eenvoudige technische parameters, vergelijkbaar met metadata van vroeger, soms bevatten die (in webwinkels) de hele boodschappenlijst. Het laatste is zeker als inhoud te beschouwen.

Er heeft ook een verschuiving plaatsgevonden in het denken over metadata. Aanvankelijk werd bij een email de metadata (de '*header*') gescheiden van de inhoud ('*body*'). In een header zitten traditionele 'metadata-elementen' zoals afzender, ontvanger, tijdstip, grootte, routering, maar ook het onderwerp. Aanvankelijk werd het onderwerp in de header ook als metadata beschouwd, omdat het 'aan de buitenkant van de envelop staat'. Later is de maatschappelijke mening hierover veranderd; omdat het onderwerp 'zicht geeft op de inhoud' moet het als inhoud worden beschouwd.

Aanbeveling 6

Laat het wettelijk onderscheid tussen metadata en inhoud los.

Aanbeveling 7

Verklaar de selectiebevoegdheid van toepassing op alle bulkdata, zonder onderscheid tussen inhoud en metadata.

De selectie van gegevens uit de bulkdatasets gebeurt gericht, aan de hand van opgegeven selectiecriteria. Dit is overeenkomstig de huidige praktijk in het OOG-stelsel. Voor de inzet van de selectiebevoegdheid is volgens de Evaluatiecommissie toestemming van de minister niet noodzakelijk. De minister heeft een belangrijke rol bij de bulk*verwerving*; zowel bij het stellen van de bulkbehoefte als bij de verwerving van bulkdata via bijzondere bevoegdheden. Hiermee geeft de minister *de facto* al toestemming om de te verwerven bulkdata ook daadwerkelijk te

gebruiken voor het inlichtingenonderzoek. Het aanvullend vragen om toestemming voor het gebruik, wordt door de Evaluatiecommissie als overbodig en belastend gezien. Een interne toestemming voor de selectiebevoegdheid en bijbehorende selectiecriteria kan hier volstaan.

Aanbeveling 8

Beleg het toestemmingsniveau voor selectie intern bij de diensten.

Net zoals nu het geval is voor inhoud uit OOG-interceptie, beveelt de Evaluatiecommissie aan om de gegevens uit bulkdata pas bruikbaar te laten zijn voor inlichtingenteams nádat deze zijn geselecteerd op basis van selectiekenmerken. Alleen specifieke functionarissen hebben toegang tot ongeselecteerde bulkdata ('functiescheiding'). Een medewerker van een inlichtingenteam kan wel zien of de bulkdata een potentieel zoekresultaat bevat. Dit gaat via de zogenaamde '*hit-no hit*'-procedure. Hierbij ziet de medewerker alleen dát er een resultaat is van de zoekvraag (een *hit*), niet wát dit resultaat is. Om dit resultaat te mogen zien moet het eerst zijn geselecteerd. Na selectie is het resultaat te zien en ook te gebruiken in het inlichtingenproces.[142]

Het hiervoor beschreven proces is ingericht voor de zorgvuldige omgang met bulkdata. De Evaluatiecommissie ziet tegelijkertijd dat er in de praktijk aanleiding kan zijn voor het bij uitzondering anders inrichten van deze selectieprocedure.

Zo zou er een uitzondering kunnen worden gemaakt voor bulkdatasets die naar hun aard evident minder gevoelige gegevens bevatten. Daarbij kan worden gedacht aan het kentekenregister van de RDW en het register van de KvK. De relatief zware selectieprocedure die eerder is beschreven, staat niet in verhouding tot de gevoeligheid van de gegevens in deze (deels openbare) register-bulkdatasets. Bijvoorbeeld het opzoeken van een kenteken van een *target* in het kentekenregister van de RDW zou wat de Evaluatiecommissie betreft via een versimpelde selectieprocedure kunnen lopen. Een *hit* zou daarbij automatisch tot selectie kunnen leiden.

Deze versimpelde selectieprocedure zou alleen voor bepaalde register-bulkdatasets en voor bepaalde inlichtingenteams moeten gelden. Niet elk inlichtingenteam zal gebruik maken van het kentekenregister van de RDW of het register van de KvK. Dit is waarschijnlijker voor teams die onderzoek doen naar bijvoorbeeld jihadistische groeperingen in Nederland dan voor teams die cyberdreiging vanuit statelijke actoren onderzoeken. Enkel voor de teams die de specifieke bulkdatasets nodig hebben voor hun onderzoek, zou de versimpelde selectieprocedure mogelijk kunnen zijn. Een dergelijke uitzondering moet grondig worden onderbouwd en vastgelegd zodat de CTIVD daar goed op kan toezien. Voor overige teams blijft de strenge selectieprocedure van kracht.

Deze uitzonderingssituatie komt qua toegangswaarborgen overeen met het beperkte toegangsregime uit de tijdelijke bulkregeling, waarbij het hoofd van de dienst een inlichtingenteam na een gemotiveerd verzoek toegang kan verlenen tot een specifieke bulkdataset.

[142] In de tijdelijke bulkregeling geldt een soortgelijke waarborg alleen voor het strengste toegangsregime, waarbij een medewerker een interne procedure moet doorlopen voordat het resultaat mag worden gezien.

Aanbeveling 9

Laat ruimte bestaan voor onderbouwde uitzonderingen, waar een versimpelde selectieprocedure kan worden gevolgd.

Ten aanzien van het delen van bulkdata met buitenlandse diensten beveelt de Evaluatiecommissie aan om wettelijk vast te leggen dat er altijd ministeriële toestemming nodig is voor het verstrekken van bulkdata aan buitenlandse diensten. In de huidige wet geldt de wettelijke verplichting voor toestemming van de minister alleen wanneer het ongeëvalueerde gegevens betreft of wanneer de minister dient te worden betrokken vanwege de buitenlandse dienst met wie gegevens worden gedeeld (zie hoofdstuk 8). Vanwege de gevoelige aard van bulkdata acht de Evaluatiecommissie het aangewezen om hiervoor altijd het toestemmingsniveau van de minister te hanteren. Juist bij het delen van bulkdata – waarvan niet altijd precies bekend is welke gegevens in de bulkdataset zitten – is er sprake van meer risico. De betrokken minister maakt een afweging of de risico's in verhouding staan tot het doel van de verstrekking. Voor de risico's wordt zowel naar de wegingsnotitie van de betreffende dienst gekeken als naar de aard en omvang van de te verstrekken gegevens in de bulkdataset.[143] De betrokken minister moet eveneens toetsen op de extra inhoudelijke waarborgen zoals voorgesteld in hoofdstuk 8. Van een verleende toestemming wordt melding gemaakt bij de CTIVD. Het vereiste van ministeriële toestemming en meldplicht aan de CTIVD is overigens overeenkomstig met de tijdelijke bulkregeling.[144] De introductie van de voorwaarde van ministeriële toestemming voor het delen van bulkdata betekent ook dat het wettelijke onderscheid tussen geëvalueerde en ongeëvalueerde gegevens kan komen te vervallen. Door de minister een rol te geven bij het delen van bulkdata wordt in *alle* gevallen voorzien in de waarborgen die onder de huidige wet gelden voor ongeëvalueerde gegevens.

Gegevens die daarentegen geselecteerd zijn uit bulkdata, zijn op zichzelf geen bulkdata meer. Doordat deze gegevens gericht zijn geselecteerd, is in voldoende mate bekend wat er wordt verstrekt.[145] Voor het delen van deze gegevens voldoet het huidige wettelijke kader.

Aanbeveling 10

Het verstrekken van bulkdata aan buitenlandse diensten wordt op het niveau van de minister belegd en is onderhevig aan meldplicht aan de CTIVD. Het wettelijke onderscheid tussen 'geëvalueerd' en 'ongeëvalueerd' komt daarmee te vervallen.

Naast het selecteren en delen van bulkdata bestaat er ook de handelingsvorm van GDA voor bulkdata. In hoofdstuk 5 wordt hier separaat op ingegaan.

---

[143] CTIVD. (2019). *Toezichtsrapport 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD*. p. 13.
[144] Regeling van 5 november 2020, *Stcrt*. 2020, 56482, artikel 10.
[145] Dit is bovendien in lijn met het voorbeeld in de MvT dat nog niet geselecteerde gegevens uit OOG-interceptie als ongeëvalueerd moeten worden beschouwd. *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 163.

4.4.5.2 Toegangswaarborgen bulkverwerkingsregime

Het nieuwe bulkverwerkingsregime zou wat de toegangswaarborg betreft moeten aansluiten bij de huidige toegangswaarborgen voor inhoud uit OOG-interceptie. Het uitgangspunt is dat medewerkers in het inlichtingenproces van de diensten in beginsel geen toegang hebben tot bulkdata. Alleen na selectie kunnen medewerkers in het inlichtingenproces gegevens uit bulkdatasets gebruiken voor hun onderzoek. Ten behoeve van deze selectie is het noodzakelijk dat – net als in het huidige OOG-stelsel – een kleine groep daartoe aangewezen functionarissen wel toegang krijgen tot de bulkdata voor *search* gericht op selectie. De *search* gericht op selectiebevoegdheid wordt veralgemeniseerd naar alle bulkdata.

Voor geselecteerde gegevens uit bulkdata geldt overigens niet dat elke medewerker in het inlichtingenproces hier toegang toe heeft. Dit kan alleen als de medewerker de benodigde autorisatie heeft. Deze autorisatie wordt alleen verleend indien toegang tot de geselecteerde gegevens nodig is voor de uitvoering van zijn/haar onderzoek.

Aanbeveling 11

Maak bulkdata niet toegankelijk voor alle medewerkers in het inlichtingenproces. Slechts bepaalde functionarissen krijgen toegang voor search gericht op selectie.

4.4.5.3 Tijdswaarborgen bulkverwerkingsregime

De tijdswaarborgen bij bulkdata zien op hoe lang de diensten bulkdata mogen bewaren. Twee elementen zijn daarbij van belang: de relevantiebeoordeling en het toetsen van de betekenis. Zoals beschreven onder §4.4.4 geldt nu voor de ene bulkdataset de eis om deze op relevantie te beoordelen, terwijl de andere bulkdataset direct in het betekenisregime terecht komt. Dit gebrek aan uniformiteit moet worden verholpen.

Allereerst beveelt de Evaluatiecommissie aan om het vereiste van de relevantiebeoordeling (artikel 27) te laten gelden voor alle bulkdata, niet alleen voor bulkdata verkregen via bijzondere bevoegdheden. De verbreding van deze belangrijke waarborg draagt bij aan de uniformiteit van het bulkverwerkingsregime.

Aanbeveling 12

Het vereiste van relevantiebeoordeling geldt voor alle bulkdata.

Voor de termijn waarbinnen de bulkdata op relevantie moet worden beoordeeld, adviseert de Evaluatiecommissie om de huidige termijn van drie jaar voor OOG-interceptie (ether) uniform te hanteren. Zoals reeds beschreven wordt in de huidige wet alleen van bulkdata gesproken bij OOG-interceptie. Juist voor deze gegevens heeft de wetgever het noodzakelijk geacht om niet de standaardtermijn van één jaar maar een termijn van drie jaar te stellen aan de relevantiebeoordeling. Dit vanwege het belang van deze data voor het doen van onderzoek naar onbekende *targets* en ongekende dreiging. In de praktijk blijkt dat de periode van een jaar (met mogelijke

verlenging van een half jaar) te kort is om bulkdata te beoordelen op relevantie.[146] Het betreft grote hoeveelheden gegevens die bovendien juist over langere tijd hun waarde voor het onderzoek bewijzen. Om dezelfde redenen zou het vereiste van 'zo spoedig mogelijk' niet van toepassing moeten zijn op de relevantiebeoordeling van bulkdata.[147] Ook dit is in lijn met de huidige relevantiebeoordeling van OOG-data waarbij dit vereiste bewust niet is opgenomen.

Aanbeveling 13

Stel een termijn in van drie jaar voor de relevantiebeoordeling van bulkdata.

Aanbeveling 14

Verklaar het vereiste van zo spoedig mogelijk niet van toepassing op de relevantiebeoordeling van bulkdata.

De Evaluatiecommissie verwacht niet dat bovenstaande uniformering al voldoende is om een structurele oplossing te bieden voor de huidige knelpunten rondom de relevantiebeoordeling van bulkdata. Deze knelpunten zijn namelijk het gevolg van het ontbreken van een wettelijk kader voor de invulling van het begrip 'relevantie' en van de wijze waarop gegevens op relevantie moeten worden beoordeeld. Dit wordt met de bovenstaande aanbevelingen niet opgelost.

De relevantiebeoordeling vereist dat gegevens worden onderzocht op relevantie voor het onderzoek waarvoor gegevens zijn verworven, dan wel voor enig ander lopend onderzoek. Voor gericht verworven gegevens is deze relevantiebeoordeling in de praktijk goed uitvoerbaar en vormt het een nuttige waarborg. Deze gegevens zijn per definitie te relateren aan personen en/of organisaties die in onderzoek zijn van de diensten. Dat is immers de reden dat de verwervende bevoegdheid is ingezet. Zoals al is toegelicht, is het bij bulkdata op voorhand niet vast te stellen welke specifieke gegevens uit de bulkdata gaan bijdragen aan het inlichtingenonderzoek. De vraag is wat een passende invulling van de relevantiebeoordeling van bulkdata. De Evaluatiecommissie ziet hiervoor de volgende oplossingsrichting.

In de toelichting op de wet moet een kader worden opgenomen voor de relevantiebeoordeling van bulkdata. Voor dit kader is in ieder geval van belang dat deze relevantiebeoordeling niet kan worden gezien als een cumulatie van relevantiebeoordelingen van gericht verworven gegevens. Een bulkdataset is immers geen opeenstapeling van gegevens die gekoppeld kunnen worden aan personen en/of organisaties die in onderzoek zijn. Dit maakt de aard van bulkdata ook zo anders ten opzichte van gericht verworven gegevens. Uiteraard is het niet zo dat daardoor alle gegevens uit de bulkdataset moeten worden bewaard. Ook voor bulkdata blijven de datareductie-vereisten onverminderd van kracht. Echter, gezien de aard van bulkdata beveelt de Evaluatiecommissie aan om de relevantiebeoordeling niet te koppelen aan specifieke personen en/of organisaties maar aan de bewezen operationele waarde van (delen van) de bulkdata voor het beantwoorden

[146] CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 10.
[147] CTIVD. (2020). *Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. p. 6.

van onderzoeksvragen van de diensten. Operationele waarde kan kwalitatief worden onderbouwd (zoals belang voor specifieke onderzoeken, relatie tot landen/regio's in de Geïntegreerde Aanwijzing), of kwantitatief (zoals hoe vaak en wanneer geraadpleegd, door hoeveel teams). Zo wordt er een balans aangebracht tussen enerzijds de noodzakelijke waarborgen rondom bulkdata en anderzijds de operationele waarde van bulkdata voor de taakuitvoering van de diensten. De diensten moeten dit goed onderbouwen en vastleggen, zodat de CTIVD toezicht kan houden op de relevantiebeoordeling.

Hierbij moet het onderscheid tussen register- en gedrag-bulkdata gebruikt worden. Register-bulkdata heeft de eigenschap om voor langere tijd en als geheel van belang te kunnen zijn voor het onderzoek van de diensten. Voor gedrag-bulkdata is dit niet per se het geval. Deze gegevens zijn meer tijdsgebonden. De relevantiebeoordeling van register-bulkdata acht de Evaluatiecommissie daarom mogelijk ten aanzien van de gehele bulkdataset: een integrale relevantiebeoordeling, eventueel met een beperking in het aantal datapunten per kenmerk. Voor gedrag-bulkdata geldt dat de relevantiebeoordeling doorgaans op meer deelverzamelingen van de bulkdataset gericht kan worden, bijvoorbeeld een bepaalde periode terug in de tijd of de eerdergenoemde geografische begrenzing. De Evaluatiecommissie beveelt aan dit onderscheid op te nemen in de toelichting bij de nieuwe wet.

Aanbeveling 15

Koppel de relevantiebeoordeling niet aan specifieke personen/organisaties maar aan de operationele waarde. Hierbij kan het onderscheid register- en gedrag-bulkdata nuttig zijn.

Ten slotte vindt de Evaluatiecommissie het van belang dat de als relevant aangemerkte bulkdata in het betekenisregime periodiek worden gecontroleerd op betekenis. Het is hierbij passend om de periodieke controle meer frequent te laten plaatsvinden dan de controle van gericht verworven gegevens.

Aanbeveling 16

Toets de als relevant aangemerkte bulkdata eerder en vaker op betekenis.

4.5 Conclusie

De Evaluatiecommissie onderschrijft het belang van bulkdata voor de taakuitvoering van de diensten. Tegelijkertijd is het verwerven en verwerken van bulkdata gevoelig vanwege de aard daarvan. Het omvat gegevens van personen en/of organisaties die niet in onderzoek zijn van de diensten en dat ook nooit zullen worden. Juist over de nut en noodzaak van de verzameling van grote hoeveelheden gegevens is veel maatschappelijke discussie. De Wiv 2017 voorziet nu niet in de nodige waarborgen voor zorgvuldige omgang met bulkdata. Niet alleen is de wet qua waarborgen te veel gericht op de bevoegdheid waar gegevens mee worden verworven, de wet spreekt bovendien alleen van bulk in het kader van OOG-interceptie. Daardoor is zowel de bulkverwerving als de daaropvolgende verwerking in de wet niet uniform geregeld en onvol-

doende voorzienbaar. In de verschillende aanbevelingen maakt de Evaluatiecommissie gebruik van het conceptueel en praktisch nuttige onderscheid tussen register-bulkdata en gedrag-bulkdata.

Er is meer uniformiteit en met name voorzienbaarheid nodig in de verschillende manieren waarop de diensten bulkdata kunnen *verwerven*. Hiertoe is een bulkparagraaf in de wet de aangewezen weg. Ook is een extra stap in de huidige toestemmingsprocedure voor bulkverwerving nodig: het aantonen van de bulkbehoefte. Hierbij wordt de noodzakelijkheid van bulk gemotiveerd. Voordat tot verwerving wordt overgegaan, moet de betrokken minister akkoord zijn met de behoefte. Dit betekent een extra waarborg ten opzichte van de huidige situatie. Voor de verwerving van bulkdata beveelt de Evaluatiecommissie een passende invulling van het gerichtheidsvereiste aan. Naast het terugbrengen van aantal personen/organisaties in de bulkdataset, wordt een nieuwe invulling van gerichtheid geïntroduceerd aan de hand van datapunten.

De belangrijkste aanbeveling van de Evaluatiecommissie ten aanzien van de *verwerking* van bulkdata is om een uniform systeem van waarborgen te introduceren voor álle bulkdata, onafhankelijk van de wijze waarop deze bulkdata is verkregen. In dit systeem gelden handelings-, toegangs- en tijdswaarborgen, gebaseerd op het huidige OOG-stelsel. Gegevens uit bulkdata moeten worden geselecteerd voordat deze kunnen worden gebruikt in het inlichtingenproces (handelingswaarborg). Medewerkers uit dit inlichtingenproces hebben in beginsel geen toegang tot bulkdata (toegangswaarborg). Daarnaast moet alle bulkdata op relevantie worden beoordeeld op basis van de operationele waarde, binnen een termijn van drie jaar (tijdswaarborg). Tenslotte geldt voor het delen van bulkdata met buitenlandse diensten de eis van ministeriële toestemming en meldplicht aan de CTIVD (handelingswaarborg). Ten opzichte van de huidige situatie betekent dit een verzwaring van de waarborgen op handeling en toegang. Voor de tijdswaarborg geldt dat het enerzijds een verzwaring is van de waarborgen doordat alle bulkdata op relevantie moet worden beoordeeld. Anderzijds is de beoordelingstermijn verlengd van maximaal anderhalf naar drie jaar.

5 Geautomatiseerde Data-Analyse (GDA)

5.1 Inleiding

De Wiv 2017 geeft de diensten bevoegdheden waarmee gegevens kunnen worden verworven. Na verwerving hebben gegevens meestal nog geen betekenis en ontberen zij context. Ze moeten eerst verder worden verwerkt om van ruwe data omgezet te kunnen worden naar bruikbare informatie. Daartoe worden de gegevens doorzocht, geordend en/of geanalyseerd. Dit gebeurt door gerichte zoekvragen te stellen op basis van technische kenmerken, of door verbanden tussen gegevens op te vragen, bijvoorbeeld een communicatienetwerk op basis van een e-mailadres. In andere gevallen wordt er gebruik gemaakt van statistische methoden of meer geavanceerde *data science*-technieken om gegevens te combineren en te correleren. De verkregen informatie wordt uiteindelijk gevalideerd door een medewerker en, indien bruikbaar, vertaald naar inlichtingen. Geautomatiseerde data-analyse (GDA) is in de Wiv 2017 als nieuw begrip geïntroduceerd om de diensten een expliciete wettelijke grondslag te geven voor het verwerken van gegevens met meer geavanceerde geautomatiseerde technieken. In de Wiv 2002 werd alleen gesproken over een algemene vorm van 'gegevensverwerking' (artikel 12). Ook toen gebruikten de diensten echter al meer geavanceerde vormen van gegevensverwerking.

In toelichting op de wet heeft de wetgever het als volgt verwoord: "(...) gegevensverwerking (is) de kernactiviteit van inlichtingen- en veiligheidsdiensten. In onderhavig wetsvoorstel wordt deze kernactiviteit – met inachtneming van de eisen die daaraan vanuit grond- en mensenrechtelijk perspectief zijn te stellen – in al zijn onderdelen duidelijk genormeerd en van toereikende waarborgen voorzien. Mede gelet op de toegenomen betekenis van verwerkingen met een big data-karakter is het wenselijk om geautomatiseerde data-analyse als werkmethode van de diensten van een expliciete wettelijke grondslag te voorzien. Het voorgestelde artikel 60 strekt daartoe."[148]

Al jaren nemen de omvang, verscheidenheid en complexiteit van data, databestanden en datacommunicatievormen wereldwijd in zowel het private als publieke domein sterk toe. De verwachting is dat deze groei de komende jaren onverminderd doorgaat en dat nieuwe technieken hun intreden zullen doen. Het belang – en in feite de noodzaak – voor de diensten om data-analysetechnieken verder te professionaliseren, waaronder verdergaande en slimmere automatisering, gaat daarmee gelijk op. In de Wiv 2017 is het toepassen van GDA als een integraal onderdeel van gegevensverwerking ('kernactiviteit') gecodificeerd met daarbij behorende standaard-waarborgen. Wanneer GDA wordt toegepast op metadata verkregen uit OOG-interceptie en gericht is op het identificeren van personen of organisaties, dan geldt daarvoor een bijzondere regeling met aanvullende waarborgen (artikel 50, lid 1, onder b). Tegen de verwachting in, heeft de explicitering van de grondslag voor GDA tot problemen geleid. Deze explicitering is door diensten, ministers en toezichthouders namelijk verschillend geïnterpreteerd.

In dit hoofdstuk wordt eerst een toelichting gegeven op de wettelijke regeling van GDA. Vervolgens zal er een overzicht volgen van de toepassing van GDA in de praktijk en van de diverse standpunten van de TIB, de CTIVD en de diensten. Daarna volgt er een analyse van de huidige situatie. Tenslotte komt de Evaluatiecommissie met aanbevelingen.

[148] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 131 (MvT Wiv 2017).

5.2 GDA in de Wiv 2017

5.2.1 Wettelijke basis GDA (artikel 60)

Het fundament van GDA in de wet is artikel 60. Hierin staat dat de diensten bevoegd zijn "geautomatiseerde data-analyse toe te passen" op gegevens uit diverse bronnen. Het gaat hier om gegevens die de diensten al hebben verworven. GDA is dus een verwerkingsbevoegdheid. Het artikel noemt vervolgens drie vormen die "in ieder geval" onder GDA vallen: (i) het op geautomatiseerde wijze onderling met elkaar vergelijken van gegevens, (ii) het doorzoeken van gegevens aan de hand van profielen en (iii) het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen (artikel 60, lid 2). Dit zijn volgens de toelichting bij de wet "drie veel voorkomende vormen van data-analyse".[149]

De wet geeft derhalve geen sluitende definitie van het begrip GDA en dus ook geen scherpe afbakening van wat *niet* onder GDA kan worden verstaan. In de toelichting op de wet is aangegeven dat er bewust voor is gekozen om geen limitatieve opsomming van GDA te geven om de bepaling toekomstbestendig te maken. Hiermee zou het mogelijk zijn om eventuele nieuwe methoden en technieken ook onder GDA te laten vallen.[150] In de praktijk zijn daardoor verschillende interpretaties ontstaan over welke vormen van gegevensverwerking nu precies als GDA moeten worden aangemerkt. Deze situatie zal verder worden toegelicht in de volgende paragraaf.

In de toelichting op de wet op GDA zijn elementen opgenomen uit het WRR-rapport 95 'Big Data in een vrije en veilige samenleving'.[151] De toelichting hanteert een drietal hoofdkenmerken uit dit rapport voor de duiding van *big data*. Allereerst gaat het om grote hoeveelheden gestructureerde en ongestructureerde data uit verschillende bronnen. Daarnaast is de analyse 'datagedreven', waarbij geautomatiseerd naar correlaties wordt gezocht. Dit heeft vooral potentie voor analyses van het heden (*realtime analysis*) en de toekomst (*predictive analysis*). Ten slotte moet de analyse leiden tot '*actionable knowledge*': kennis om te kunnen toepassen voor beslissingen op groeps- of individueel niveau.

Tenslotte is in artikel 60, lid 3, het verbod opgenomen op automatische besluitvorming. Het is de diensten niet toegestaan om uitsluitend op basis van resultaten van GDA maatregelen te treffen jegens een persoon. Dit geldt voor alle vormen van gegevensverwerking die als GDA moeten worden aangemerkt. Voordat resultaten van GDA kunnen leiden tot maatregelen moet er dus altijd sprake zijn van menselijke validatie of nadere (menselijke) weging.[152] Dit wettelijke verbod is een belangrijke waarborg omdat daarmee de diensten worden verplicht de resultaten van GDA altijd door medewerkers te laten valideren en wegen. Resultaten worden dus nooit zonder tussenkomst van een medewerker overgenomen of gebruikt.[153]

---

[149] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 132 (MvT Wiv 2017).
[150] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 132 (MvT Wiv 2017).
[151] Wetenschappelijke Raad voor het Regeringsbeleid. (2016). *WRR-Rapport nr. 95: Big Data in een vrije en veilige samenleving*.
[152] Het verbod op automatische besluitvorming komt ook terug in de AVG, in artikel 22, lid 1: 'De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (-) gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.
[153] Vergelijk de uitspraak van de rechtbank Den Haag 5 februari 2020, (*SyRI);* NJ2020, nr. 386, aflevering 45, p. 6768-6795.

5.2.2 Toestemming voor GDA op OOG-metadata (art. 50, lid 1, onder b)

De wet kent voor één situatie een bepaling die extra waarborgen definieert bij het toepassen van GDA: in artikel 50, lid 1, onder b, is geregeld dat de diensten GDA mogen toepassen op metadata verkregen uit OOG-interceptie voor het identificeren van personen en organisaties nadat toestemming van de betrokken minister is verkregen en deze door de TIB is getoetst. De toelichting op dit artikel schaart deze metadata-analyse onder geautomatiseerde data-analyse.[154] Het is belangrijk om op te merken dat de TIB hiermee een rol heeft gekregen bij het *verwerken* van gegevens. Dit onderwerp komt nader aan de orde in hoofdstuk 9. Bij het toepassen van GDA op andere soorten gegevens, dus niet metadata uit OOG-interceptie, geldt deze uitzonderlijke rol niet.

In artikel 50, lid 4, staat welke additionele elementen nodig zijn voor de onderbouwing van een toestemmingsaanvraag voor het betrekken van OOG-metadata bij GDA. De aanvraag moet een aanduiding van de toe te passen vorm van GDA bevatten en, voor zover van toepassing, een aanduiding van de gegevensbestanden die betrokken worden. Ook over deze ogenschijnlijk vanzelfsprekende toevoeging is in de praktijk veel discussie ontstaan. Dit heeft vooral te maken met het feit dat het statische begrip 'gegevensbestand' zich niet goed laat vertalen naar de technische praktijk van grootschalige, dynamische gegevensverwerking waarbij gegevens continu worden aangevuld en verwijderd.

5.3 GDA in de praktijk

GDA is alleen aan ministeriële toestemming en een toets door de TIB onderworpen als er OOG-metadata in wordt betrokken. De vraag is echter welke vormen van gegevensverwerking als GDA moeten worden gezien en dus welke vormen aan de aanvullende toestemming onderworpen zijn.

De TIB en de CTIVD hebben in hun rechtseenheidsbrief in 2018 aangegeven wat zij gezamenlijk verstaan onder GDA en welk kader gehanteerd wordt bij de rechtmatigheidstoets van een toestemmingsaanvraag.[155] Zij zijn van mening dat zowel eenvoudige als complexe vormen van gegevensverwerking als GDA moet worden gezien en verwijzen hierbij naar de toelichting waarin wordt geschreven dat metadata-analyse een vorm van GDA is.[156] De TIB en de CTIVD zien daarmee een grotere reikwijdte van de GDA-bepalingen dan de ministers en de diensten.[157] De ministers en de diensten geven aan dat er verschillende vormen van gegevensverwerking bestaan met verschillende mate van inbreuk op de persoonlijke levenssfeer. Een voorbeeld van een van gegevensverwerking met beperkte inbreuk is volgens de ministers en de diensten 'naslag'; het invoeren van een telefoonnummer in een applicatie die de bron(nen) waarin dat nummer voorkomt laat zien. Een vorm die meer inbreuk maakt, ook volgens de ministers en de diensten, is het geautomatiseerd analyseren van gegevensbestanden die als resultaat statistische verbanden en mogelijke patronen tussen personen weergeeft. Alleen de vormen van gegevensverwerking waar er een grotere inbreuk worden gemaakt op de persoonlijke levenssfeer, zouden volgens de ministers en de diensten als GDA moeten worden gezien. Alleen voor die vormen zou dan ook de toestemming van de minister en toets door de TIB moeten gelden.

---

[154] Kamerstukken II 2016/17, 34 588, nr. 3, p. 112 (MvT Wiv 2017).
[155] *Kamerstukken II* 2018/19, 29 924, nr. 173, p. 3 (brief rechtseenheidsoverleg iz. reikwijdte en GDA).
[156] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 112 (MvT Wiv 2017).
[157] Bijlage bij *Kamerstukken II* 2018/19, nr. 179, p. 5.

Uitleg terminologie naslag

Enkelvoudige naslag: een enkelvoudige zoekvraag op basis van een kenmerk, zoals het zoeken van een naam bij een kenteken, een IMEI[158] bij een IMSI[159] of een geolocatie bij een IP-adres.

Meervoudige naslag: een samengestelde zoekvraag op basis van een meerdere kenmerken en eventuele andere elementen, bijvoorbeeld locatie of tijd.

Cumulatieve naslag: het automatisch doorzoeken op basis van een **startkenmerk**. Hier zijn in de praktijk twee hoofdvormen in te onderscheiden:

1. Op basis van het startkenmerk automatisch opzoeken welke andere kenmerken in de communicatie zijn betrokken. Dit levert, als de gegevens voorhanden zijn, een communicatienetwerk op ('welk toestel heeft contact met welk ander toestel'). Dit automatisch doorzoeken wordt beperkt tot een aantal stappen: in de praktijk wordt dit de 'diepte' van de naslag genoemd.
2. Op basis van een startkenmerk automatisch opzoeken welke andere kenmerken te vinden zijn die horen bij het startkenmerk. Bij een mobiel telefoonnummer kan een IMSI, een IMEI, een locatie, een tijdstip en een chat-id gevonden worden indien die gegevens voorhanden zijn. Deze manier van naslaan wordt in de praktijk 'breed' zoeken genoemd.

Door alle partijen wordt onderschreven dat het kunnen verwerken van gegevens noodzakelijk is voor de taakuitvoering van de diensten.[160] Tot op heden hebben de ministers en de diensten enerzijds en de TIB en de CTIVD anderzijds nog steeds discussie over welke vormen van gegevensverwerking moeten worden aangemerkt als GDA en waar een toestemmingsaanvraag voor GDA aan moet voldoen. Deze discussie heeft een impasse bereikt. De Evaluatiecommissie vindt het belangrijk deze impasse te doorbreken, met het oog op de systematische praktijk van kabelinterceptie en het groeiend belang van GDA.

5.4 Voorgestelde oplossing

Het GDA-probleem heeft volgens de Evaluatiecommissie twee oorzaken. Ten eerste geeft de wet geen duidelijkheid over welke vormen van gegevensverwerking als GDA zijn aan te merken en met name ook welke niet. Ten tweede biedt GDA de enige expliciete waarborg bij de verwerking van OOG-metadata, dus bulkdata uit de ether en van de kabel, gericht op de identificatie van personen en organisaties. De discussie over de interpretatie van GDA is vermengd geraakt met de discussie over de benodigde waarborgen voor de verwerking van OOG-metadata.

De eerste stap naar een oplossing is om deze discussies van elkaar te scheiden. De eerste discussie gaat over de vraag welke waarborgen moeten gelden voor welke vormen van gegevensverwerking (handelingswaarborgen). De tweede discussie gaat over de vraag welke waarborgen

[158] IMEI: International Mobile Equipment Identity. Code die hoort bij een mobiele telefoon.
[159] IMSI: International Mobile Subscriber Identity: Code die hoort bij een SIM-kaart van een mobiele telefoon.
[160] *Kamerstukken II* 2018/19, 29 924, nr. 173, p. 1 (brief rechtseenheidsoverleg iz. reikwijdte en GDA).

gelden voor de verwerking van OOG-metadata (toegangswaarborgen). Deze waarborgen werken onafhankelijk van elkaar zodat ze, indien dat nodig is, elkaar ook kunnen aanvullen.

De verwerking van OOG-metadata valt onder het verwerkingsregime van bulk, zoals reeds in §4.4.5 besproken en waarvoor een uniform regime wordt aanbevolen. Daarom wordt in dit hoofdstuk vanaf nu niet meer gesproken van OOG-metadata maar van bulkdata.

Toegangswaarborgen
De verwerking van bulkdata rechtvaardigt eigen waarborgen vanwege de aard van de gegevens. In §4.4.5 is door de evaluatiecommissie een nieuw bulkdataverwerkingsregime gedefinieerd. Daaruit volgen toegangswaarborgen. Die waarborgen op toegang staan los van de vraag of de vorm van gegevensverwerking moet worden gezien als GDA.

Handelingswaarborgen
Bepaalde vormen van gegevensverwerking zijn op zichzelf gevoelig en rechtvaardigen daarom additionele waarborgen. Deze handelingswaarborgen zijn onafhankelijk van de aard van de gegevens (bulkdata of andersoortige gegevens).

Dan rijst de vraag voor welke handelingen deze waarborgen moeten gelden. Daarbij is het zinvol te kijken naar het resultaat van een bepaalde gegevensverwerking. Dit resultaat kan verdeeld worden in twee categorieën:

1. Het resultaat (van de gegevensverwerking) is in essentie een deelverzameling van de betrokken gegevens. Bij de handeling 'opvragen van gegevens' is het resultaat dan een verzameling van gegevens die voldoet aan de zoekvraag. Ook wanneer het resultaat op een bepaalde manier wordt samengesteld of gevisualiseerd (met bijvoorbeeld een grafiek), bestaat het resultaat nog steeds uit de bevraagde gegevens.
2. Het resultaat (van de gegevensverwerking) voegt iets toe aan de betrokken gegevens (zie de voorbeelden hierna). Het resultaat bestaat dus uit méér dan de bevraagde gegevens.

Voorbeelden categorie 1:

Opzoeken van gegevens
Resultaat: **gegevens** die voldoen aan zoekvraag, zoals kenteken in RDW, telefoonnummer in communicatiebulkdataset.

Weergeven communicatienetwerk
Resultaat: grafische weergave van **gegevens** die handelt over hetzelfde als de gegevens zelf, namelijk met welke andere nummers een nummer in contact is geweest (wordt alleen geautomatiseerd opgezocht en weergegeven).

Opzoeken van gegevens op basis van locatie
Resultaat: **gegevens** met een locatie die voldoet aan de zoekvraag. De gegevens worden weergegeven op een kaart.

Voorbeelden categorie 2:

Target discovery
Het automatisch classificeren van nieuwe *targets* op basis van het bezoeken van bepaalde websites.

Resultaat: **toevoeging** dat iemand met een bepaalde **waarschijnlijkheid** voldoet aan *target*-profiel.

Groepsdetectie
Resultaat: **toevoeging** dat een verzameling kenmerken met een bepaalde **waarschijnlijkheid** als samen reizende groep kan worden beschouwd.

Gezichtsherkenning
Resultaat: **toevoeging** dat een foto met een bepaalde **waarschijnlijkheid** overeenkomt met foto's van gekende individuen.

Wanneer een gegevensverwerking plaatsvindt uit de tweede categorie, is er volgens de Evaluatiecommissie sprake van een grotere gevoeligheid. Hierbij wordt er namelijk informatie toegevoegd aan gegevens, zoals de voorbeelden hierboven laten zien. Deze informatie wordt door algoritmen op basis van de onderliggende gegevens gegenereerd. Deze extra informatie heeft ook een inhoudelijke betekenis: Wie voldoet aan een profiel? Wie zou een mogelijk nieuw *target* kunnen zijn? Welke personen behoren tot deze groep? Het gaat hier dus om 'sturingsinformatie' die gebruikt wordt bij verder onderzoek, en niet om informatie die direct leidt tot een maatregel (zoals het uitbrengen van een ambtsbericht). Er geldt immers een verbod op automatische besluitvorming.

De toepassing van gegevensverwerking uit de tweede categorie door de diensten ligt maatschappelijk gevoelig. Er zijn zorgen over welke vormen van gegevensverwerking de diensten mogen toepassen en hoe dit in de dagelijkse praktijk zorgvuldig en gecontroleerd plaatsvindt. De Evaluatiecommissie stelt vast dat dit beter moet worden vastgelegd. Daarom wordt het begrip 'GDA+' geïntroduceerd om deze tweede categorie gegevensverwerking te omschrijven. Deze categorie moet bovendien met specifieke handelingswaarboren worden omkleed.

Met GDA+ wordt het volgende bedoeld:

Het verwerken van gegevens met als **resultaat** een uitkomst:
- die zelf géén onderdeel uitmaakt van de gegevens;
- en die over zaken handelt anders dan waar de gegevens zelf over gaan;
- en die een bepaalde waarschijnlijkheid heeft;
- en die een classificatie en zelfs een identificatie kunnen geven;
- en die als doel heeft het identificeren van personen of organisaties;
- en die de basis biedt voor verder onderzoek, niet voor handelen.

Aanbeveling 17

Herdefinieer de categorie gegevensverwerking (hier genoemd GDA+) die voorzien moet worden van handelingswaarborgen. Het oorspronkelijke begrip GDA wordt vervangen door GDA+.

De Evaluatiecommissie beveelt aan om de categorie gegevensverwerking GDA+ duidelijk en afgebakend in de wet vast te leggen. Het gaat hier om gegevensverwerking uit de tweede categorie. Gegevensverwerking uit de eerste categorie, waarbij het resultaat in essentie een deelverzameling van de betrokken gegevens is, valt hier niet onder. Deze gegevensverwerking volgt namelijk uit de algemene bepaling voor gegevensverwerking, te weten artikel 1, onder f, van de Wiv 2017, en behoeft geen aparte grondslag. Het is van belang om te constateren dat de gegevensverwerking die volgt uit artikel 1, onder f, naadloos aansluit op GDA+, zonder uitzonderingen. De Evaluatiecommissie meent met deze herdefinitie te omschrijven wat de oorspronkelijke bedoeling van GDA is geweest.

5.5 Handelingswaarborgen GDA+

GDA+ is een vorm van gegevensverwerking. Het verwerken van gegevens is een dynamisch proces en leent zich daarom minder goed voor een statische ex-ante toets door de TIB, maar bij uitstek voor (dynamisch) toezicht door de CTIVD (zie §9.3 en §9.4). Dit toezicht moet volgens de Evaluatiecommissie niet alleen zien op de uitvoering van GDA+, maar ook de ontwikkeling en validatie van technische functionaliteiten voor GDA+ omvatten.

Europese jurisprudentie over GDA

In het vorige hoofdstuk kwam de uitspraak van het HvJEU (*Quadrature du Net e.a./Ordre des barreaux francophones et germanophone e.a.*) ter sprake. In deze uitspraak werd ook gerefereerd aan de waarborgen rondom de inzet van geautomatiseerde data-analyse.

Geautomatiseerde data-analyse door telecomproviders op verzoek de nationale autoriteiten wordt als een zwaar middel gezien:

> *"Moreover, the interference resulting from the automated analysis of traffic and location data, such as that at issue in the main proceedings, is particularly serious since it covers, generally and indiscriminately, the data of persons using electronic communication systems (-) In addition, such automated analysis is applied generally to all persons who use electronic communication systems and, consequently, applies also to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with terrorist activities."* [161]

[161] HvJEU 6 oktober 2020, (*Quadrature du Net and others*), r.o. 172-174.

Vanwege de kans op schending van privacyrechten kan de inzet van deze vorm van geautomatiseerde analyse alleen maar plaatsvinden in situaties:

> "*in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding.*"[162]

Daarnaast moeten de modellen en criteria die ingezet worden voor de analyse onder andere voldoen aan de eisen van betrouwbaarheid.[163]

Omdat het in voorliggende zaak specifiek gaat om wetgeving met betrekking tot activiteiten van telecomproviders, die onder het bereik van de EU-privacy en elektronische communicatierichtlijn (2002/58/EG) vallen, heeft het Hof zich naar het oordeel van de Evaluatiecommissie in deze uitspraak niet uitgelaten over eisen met betrekking tot geautomatiseerde data-analyse die wordt uitgevoerd door de Nederlandse inlichtingen- en veiligheidsdiensten zelf.

Voordat de diensten nieuwe technische functionaliteiten, zoals bijvoorbeeld gezichtsherkenning, ontwikkelen voor de toepassing van GDA+, moet de betrokken minister hiervoor toestemming geven. In deze toestemmingsaanvraag wordt aangegeven ten behoeve van welke soort onderzoeken deze wordt gedaan. Ook wordt een omschrijving gegeven van de werking en het doel van de beoogde functionaliteit en het type gegevens dat daarbij wordt gebruikt.[164] De CTIVD wordt van een gegeven toestemming op de hoogte gebracht. Zo kan de CTIVD al vanaf de ontwikkeling van een nieuwe functionaliteit toezicht houden. De CTIVD houdt deels al toezicht op de ontwikkeling van zulke nieuwe functionaliteiten en heeft daarover in de vierde voortgangsrapportage reeds aanbevelingen gedaan.[165]

Daarnaast houdt de CTIVD toezicht op toepassing van GDA+ in de praktijk. Bij het ontwerp en de ontwikkeling van de functionaliteit wordt daarom door de diensten al rekening gehouden met het technisch faciliteren van het toezicht door de CTIVD.

Aanbeveling 18

Voor het ontwikkelen van nieuwe technische functionaliteiten ten behoeve van GDA+ moet de betrokken minister vooraf toestemming geven. Als deze toestemming wordt gegeven, dan wordt de CTIVD daarvan op de hoogte gebracht.

[162] Ibidem, rule nr. 2.
[163] Ibidem, r.o. 179.
[164] Door de afbakening van GDA+ is het aanduiden van de te betrekken gegevensbestanden vereenvoudigd (zie §5.2.2).
[165] CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 16.

Combinatie toegangs- en handelingswaarborgen

In het hierboven beschreven systeem werken de handelingswaarborgen voor GDA+ en de toegangswaarborgen op gegevensverwerking onafhankelijk van elkaar. Gegevensverwerking die volgt uit artikel 1, onder f, wordt omkleed met extra toegangswaarborgen wanneer het gaat om verwerking van bulkdata. Deze extra toegangswaarborgen volgen uit de *aard* van de gegevens, namelijk bulkdata. Wanneer het gaat om gegevensverwerking GDA+, wordt deze gegevensverwerking omkleed met extra handelingswaarborgen, vanwege de gevoeligheid van de *handeling*. De toepassing van GDA+ op bulkdata ligt evident het meest gevoelig. In dat scenario gelden extra toegangswaarborgen (vanwege bulkdata) én extra handelingswaarborgen (vanwege GDA+). In onderstaande tabel wordt dit schematisch weergegeven.

	Niet-bulkdata	**Bulkdata**
Gegevensverwerking artikel 1, onder f	Standaard waarborgen (algemene bepalingen gegevensverwerking)	Toegangswaarborg
Gegevensverwerking GDA+	Handelingswaarborg	Toegangswaarborg én Handelingswaarborg

5.6 Conclusie

Grootschalige gegevensverwerking is een kernactiviteit van de diensten. GDA is in de Wiv 2017 opgenomen om de diensten een grondslag te bieden voor het doen van geavanceerde vormen van gegevensverwerking. Omdat de toepassing hiervan op OOG-metadata als extra gevoelig werd gezien, zijn daarvoor waarborgen in het leven geroepen: om GDA te verrichten met OOG-metadata moet vooraf toestemming gevraagd worden aan de minister, getoetst door de TIB.

Aangezien deze waarborg op OOG-metadata de enige waarborg op het verwerken betrof, is er in de zoektocht naar een gemeenschappelijk wettelijk kader een situatie ontstaan waarin het begrip GDA uiteindelijk vrijwel elke vorm van gegevensverwerking omvat. De discussie hierover tussen de minister en de diensten enerzijds en de TIB en CTIVD anderzijds is vastgelopen. Dit rapport doet een voorstel om uit deze situatie te geraken.

De Evaluatiecommissie beveelt aan om een specifiek omschreven categorie gegevensverwerking, GDA+, te introduceren. GDA+ komt in de plaats van het oorspronkelijke GDA begrip en moet worden voorzien van extra handelingswaarborgen: voor het ontwikkelen van nieuwe technische functionaliteiten ten behoeve van GDA+ moet de betrokken minister vooraf toestemming geven en de CTIVD kan op de ontwikkeling en de toepassing systeemtoezicht houden.

6 OOG-interceptie

6.1 Inleiding

De belangrijkste modernisering in de Wiv 2017 is de introductie van OOG-interceptie van communicatie via de kabel (zie §2.2).[166] Onder de Wiv 2002 was OOG-interceptie (destijds 'ongerichte interceptie' genoemd) alleen toegestaan op de ether (niet-kabelgebonden telecommunicatie). De Wiv 2017 bepaalt voor beide vormen van interceptie, via ether en kabel, dat dit niet volledig ongericht plaatsvindt, maar aan de hand van onderzoeksopdrachten. Daarom wordt gesproken van 'onderzoeksopdrachtgerichte' interceptie. Kabelinterceptie (door critici van deze nieuwe bevoegdheid 'sleepnet' genoemd) heeft in de aanloop naar de inwerkingtreding van de wet in het middelpunt van de maatschappelijke en politieke belangstelling gestaan.

In dit hoofdstuk wordt kort ingegaan op de totstandkoming en implementatie van OOG-interceptie op de kabel door de diensten. Het stelsel voor OOG-interceptie (zowel kabel als ether) wordt besproken en de Evaluatiecommissie formuleert enige praktische aanbevelingen ter verbetering.

6.2 Introductie van kabelinterceptie

De introductie van kabelinterceptie vloeide voort uit de aanbevelingen van de commissie Dessens. In haar rapport werd geconcludeerd dat de interceptiebepalingen in de Wiv 2002 vanwege de voortschrijdende technologische ontwikkelingen "anno 2013 te weinig recht deden aan de noodzakelijke bevoegdheden in het kader van de nationale veiligheid".[167] Steeds meer communicatie verplaatste zich naar het internet via de kabel, waardoor de diensten grote hoeveelheden potentieel waardevolle informatie misten.

Kabelgebonden en niet-kabelgebonden

De Wiv 2017 maakt OOG-interceptie mogelijk van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk (artikel 48, lid 1). In de praktijk wordt het onderscheid gemaakt tussen kabelgebonden en niet-kabelgebonden (ether) telecommunicatie. Waar hebben we het dan over?

Telecommunicatie verloopt ofwel via de lucht ofwel via de kabel. De communicatie via de lucht wordt ook wel etherverkeer genoemd. Een voorbeeld hiervan is communicatie door middel van geostationaire satellieten zoals telefonie- of berichtenverkeer, maar ook internetverkeer. Deze communicatie vindt plaats in de SHF (*Super High Frequency*) band en wordt door de diensten onder meer met behulp van het grondstation in Burum geïntercepteerd.[168]

[166] Interceptie op de kabel mocht onder de Wiv 2002 alleen als dit kon op basis van een enkel kenmerk (gerichte interceptie).
[167] Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*. p. 78.
[168] CTIVD. (2019). *Toezichtsrapport 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD*. p. 9.

Een ander voorbeeld van etherverkeer van belang voor de diensten zijn *High Frequency* (HF)-berichten die worden verzonden via radiozenders. HF-verkeer wordt doorgaans niet gebruikt door burgers, maar door overheden, diplomatieke instellingen en militaire organisaties. De interceptie van HF-verkeer vindt voornamelijk plaats in Eibergen.[169]

Daarnaast is er telecommunicatie via de kabel. Het overgrote deel van het wereldwijde internetverkeer wordt afgehandeld via kabels, waaronder onderzeese kabels tussen continenten. Veel communicatie heeft zich afgelopen jaren vanwege de kosten en beschikbare capaciteit naar de kabel verplaatst.

In reactie op deze aanbevelingen van de commissie Dessens besloot het kabinet tot de introductie van een nieuw uniform en techniekonafhankelijk interceptiestelsel waarbij kabelinterceptie mogelijk zou worden. Dit stelsel zou drie fases gaan bevatten: verwerving, voorbewerking (wat nu *searchen* wordt genoemd, zie §4.4.2 en §6.3) en verwerking. Binnen elke fase gelden versterkte waarborgen zoals ministeriële toestemming, bewaar- en vernietigingstermijnen en functie- en taakscheiding. Om toegang mogelijk te maken, geldt voor kabelinterceptie een medewerkingsplicht voor aanbieders van communicatiediensten.[170] Zoals toegelicht in §2.1 volgde er veel kritiek op het wetsvoorstel en met name op de bevoegdheid tot kabelinterceptie. Zowel de noodzakelijkheid van onderzoeksopdrachtgerichte kabelinterceptie als de daarbij voorgestelde waarborgen werden bekritiseerd. Er is vervolgens veel gewijzigd in het wetsvoorstel, onder meer door de TIB te introduceren, maar het interceptiestelsel zelf is grotendeels gelijk gebleven.[171] Het raadgevend referendum leidde uiteindelijk niet alleen tot de invoering van het gerichtheidsvereiste maar ook tot een veranderde bewaartermijn voor OOG-data. De bewaartermijn van drie jaar voor gegevens verkregen uit kabelinterceptie werd onderverdeeld in drie termijnen van één jaar, die per jaar verlengd mogen worden.[172]

6.3 OOG-interceptie in de wet

De wettelijke basis voor OOG-interceptie (kabel en ether) is artikel 48. De diensten kunnen op basis van dit artikel een toestemmingsaanvraag indienen voor interceptie ten behoeve van een bepaalde onderzoeksopdracht. Na ministeriële goedkeuring en een rechtmatigheidstoets door de TIB mag er vervolgens een jaar lang geïntercepteerd worden. Dit moet zo gericht mogelijk gebeuren. Dit houdt onder meer in dat de diensten voor het intercepteren van SHF-verkeer van geostationaire satellieten een bepaalde satelliet kiezen en daarbinnen een frequentieband. Alles wat daarbuiten valt, wordt niet geïntercepteerd. Vervolgens wordt er filtering toegepast op de geïntercepteerde gegevens. Voor kabelinterceptie geldt grofweg dezelfde systematiek: De diensten kiezen voor een bepaalde accesslocatie bij een aanbieder van een communicatiedienst en vervolgens voor een bepaalde fiber.

Artikel 49 biedt de diensten de mogelijkheid om de geïntercepteerde gegevens te doorzoeken (*searchen*) ten behoeve van optimalisatie van de interceptie én de selectie. Hierbij wordt bijvoorbeeld gekeken of inderdaad datgene wordt geïntercepteerd wat was beoogd en worden selectie-

[169] Ibidem.
[170] *Kamerstukken II* 2014/15, 33 820, nr. 4, p. 3-5 (Kabinetsstandpunt advies commissie Dessens).
[171] *Kamerstukken II* 2016/17, 34 588, nr. 4, p.40-43 (Advies Afdeling Advisering Raad van State en Nader Rapport).
[172] Beleidsregels Wiv 2017 van 25 april 2018, *Stcrt*, nr. 24397.

criteria geverifieerd en zo nodig bijgesteld. Voor beide vormen van *searchen* is ministeriële toestemming nodig die wordt getoetst door de TIB.

Artikel 50 vormt de basis voor het gebruiken van de gegevens voor het inlichtingenproces. Met selectie (artikel 50, lid 1) kunnen geïntercepteerde gegevens worden geselecteerd, oftewel betrokken in het inlichtingenproces, aan de hand van bepaalde criteria. De metadata uit OOG-interceptie kan rechtstreeks zonder selectie worden betrokken in GDA (artikel 50, lid 1, onder b) (zie hoofdstuk 5). Voor beide verwerkingsvormen geldt in de huidige wet de eis van ministeriële toestemming met TIB-toets.

Voor etherinterceptie zijn deze drie artikelen voldoende. De diensten hoeven voor deze vorm van interceptie niet aan te kloppen bij aanbieders van communicatiediensten, ze hebben immers hun eigen interceptiefaciliteiten zoals in Eibergen en Burum. Bij kabelinterceptie ligt dit anders. Hiervoor is medewerking nodig van een aanbieder van een communicatiedienst. Met artikel 52 kunnen de diensten voorbereidende informatie opvragen bij aanbieders van communicatiediensten die zij nodig hebben voor de inzet van gerichte én OOG-interceptie. Het gaat hierbij bijvoorbeeld om informatie over de netwerkarchitectuur en –topologie van een bepaalde provider, maar ook het soort telecommunicatie over bepaalde kabels.[173] Dit is informatie waar providers in het kader van hun eigen dienstverlening in principe al over beschikken.[174] Deze gegevens hebben de diensten nodig om kabelinterceptie überhaupt in te kunnen zetten. De wet verplicht aanbieders om deze informatie te geven. Voor de beantwoording van dit verzoek is echter geen termijn in de wet opgenomen.[175]

Wanneer de diensten weten bij welke aanbieder zij de kabelinterceptie willen inzetten, en zij hiervoor toestemming hebben, is de aanbieder verplicht om medewerking te verlenen (artikel 53).[176] Dan mogen de diensten een accesslocatie bouwen bij die aanbieder. In de praktijk blijkt deze opbouw ingewikkeld en vergt het hele proces de nodige tijd.

6.4 Implementatie van kabelinterceptie

Kabelinterceptie was een belangrijke reden om een nieuwe wet te maken. Toch hebben de diensten nog geen kabelinterceptie ingezet voor het inlichtingenonderzoek. De Evaluatiecommissie constateert, evenals de TIB en CTIVD[177], dat de implementatie van kabelinterceptie erg veel tijd blijkt te kosten. Voor zover mogelijk, gelet op de rubricering, gaat de Evaluatiecommissie in op de implementatie van kabelinterceptie. Dit is ook van belang vanwege de maatschappelijke en politieke aandacht die er is (geweest) voor deze nieuwe bevoegdheid.

De diensten hebben tijd nodig gehad voor de voorbereiding van kabelinterceptie. Naast het voorbereiden van de interne systemen bestond de eerste fase vooral uit het zoeken naar geschikte communicatieaanbieders. Hiervoor hebben de diensten informatie opgevraagd en

[173] *Stb.* 2018, nr. 116 (Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017).
[174] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 114 (MvT Wiv 2017).
[175] Met de Wiv 2017 is de reikwijdte van de medewerkingsverplichting groter geworden, zowel qua aanbieders (definitie is verbreed van 'telecomaanbieders' naar aanbieders van communicatiediensten) als qua situaties waarin de verplichting geldt (onder Wiv 2002 alleen bij gerichte interceptie en gerichte uitvraag, onder Wiv 2017 bij zowel gerichte als OOG-interceptie). Hierbij wordt verwezen naar artikel 13.2 van de Telecommunicatiewet (artikel 51 Wiv 2017).
[176] Deze bepaling geldt ook voor medewerking bij de uitvoering van gerichte interceptie als bedoeld in artikel 47, lid 1.
[177] Zie onder meer de TIB-jaarverslagen en de voortgangsrapportages van de CTIVD.

na enige tijd gekregen van verschillende aanbieders. In het najaar van 2018, ongeveer een half jaar na inwerkingtreding van de Wiv 2017, was een geschikte aanbieder gevonden en konden de diensten de eerste toestemmingsaanvragen voor kabelinterceptie (artikel 53 en artikel 48) schrijven. Eind 2018 gaf de minister toestemming voor deze aanvragen. De TIB beoordeelde deze toestemmingen vervolgens als onrechtmatig omdat die niet proportioneel en zo gericht mogelijk waren (zie §4.3.4).[178] Nieuwe toestemmingen zijn na aanvullende vragen in het voorjaar van 2019 door de TIB geclausuleerd goedgekeurd. Deze toestemmingen verschilden ten opzichte van de eerdere verzoeken in reikwijdte.[179]

Na het geclausuleerde rechtmatigheidsoordeel van de TIB konden de diensten de aanbieder benaderen en de technische realisatie van de accesslocatie starten. Dit proces duurde langer dan de diensten hadden verwacht. Met de desbetreffende aanbieder moest een plan van aanpak worden gemaakt en vergoedingen worden overeengekomen. Daarnaast dienden besluiten te worden genomen over de benodigde apparatuur en de bestelling, levering en installatie daarvan. Het opstellen van een plan inclusief implementatie voor het transport van geïntercepteerde data van aanbieder naar de diensten vergde eveneens tijd. Voor zowel de diensten als de aanbieder was dit allemaal nieuw terrein. Eind 2019 is deze fase afgerond en konden de eerste opnamen worden gemaakt bij de aanbieder. Deze opnamen waren niet ten behoeve van het inlichtingenproces, maar om de kabelinterceptie technisch te optimaliseren.

Begin 2020 zijn goedgekeurde verlengingsaanvragen voor kabelinterceptie door de TIB als onrechtmatig beoordeeld. Dit zag op de wijze van toepassing van filtering. Vervolgens zijn nieuwe aanvragen ingediend en als rechtmatig beoordeeld door de TIB. De Evaluatiecommissie heeft begrepen dat de gegevens die hiermee zijn verworven, op het moment van de afronding van de evaluatie, twee-en-een-half jaar nadat de wet van kracht is geworden, nog niet voor het inlichtingenproces worden gebruikt. Voor een deel kan deze lange periode verklaard worden door eenmalige aanloopmoeilijkheden. De vertraging hangt ook samen met de knelpunten besproken in hoofdstuk 4 en 9 (waaronder de interpretatie van het gerichtheidsvereiste).

De systematiek van etherinterceptie is gedurende de implementatieperiode van kabelinterceptie grondig gewijzigd. Dit gebeurde naar aanleiding van aanbevelingen van de CTIVD in verschillende rapporten over OOG-interceptie.[180] De wijziging van de systematiek voor etherinterceptie, waaronder met name de wijze van filtering, had ook effect op de implementatie van kabelinterceptie. De systematiek van etherinterceptie werd namelijk zoveel mogelijk gespiegeld aan kabelinterceptie. Ook dit heeft tijd gekost. Uiteindelijk heeft dit er volgens de CTIVD toe geleid dat de diensten voldoende zijn voorbereid op kabelinterceptie ten behoeve van het inlichtingenonderzoek.[181]

[178] TIB. (2019). *Jaarverslag 2018-2019*. p. 2, 13-14.
[179] TIB. (2019). *Jaarverslag 2018-2019*. p. 14.
[180] Zie hiervoor de verschillende voortgangrapportages alsook CTIVD toezichtsrapporten nummers 63 en 64.
[181] CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 14-15.

6.5 Knelpunten en aanbevelingen OOG-stelsel

De Evaluatiecommissie constateert dat het stelsel van OOG-interceptie zoals dat in de Wiv 2017 staat voor verbetering vatbaar is. Het gaat voor een groot deel om verbetering van de codificering omdat gebleken is dat de formuleringen in de wet niet goed aansluiten op de praktijk. Daarom doet de Evaluatiecommissie de onderstaande praktische aanbevelingen tot verbetering van het stelsel. Bij deze aanpassingen blijven de waarborgen die gelden voor OOG-interceptie onveranderd.

6.5.1 Metingen op de kabel

Voor de onderbouwing van de gerichtheid van de inzet van kabelinterceptie in de toestemmingsaanvraag moeten de diensten een inschatting maken van de aard, herkomst en bestemming van de te intercepteren verkeersstromen. De diensten hebben dit inzicht voorafgaand aan de inzet van interceptie echter nog niet in detail. Zij beschikken wel over relevante informatie, bijvoorbeeld de netwerkarchitectuur (verkregen op basis van artikel 52), maar zij kunnen voorafgaand aan interceptie niet meten hoe de gegevensstromen er precies uitzien en wat erin zit. Waar artikel 52 bedoeld was om aan de benodigde informatie te komen, is in de praktijk gebleken dat hiermee onvoldoende inzicht in de daadwerkelijke gegevensstromen wordt verkregen.

De diensten mogen pas kijken in deze stromen nadat er toestemming is verleend voor de interceptie. De diensten zijn daarom aangewezen op 'indirecte' informatie. Het gebrek aan deze metingsinformatie vormt een knelpunt bij de onderbouwing voor de inzet van interceptie (artikel 48) alsmede bij de aanvraag om een accesslocatie te creëren bij een bepaalde aanbieder (artikel 53). De diensten kiezen nu voor een bepaalde locatie, op basis van beperkt inzicht. Het realiseren van zo'n accesslocatie is een langdurige en strategische investering, zoals blijkt uit de implementatie van kabelinterceptie tot nu toe. Het ontbreken van metingsinformatie voorafgaand aan zo'n belangrijke keuze doet volgens de Evaluatiecommissie geen recht aan het belang van zorgvuldigheid, juist waar het een verstrekkend middel als kabelinterceptie betreft.

Een toestemmingsaanvraag voor het realiseren van een accesslocatie zou volgens de Evaluatiecommissie bovendien niet moeten worden gekoppeld aan een specifieke interceptieaanvraag, zoals de wet nu voorschrijft. In de praktijk is de realisatie van een locatie een langlopend traject, en zo lang dat traject loopt kan nog niet daadwerkelijk worden geïntercepteerd voor het inlichtingenonderzoek. Bovendien suggereert de koppeling dat de acceslocatie voor één interceptieaanvraag wordt gebruikt. In de praktijk zal een accesslocatie worden gebruikt voor meerdere onderzoeken.

De Evaluatiecommissie doet dan ook de aanbeveling om de realisatie van een accesslocatie (artikel 53) en de inzet van kabelinterceptie (artikel 48) los te koppelen. Daarnaast beveelt de Evaluatiecommissie aan om de wettelijke mogelijkheid te creëren om korte metingen uit te voeren bij verschillende aanbieders van communicatie. Dit is een tussenstap die voorafgaand aan de inzet van artikel 53 plaatsvindt.

Deze meting gaat verder dan de huidige wettelijke mogelijkheid van artikel 52 om informatie op te vragen. De meting moet immers inzicht geven in de gegevensstromen die zich op de kabel bevinden. Metingsinformatie zorgt ervoor dat de diensten beter doordacht een keuze kunnen maken én een betere invulling kunnen geven aan het gerichtheidsvereiste. Hierbij is het van belang om te benadrukken dat deze meting *alleen* is bedoeld om het plaatsen van een acceslocatie en/of de daadwerkelijke interceptie te optimaliseren. De meting dient dan ook

door specifieke (technische) functionarissen te worden uitgevoerd die op afstand staan van het inlichtingenonderzoek (zie §4.4.3). De gegevens uit deze meting komen niet ter beschikking voor het inlichtingenonderzoek en worden na afloop van de meting vernietigd.

Hiermee komt het systeem voor kabelinterceptie er als volgt uit te zien:

Stap 1:	Artikel 52 om informatie op te halen bij verschillende aanbieders
Stap 2 (nieuw):	Artikel '52 a' om metingen te doen bij bepaalde aanbieders
Stap 3:	Artikel 53 voor bouwen van een accesslocatie bij één van de aanbieders
Stap 4:	Artikel 48 ten behoeve van bepaald onderzoek

Net als het realiseren van een acceslocatie (artikel 53) en de inzet van kabelinterceptie (art. 48) vergt de inzet van artikel '52 a' toestemming op ministerieel niveau en toetsing door de TIB. Deze goedkeuring zou dan voor een termijn van bijvoorbeeld drie maanden gelden waarbinnen de diensten in staat zijn metingen te verrichten bij de desbetreffende aanbieders.

Aanbeveling 19

Koppel artikel 53 los van artikel 48 en introduceer een artikel '52 a' waarmee de diensten metingen kunnen doen bij bepaalde aanbieders.

Het is in de praktijk een knelpunt gebleken dat artikel 52 niet voorziet in een termijn voor de verstrekking van informatie door een aanbieder. Dit zorgt voor onduidelijkheid voor alle betrokken partijen en levert vertraging op. De Evaluatiecommissie beveelt daarom aan in de wet een termijn op te nemen waarbinnen de aanbieders van communicatiediensten aan deze medewerkingsplicht moeten voldoen. Hierbij kan worden gedacht aan de termijn van vier weken.

Aanbeveling 20

Voorzie de verplichting van artikel 52 van een termijn van vier weken.

6.5.2 Search gericht op interceptie

In het nieuwe voorgestelde bulkverwerkingsregime – waar ook OOG-data onderdeel van uitmaakt – wordt de huidige bevoegdheid om selectie te optimaliseren via search gericht op selectie (art. 49, lid 2) verbreed naar alle bulkdata (zie §4.4.5). Deze bevoegdheid geldt daarmee niet alleen meer voor OOG-interceptie. Dit is anders voor de andere *search*-variant, namelijk *search* gericht op interceptie (art. 49, lid 1), waarbij geïntercepteerde OOG-data wordt doorzocht om de interceptie te optimaliseren. Hierbij wordt het geïntercepteerde verkeer bekeken om te controleren of er wordt geïntercepteerd wat beoogd was.[182] Deze bevoegdheid is dan ook sterk gekoppeld aan de inzet van interceptie. Het ligt daarom in de rede om deze vorm van search op te nemen in de wettelijke bepaling van artikel 48.

[182] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 104 (MvT Wiv 2017).

Aanbeveling 21

Voeg *search* gericht op interceptie toe aan de huidige wettelijke bepaling voor de interceptiebevoegdheid.

6.5.3 Uitzondering voor interceptie van HF-verkeer

Met etherinterceptie wordt ook HF-verkeer onderschept. Zoals al aangegeven wordt deze vorm van communicatie doorgaans door overheden, diplomatieke instellingen en (para)militaire organisaties gebruikt. Het bevat dus vrijwel geen (privé)communicatie van burgers.[183] Het is vooral de MIVD die HF-verkeer intercepteert, vanwege het gebruik van HF door militaire actoren. Ondanks dat de mate van inbreuk op de privacy van burgers dus zeer beperkt is, is HF-verkeer als onderdeel van het OOG-stelsel onderworpen aan dezelfde strenge waarborgen als voor de meer inbreukmakende kabel- en SHF-interceptie.

Bij gerichte interceptie wordt wel een onderscheid gemaakt tussen interceptie van militair en niet-militair verkeer. Ministeriële toestemming en de toets door de TIB gelden niet "voor zover het gericht ontvangen en opnemen van telecommunicatie die zijn oorsprong of bestemming heeft in andere landen betrekking heeft op militair verkeer" (artikel 47, lid 8). In dat geval is toestemming van het hoofd van de MIVD voldoende.[184] Dit onderscheid stamt uit de Wiv 2002 (artikel 25, lid 8) en is op vergelijkbare wijze opgenomen in de huidige wet. Echter, alleen ten aanzien van gerichte interceptie. Voor OOG-interceptie van militair HF-verkeer geldt in de wet nog altijd de eis van ministeriële toestemming die wordt getoetst door de TIB. Waar de Evaluatiecommissie deze waarborgen zeer passend vindt voor kabel- en SHF-interceptie waarbij er sprake is van mogelijke inbreuk op de privacy van (wereld)burgers, zijn deze waarborgen te zwaar voor de interceptie van militair HF-verkeer. De Evaluatiecommissie beveelt daarom aan ook in de wettelijke bepaling voor OOG-interceptie een soortgelijke uitzondering voor militair HF-verkeer te maken als bij gerichte interceptie.

Aanbeveling 22

Maak in de wettelijke bepaling voor OOG-interceptie een uitzondering voor militair HF-verkeer, net als bij gerichte interceptie.

[183] CTIVD. (2019). *Toezichtsrapport 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD*. p. 9.
[184] Tenzij medewerking van een aanbieder van een communicatiedienst is vereist, in dat geval moet de minister wel toestemming geven.

6.6 Conclusie

De mogelijkheid om te kunnen intercepteren op de kabel was de belangrijkste modernisering van de Wiv 2017. Het is sinds de introductie van deze wet, nu ruim twee jaar geleden, de diensten nog niet gelukt deze bevoegdheid in zijn volledigheid in te zetten. Dat komt vooral doordat OOG-interceptie op de kabel technisch, juridisch en organisatorisch een complexe en bovendien nieuwe bevoegdheid is. Ook het ontwikkelen van een gemeenschappelijk begrippenkader waardoor voor alle stappen in het OOG-stelsel toestemming kon worden gevraagd én kon worden getoetst, vergt kennelijk de nodige inspanningen.

De belangrijkste aanbevelingen in dit hoofdstuk betreffen het stroomlijnen, optimaliseren en soms repareren van het oorspronkelijke OOG-stelsel. Er worden geen fundamentele wijzigingen voorgesteld en de oorspronkelijke waarborgen blijven intact.

De aanbevelingen stellen de diensten in staat om op basis van metingen een geschikte accesslocatie uit te zoeken. Dit komt de gerichtheid van de inzet van het middel ten goede en doet meer recht aan het strategische karakter van een accesslocatie. Ook de eventuele toestemmingsaanvraag voor interceptie is door de metingen beter te onderbouwen en te toetsen. Daarnaast wordt aanbevolen om artikel 52 van een termijn te voorzien waarbinnen de aanbieders van communicatiediensten een informatieverzoek moeten beantwoorden. Tenslotte wordt er een aanbeveling gedaan om in de wettelijke bepaling voor OOG-interceptie een uitzondering te maken op de eis van ministeriële toestemming en toets door de TIB voor interceptie van militair HF-verkeer.

7 De hackbevoegdheid

7.1 Inleiding

Artikel 45 uit de Wiv 2017 maak het mogelijk voor de diensten om 'geautomatiseerde werken' binnen te dringen. Deze bevoegdheid wordt ook wel de 'hackbevoegdheid' genoemd (zie kader). Met de hackbevoegdheid kan op afstand of door direct contact controle worden verkregen over (een deel van) een computer. De term computer kan breed worden opgevat. Veel objecten en apparaten beschikken immers over een computerfunctionaliteit. Hierbij kan gedacht worden aan een mobiele telefoon of een webserver, maar ook horloges of auto's kunnen steeds meer als een computer worden gezien.

Hacken

Artikel 45 wordt vaak geduid als de 'hackbevoegdheid', maar strikt genomen is dit niet correct. Hacken is een onderdeel van artikel 45, maar artikel 45 is breder dan dat. Naast het binnendringen zelf gaat artikel 45 namelijk ook over het verkennen van een geautomatiseerd werk en over het overnemen van gegevens. Bovendien is 'hacken' normaal gesproken illegaal, want er wordt immers een geautomatiseerd werk binnengedrongen van iemand anders. Voor de diensten is de inzet van de hackbevoegdheid echter onder omstandigheden wel wettelijk toegestaan. Omwille van leesgemak zal in de rest van dit hoofdstuk de term 'hacken' of 'hackbevoegdheid' gebruikt worden als verwijzing naar artikel 45.

De hackbevoegdheid is, mede gezien de ontwikkelingen zoals geschetst in hoofdstuk 3, van groot belang voor de diensten. Interstatelijke spanningen en conflicten kennen een steeds grotere digitale component, waarbij informatietechnologie wordt gebruikt voor spionage en sabotage. Dit wordt deels gevoed door de toenemende omvang en complexiteit van datastromen en opslag. Bovendien worden communicatiestromen steeds beter versleuteld, ook door non-statelijke actoren, waardoor de noodzaak voor de diensten toeneemt om bij apparaten waar die communicatie wordt verzonden of ontvangen – en dus ontsleuteld – binnen te kunnen dringen.

7.2 De hackbevoegdheid in de Wiv 2017

7.2.1 Inleiding

De hackbevoegdheid van artikel 45 is geen nieuwe bevoegdheid; deze bestond ook in de Wiv 2002 onder artikel 24. Wel is een aantal deelaspecten van de bevoegdheid expliciet in de Wiv 2017 geformuleerd. Zo is de mogelijkheid om toegang te krijgen tot een computer via een 'derde' wettelijk vastgelegd. Hiermee kunnen de diensten de computer van een derde partij binnendringen om vervolgens 'door te stappen' naar het *target*. In de Wiv 2017 is ook vastgelegd dat de diensten op een computer software mogen installeren om iemand te kunnen observeren, bijvoorbeeld door de camera of microfoon te activeren. Verder is de bevoegdheid om geautomatiseerde werken te 'verkennen' een expliciete bevoegdheid geworden.

De hackbevoegdheid is een verstrekkende bevoegdheid die een grote inbreuk op de privacy met zich mee kan brengen. Bovendien kan de inzet van de hackbevoegdheid, bijvoorbeeld door het verzwakken van beveiliging of door het gebruik van onbekende kwetsbaarheden, mogelijk tot nevenschade leiden (zie het kader over *zerodays* hierna). De commissie Dessens constateerde al dat de hackbevoegdheid uit de Wiv 2002 "in potentie niet minder indringend" was dan de

interceptiebevoegdheid.[185] Daarom is het toestemmingsniveau voor de inzet van de hackbevoegdheid in de Wiv 2017 verhoogd naar de betrokken minister, wiens toestemming door de TIB op rechtmatigheid wordt getoetst.

Onbekende kwetsbaardheden (*zerodays*)

Een onbekende kwetsbaarheid is een kwetsbaarheid in een geautomatiseerd werk die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen. Van deze kwetsbaarheid kan worden verondersteld dat deze niet bekend is bij de producent of leverancier.[186] Er is een grote variëteit in *zerodays*. De meest beruchte zijn ook meteen de meest zeldzame. Het gaat bij de bekende zaken om kwetsbaarheden in Windows waarmee een gebruiker op afstand, zonder al te veel moeite, een systeem kan overnemen. In de praktijk gaat het echter ook om programmeerfouten in simpele software, of verouderde software die maar op enkele plekken wordt gebruikt. Vaak spelen lokale omstandigheden op de systemen een rol bij het kunnen toepassen van die *zeroday*. De technische en operationele verscheidenheid van *zerodays* speelt zich af tussen deze uitersten.

Het gebruik van onbekende kwetsbaarheden is onderwerp van een maatschappelijke discussie die vooral gaat over conflicterende *belangen*. Enerzijds het belang van een goedwerkende en veilige ICT-infrastructuur waar de overheid en de samenleving op kan vertrouwen en anderzijds het belang om in bepaalde gevallen als overheid deze kwetsbaarheden zelf te gebruiken wanneer nodig voor de nationale veiligheid. De kern van de zaak is de *weging* van deze belangen. Deze afweging wordt besproken in de toelichting op de Wiv 2017, maar de wet geeft voor deze afweging geen nader kader.[187]

In 2015 heeft de CTIVD onderzoek gedaan naar de inzet van de hackbevoegdheid door de diensten.[188] Aan de hand van aanbevelingen in dit rapport hebben de diensten beleid ontwikkeld over hoe om te gaan met onbekende kwetsbaarheden.[189]

Over het onderwerp *zerodays* ligt op dit moment een initiatiefwetsvoorstel voor in de Tweede Kamer. In het debat over deze wet is sprake geweest van een motie waarin deze Evaluatiecommissie zou worden gevraagd dit onderwerp ook mee te nemen in het onderzoek. Het wetsvoorstel en de motie zijn op het moment van het opstellen van dit rapport nog in behandeling in de Tweede Kamer. Daarom heeft de Evaluatiecommissie ervoor gekozen dit onderwerp niet verder te betrekken in haar onderzoek.

Met het oog op de door de Evaluatiecommissie waargenomen knelpunten bij artikel 45 is het van belang om allereerst drie elementen uit het artikel nader toe te lichten: verkennen, technische risico's en bijschrijven. Deze toelichting volgt hieronder, waarna de knelpunten en aanbevelingen worden uiteengezet.

---

[185] Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*. p. 83.
[186] Artikel 126fa Wetboek van Strafvordering zoals voorgesteld in kader CCIII.
[187] *Kamerstukken* II 2016/17, 34 588, nr. 3, p. 80 (MvT Wiv 2017).
[188] CTIVD. (2017). *Toezichtsrapport 53 over de inzet van de hackbevoegdheid door de AIVD en MIVD*.
[189] AIVD. (2018). *Beleid AIVD en MIVD over omgang met 'onbekende kwetsbaarheden*. **https://www.aivd.nl/documenten/publicaties/2018/05/01/beleid-omgang-met-onbekende-kwetsbaarheden**.

7.2.2 Verkennen

Voor een goede voorbereiding van een hackoperatie wordt een geautomatiseerd werk eerst verkend om een beeld te kunnen krijgen van de eigenschappen van het geautomatiseerde werk, zoals de geïnstalleerde software, aanwezige netwerkverbindingen en onderliggende hardware. Deze handeling is in artikel 45, lid 1, onder a, opgenomen als bijzondere bevoegdheid waarvoor de minister toestemming moet geven en die vervolgens door de TIB wordt getoetst. Bij het verkennen van een geautomatiseerd werk wordt deze niet binnengedrongen. Wel wordt van buitenaf gescand op belangrijke basiskenmerken zoals IP-adressen, toegangspoorten en andere technische eigenschappen. Deze informatie is in principe door iedereen te achterhalen, maar wel cruciaal om verder richting te geven aan de operatie. Volgens de toelichting op de wet heeft de bevoegdheid om te verkennen een 'ondersteunend karakter':

> "De door de AIVD en MIVD door middel van de inzet van de verkennende bevoegdheid verworven kenmerken, stellen de diensten aldus in staat in het belang van het onderzoek gericht, efficiënt en zorgvuldig in relevante geautomatiseerde werken binnen te dringen." [190]

7.2.3 Technische risico's

Het binnendringen van een geautomatiseerd werk kan andere gebruikers van datzelfde geautomatiseerde werk – of gebruikers van een ander geautomatiseerd werk dat gebruik maakt van hetzelfde soort hard- of software – blootstellen aan technische risico's. Hun computer zou in het ergste geval beschadigd of defect kunnen raken of gegevens zouden verloren kunnen gaan. In de toelichting op de wet zijn de technische risico's onderverdeeld in twee categorieën:

1. De risico's die bestaan doordat een geautomatiseerd werk bepaalde zwakheden kent. De diensten maken gebruik van deze zwakheden om het geautomatiseerde werk binnen te dringen. Dat betekent dat andere partijen dat eventueel ook zouden kunnen.
2. De risico's die ontstaan door handelingen van de diensten zelf. Mogelijk bevat het technisch hulpmiddel waarmee de diensten toegang behouden tot het geautomatiseerde werk, zelf kwetsbaarheden. Eventuele andere partijen zouden dan hiervan gebruik kunnen maken om ook toegang te krijgen tot het geautomatiseerde werk.[191]

Om een goede afweging te kunnen maken tussen het belang van nationale veiligheid en eventuele technische risico's, moeten de diensten deze risico's 'voor zover deze kunnen worden overzien' opnemen in de toestemmingsaanvraag.[192] Deze risico's worden meegewogen in de proportionaliteitstoets.

7.2.4 Bijschrijven

De diensten kunnen via artikel 45, lid 8, geautomatiseerde werken 'bijschrijven' op een eerdere goedgekeurde toestemmingsaanvraag, onder de voorwaarde dat deze tot hetzelfde *target* of derde behoren. Dit bijschrijven gebeurt op basis van technische kenmerken, zoals een IP-adres of een telefoonnummer. Zodra blijkt dat eenzelfde *target* gebruik maakt van bijvoorbeeld een nieuwe server of telefoon, kunnen de technische kenmerken van deze nieuwe geautomatiseerde werken zonder nieuwe toestemmingsaanvraag aan de bestaande aanvraag worden toegevoegd. Voor bijschrijven geldt daarmee geen nieuwe toets door de TIB.

---

[190] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 77 (MvT Wiv 2017).
[191] Ibidem. p. 80.
[192] Ibidem.

De toelichting op de wet schetst twee gevallen waarin bijschrijven mogelijk is: als een nieuw geautomatiseerd werk *in de plaats treedt* van een eerder geautomatiseerd werk, of als een *target aanvullend* gebruikmaakt van een nieuw geautomatiseerd werk.[193] Het bijschrijven van geautomatiseerde werken van *nieuwe* derden, zoals een nieuwe hostingprovider, mag niet. Dit wordt niet als een vervangend werk gezien, waardoor hiervoor opnieuw toestemming moet worden gevraagd.

Bijschrijven van derden

In bepaalde gevallen is het geautomatiseerde werk van *target* niet direct toegankelijk, maar is daarvoor technische informatie of connectiviteit benodigd die alleen bij een andere partij te vinden is. Het gaat hier dus om een partij die geen *target* is van de diensten: een zogenaamde 'non-*target*'. Het begrip 'derde' is hier een specifieke invulling van, namelijk de partij die diensten in staat stelt om überhaupt toegang te krijgen tot het geautomatiseerde werk van het uiteindelijke *target*. Via een derde kan worden doorgestapt naar het *target*, of door het binnendringen van een derde kunnen gegevens worden verworven die noodzakelijk zijn om vervolgens bij het *target* binnen te dringen.

Artikel 45, lid 8, maakt het mogelijk om een vervangend of aanvullend geautomatiseerd werk van een derde bij te schrijven als die derde bij de oorspronkelijke toestemmingsaanvraag is vermeld. Het bijschrijven van het geautomatiseerd werk van een *nieuwe* derde mag echter niet, omdat dit niet als een vervangend of aanvullend werk wordt gezien.

7.3 De hackbevoegdheid in de praktijk: knelpunten en aanbevelingen

7.3.1 Inleiding

Uit de evaluatie is een aantal knelpunten gebleken die samenhangen met de hackbevoegdheid. In algemene zin zijn twee zaken de Evaluatiecommissie opgevallen. Ten eerste lijkt de wet met betrekking tot de hackbevoegdheid redelijk te functioneren, maar is er een aantal specifieke tekortkomingen die om een wetswijziging vragen. Zo is gebleken dat het ministeriële toestemmingsniveau voor het vooraf verkennen van een geautomatiseerd werk te hoog is in relatie tot de inbreuk. Door het toestemmingsniveau voor verkennen intern bij de diensten te beleggen, is de verwachting dat de toestemmingsaanvragen voor het binnendringen van een geautomatiseerd werk beter en gerichter zullen zijn. Verder ontbreekt er een bijschrijfmogelijkheid bij artikel 54, waarmee de diensten gegevens op kunnen vragen bij aanbieders van telecommunicatie- en opslagdiensten. Deze punten werden zowel door de diensten als door de TIB onderschreven als gebreken in de wet. In dit hoofdstuk doet de Evaluatiecommissie specifieke aanbevelingen om de wet hierop aan te passen.

Ten tweede sluit artikel 45 op sommige punten niet meer aan bij de technische ontwikkelingen van de afgelopen jaren. Doorgaans wordt de hackbevoegdheid gericht ingezet op een geautomatiseerd werk van – of in gebruik bij – een *target*. Het bezit, gebruik of eigenaarschap van computers heeft echter de afgelopen jaren een grote verandering ondergaan, onder andere als het gaat om afnemers van clouddiensten, VPN-diensten of hostingproviders. Het hebben van een website op

[193] Ibidem. p. 81.

internet betekent niet dat het onderliggende systeem ook van één persoon is. Dit lijkt echter wel de gedachte te zijn geweest bij het formuleren van het artikel in de Wiv 2017. Juist bij dit soort gevallen blijkt het toepassen van de wet bij het vragen van toestemming en het toetsen daarvan minder evident, wat in de praktijk voor discussies zorgt. Om deze discussies in goede banen te leiden vindt de Evaluatiecommissie een wijziging van artikel 45 niet noodzakelijk. Wel moet de wetgever bij een aantal punten een nadere toelichting geven. In de volgende paragrafen zal hier verder op in worden gegaan.

7.3.2 Het knelpunt bij verkennen: toestemmingsniveau

De verkennende bevoegdheid is bedoeld om bij te dragen aan een gerichtere inzet van de hackbevoegdheid. De verkenningsbevoegdheid is echter als bijzondere bevoegdheid met dezelfde waarborgen omkleed als de aanvraag voor het daadwerkelijk binnendringen van het geautomatiseerde werk zelf. Hiervoor is toestemming vereist van de betrokken minister, met rechtmatigheidstoets door de TIB. In de praktijk blijkt daarom dat de diensten uit praktische overwegingen de verkennende bevoegdheid niet meer op zichzelf aanvragen, maar alleen gecombineerd met een aanvraag om een geautomatiseerd werk binnen te dringen. Daardoor wordt geen optimaal gebruikgemaakt van de verkenningsmogelijkheid.

In het licht van het bovenstaande constateert de Evaluatiecommissie dat het huidige toestemmingsniveau erg hoog is voor een relatief licht instrument met een zeer beperkte inbreuk op de privacy. Dit is onhandig geregeld in de wet. Over dit punt zijn zowel de diensten als de toezichthouders het eens. Daarom kan het toestemmingsniveau voor verkennen in de wet beter intern belegd worden bij de diensten. Deze wijziging draagt bij aan een gerichtere inzet van de hackbevoegdheid.

Aanbeveling 23

Beleg het toestemmingsniveau voor verkennen intern bij de diensten.

7.3.3 Afbakening technische risico's

In algemene zin overlapt het minimaliseren van de technische risico's met de operationele behoefte van de diensten om niet ontdekt te worden. De eis om voorafgaand aan de inzet van de hackbevoegdheid in detail een omschrijving te geven van de technische risico's staat echter op gespannen voet met de realiteit. Omdat vooraf nog weinig bekend is over de technische omgeving van het doelwit, is een sluitende omschrijving van risico's moeilijk te geven.[194] Door het beter gebruik maken van de verkennende bevoegdheid, waarvoor bovenstaande aanbeveling is gedaan, wordt een belangrijke stap gezet richting een beter onderbouwde risico-inschatting.

De verwachting is echter niet dat hiermee de huidige knelpunten rondom de omschrijving van technische risico's helemaal worden opgelost. Dit heeft te maken met de mate van (on)voorzienbaarheid. Zoals al beschreven is het allereerst doorgaans moeilijk om voorafgaand aan de inzet de risico's te beschrijven die gedurende de operatie naar boven zullen komen. Veel risico's worden namelijk pas gaandeweg duidelijk en zijn vooraf nog onbekend. Hier knelt de statische aard van de ex-ante toetsing met de dynamische aard van de operatie die daarop

[194] CTIVD. (2020). *Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. p. 16.

volgt. De toelichting op de wet lijkt hier wel aandacht voor te vragen door de voorzienbaarheid te noemen, maar dit wordt niet verder toegelicht. Tegelijkertijd ziet de wetgever terecht ook een belangrijke waarborg in een gedegen afweging van de technische risico's. Het is een dilemma hoe hier in de praktijk mee om te gaan.

De Evaluatiecommissie ziet een belangrijke waarborg in het omschrijven van technische risico's en het betrekken van deze risico's in de weging door de TIB. Hierbij moet wel rekening gehouden worden met de statische aard en inherente beperktheid van de ex-ante toets, zeker bij de veelal dynamische en complexe uitvoering van de hackbevoegdheid. De toelichting op de wet moet daarom uitleggen dat in bepaalde situaties, met name waar het eerste toestemmingsaanvragen voor nieuwe operaties betreft, een mindere mate van detail volstaat in de omschrijving van de technische risico's. Wanneer de diensten ervaringen hebben met (vergelijkbare) systemen, bijvoorbeeld bij een verlengingsaanvraag, kan een grotere mate van detail worden gegeven.

Aanbeveling 24

Bied in de toelichting op de wet meer ruimte voor differentiatie in de mate van detail van de omschrijving van de technische risico's voor de ex-ante toets door de TIB.

Daarnaast constateert de Evaluatiecommissie dat de TIB het vereiste van de omschrijving van de technische risico's in de praktijk soms breed interpreteert en de diensten vraagt om informatie die ziet op de manier waarop de diensten de bevoegdheid ten uitvoer brengen. Deze vragen kunnen verder strekken dan hetgeen noodzakelijk is voor een afweging van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid. Het gaat bijvoorbeeld om vragen als hoe de diensten de verkregen toegang tot een computer beveiligen. De Evaluatiecommissie begrijpt dat de TIB controleert *dat* deze toegang beveiligd wordt, maar *hoe* dit precies ten uitvoer wordt gebracht valt onder het dynamisch toezicht door de CTIVD. Ook vanwege de hierboven genoemde onvoorzienbaarheid van de hackbevoegdheid is het (dynamisch) toezicht door de CTIVD een geschiktere vorm van toezicht op de bestrijding van technische risico's dan de ex-ante TIB-toets. Hierdoor ontstaat geen verminderd toezicht op de uitvoering, maar wordt het zwaartepunt verschoven naar het dynamisch toezicht door de CTIVD. In §9.3 wordt verder ingegaan op de scheiding tussen de ex-ante toets op verwerving en het dynamisch toezicht op verwerking en een goede aansluiting daartussen.

7.3.4 Bijschrijven van derden

Zoals eerder toegelicht vragen de diensten toestemming aan de minister en de TIB als ze een geautomatiseerd werk van een *nieuwe* derde willen bijschrijven. Uit de praktijk blijkt echter dat actoren in een steeds hoger tempo wisselen van omgeving, bijvoorbeeld door continu te wisselen van hostingprovider. Omdat een dergelijke hostingprovider geldt als nieuwe derde moet opnieuw toestemming worden verkregen van de minister, getoetst door de TIB. De procedure om tot een nieuwe toestemming te komen kost relatief veel tijd, doorgaans meerdere weken, waardoor een *target* uit zicht van de diensten kan raken.

Om zicht te kunnen blijven houden op *targets* in het cyberdomein geven de diensten aan dat de wet meer mogelijkheden zou moeten bieden om sneller met een *target* mee te kunnen bewegen via een nieuwe derde, bijvoorbeeld door het wettelijk mogelijk te maken om nieuwe derden bij te schrijven op een bestaande last. De TIB ziet dit echter niet zozeer als een probleem van de

wet, maar verwijst hiervoor naar de mogelijkheid van een spoedprocedure zoals uiteengezet in artikel 37.

De reguliere toestemmingsprocedure voor het bijschrijven van nieuwe derden lijkt inderdaad te botsen met de vereiste snelheid in het cyberdomein. Tegelijkertijd mag de snelheid geen afbreuk doen aan de waarborgen. De bijzondere gevoeligheid van het hacken van een nieuwe derde blijft immers bestaan, omdat hiermee ook andere personen en organisaties kunnen worden geraakt die geen onderwerp van onderzoek van de diensten zijn. Vanwege deze gevoeligheid vindt de Evaluatiecommissie het belangrijk dat de TIB haar toetsende rol op aanvragen die zien op nieuwe derden blijft vervullen. Bovendien neemt in het totale tijdsbestek van een toestemmingsprocedure de TIB-toets een relatief beperkt aandeel in. Daarom moedigt de Evaluatiecommissie de diensten aan om ook aandacht te besteden aan het verkorten van de interne procedures voor toestemmingsverlening, met name voor het bijschrijven van nieuwe derden.

Als er desondanks gevallen bestaan waar een *target* uit zicht dreigt te raken door de duur van een toestemmingsprocedure, moedigt de Evaluatiecommissie de diensten aan om minder terughoudend te zijn in het gebruik van de spoedprocedure in deze specifieke situatie. Uit de toelichting op artikel 37 lijkt deze voldoende ruimte te bieden om de spoedprocedure te gebruiken voor cyberoperaties waarbij op zeer korte termijn gehandeld moet worden.[195] Met behulp van deze spoedprocedure zou een nieuwe derde direct na toestemming van de minister bijgeschreven kunnen worden, waarna deze toestemming zo spoedig mogelijk aan de TIB wordt voorgelegd. De TIB kan vervolgens de rechtmatigheid van de toestemming toetsen en of er terecht is gekozen voor een spoedprocedure. Als de toestemming rechtmatig is, maar de spoedprocedure ten onrechte is gebruikt, bepaalt de TIB wat er moet gebeuren met de eventueel verworven gegevens.[196]

7.3.5 Exclusiviteitsvereiste

Artikel 45, lid 8, maakt het mogelijk om geautomatiseerde werken bij te schrijven indien zij in plaats treden van of een aanvulling zijn op het werk waar de toestemmingsaanvraag oorspronkelijk op zag. De bepaling wordt niet verder uitgelegd. Ter invulling van deze bepaling heeft de TIB via een gerubriceerde brief een eigen bovenwettelijk 'exclusiviteitsvereiste' geïntroduceerd. Alleen als een geautomatiseerd werk *uitsluitend* gebruikt wordt door het *target* of de derde waarop de initiële aanvraag gericht was, mag dit werk worden bijgeschreven volgens de TIB. Als dit niet het geval is, moet voor het hacken van dit geautomatiseerde werk toestemming worden gevraagd aan de minister, getoetst door de TIB.

De diensten hebben aangegeven het in de praktijk steeds lastiger is te voldoen aan dit exclusiviteitsvereiste en dat het een belemmerend effect heeft. De toelichting op de bijschrijfmogelijkheid lijkt bij het begrip 'gebruik maken van' vooral uit te gaan van het gebruik van een *fysiek* systeem, terwijl er een trend is waarin particulier eigendom van een fysieke computer steeds meer plaats maakt voor het gebruik van *virtuele* computers op gedeelde servers.[197] Deze virtuele computers kunnen bijvoorbeeld qua functionaliteit in exclusief gebruik zijn, maar omdat ze draaien op een fysieke infrastructuur die in bezit is van een andere partij (met meerdere gebruikers) is niet duidelijk of het bijschrijven hier van deze virtuele computers voldoet aan het exclusiviteitsvereiste.

[195] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 54 (MvT Wiv 2017).
[196] Volgens het TIB jaarverslag 2019-2020 waren 3,3% van de AIVD-aanvragen en 1,6% van de MIVD-aanvragen dat jaar een spoedaanvraag. Zie: TIB. (2020). *Jaarverslag 2019-2020*. p. 19.
[197] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 81 (MvT Wiv 2017).

Met het oog op de genoemde verschillende standpunten van de diensten en de TIB aarzelt de Evaluatiecommissie of het exclusiviteitsvereiste realistisch is bij de technologische ontwikkelingen. Artikel 45, lid 8, biedt weinig duidelijkheid over de vraag wanneer een geautomatiseerd werk 'in gebruik is' van een actor, terwijl daaraan wel behoefte bestaat. De toelichting moet hierover meer handvatten bieden, waarbij aandacht wordt besteed aan de vraag wanneer een fysiek dan wel virtueel geautomatiseerd werk 'in gebruik is' van een actor.

Aanbeveling 25

Bied in de toelichting bij artikel 45, lid 8, een werkbare uitleg wanneer een geautomatiseerd werk 'in gebruik is' van een actor.

7.3.6 Bijschrijven bij artikel 54

Aanvullend op artikel 45 is ook artikel 54 relevant voor digitaal onderzoek. Hiermee kunnen gegevens zoals *disk images* opgevraagd worden bij aanbieders van telecommunicatie- en opslagdiensten, indien is vastgesteld dat een *target* gebruikmaakt van de dienstverlening van dat bedrijf. Artikel 54 geeft de bevoegdheid voor een eenmalige inzet. Deze bevoegdheid wordt gezien als minder indringend dan een hackoperatie uit artikel 45, omdat bij artikel 54 de aanbieder van een telecommunicatie- en opslagdienst vooraf wordt geïnformeerd en omdat de gewenste gegevens hierbij vaak zonder heimelijk binnendringen verworven worden.

In tegenstelling tot artikel 45 bestaat er bij artikel 54 in het geheel geen bijschrijfmogelijkheid. Als na ontvangst van de gegevens blijkt dat een *target* inmiddels gebruikmaakt van een ander technisch kenmerk moet hiervoor opnieuw toestemming worden gevraagd aan de minister en de TIB. Bovendien kan, net als bij artikel 45, ook bij artikel 54 een *target* overstappen naar een nieuwe derde, zoals een andere hostingprovider. Ook in dit geval moet opnieuw toestemming worden gevraagd om het *target* te kunnen volgen.

Deze procedure staat de benodigde snelheid in het cyberdomein in de weg. Als een nieuwe aanvraag op basis van artikel 54 eenmaal is goedgekeurd door minister en TIB, dan kan het *target* in de praktijk alweer gewisseld zijn van aanbieder en/of kenmerk en verdwijnt deze uit beeld. Zowel de diensten als de TIB zien het ontbreken van de bijschrijfmogelijkheid bij artikel 54 als een hiaat in de wet. De diensten ervaren deze procedure verder niet alleen als een aantasting van hun effectiviteit, maar ook als een administratieve last zonder toegevoegde waarde wanneer de weging voor de nieuwe aanvraag in feite gelijkwaardig is en op hetzelfde *target* ziet. De Evaluatiecommissie beveelt daarom aan om artikel 54 te voorzien van een bijschrijfmogelijkheid.

Aanbeveling 26

Voorzie artikel 54 van een bijschrijfmogelijkheid.

7.3.7 Het begrip 'slachtofferdata'

Bij de inzet van artikel 45 of artikel 54 kan het voorkomen dat gegevens worden verworven van andere partijen dan de partij waarop de bevoegdheid is ingezet. Het kan hier bijvoorbeeld gaan om gegevens van personen of organisaties die een *target* heeft verworven bij andere partijen via een cyberoperatie. Met andere woorden, deze gegevens kunnen worden aangetroffen als de diensten andere hackende partijen hacken. Indien het gaat om bulkdata, geldt ook hier de eis van ministeriële toestemming voor de bulkbehoefte zoals aanbevolen in §4.3.4.2. Als de verwerving van bulkdata niet was voorzien, moet *achteraf* alsnog de bulkbehoefte worden aangetoond.

Voor de diensten kan het belangrijk zijn om deze gegevens uit te kunnen wisselen met andere inlichtingenteams van de diensten, betrokkenen en/of buitenlandse partners. Ten eerste kunnen deze gegevens iets zeggen over intenties, *modus operandi* en capaciteiten van bijvoorbeeld een statelijke actor waarop de inzet is gericht. Ten tweede kunnen de aangetroffen gegevens ook betrekking hebben op een ander *target* van de diensten en daarmee relevant zijn voor andere inlichtingteams van de diensten. Ten derde stellen deze gegevens de diensten ook in staat om eventueel de partij van wie de gegevens zijn te waarschuwen, zodat er mitigerende maatregelen genomen kunnen worden.

De aangetroffen gegevens kunnen echter ook betrekking hebben op personen of organisaties die geen *target* zijn van de diensten, zoals gegevens van bedrijven of publieke instellingen uit een land waar nauw mee wordt samengewerkt. De TIB noemt deze gegevens 'slachtofferdata' en heeft aangegeven dat deze gegevens wel gebruikt kunnen worden om andere partijen te waarschuwen, maar dat ze – vanwege de inbreuk op de privacy van het slachtoffer – niet automatisch kunnen worden gedeeld met andere teams en in andere inlichtingenactiviteiten van de diensten kunnen worden betrokken. De TIB ziet dit als een potentiële U-bochtconstructie waarmee de diensten bij toeval aangetroffen gegevens kunnen uitwisselen die zij onder andere omstandigheden niet hadden mogen verwerven.

De Evaluatiecommissie sluit zich aan bij het standpunt van de TIB dat het niet mogelijk moet zijn om gegevens te delen met andere teams zonder expliciete toestemming als het aannemelijk is dat de rechtstreekse verwerving van deze gegevens niet zou worden goedgekeurd door de TIB. Echter, gegevens die betrekking hebben op actoren die onderwerp van onderzoek van de diensten zijn, zouden wel voor de betrokken inlichtingenteams beschikbaar moeten komen. In de toelichting op de wet zou deze belangenafweging duidelijker gemaakt kunnen worden. Daarnaast kan worden overwogen om een andere term te hanteren dan 'slachtofferdata', omdat het geen neutrale term is. Deze gegevens kunnen bestaan uit zowel gegevens van onschuldige personen als van kwaadwillende actoren.

Aanbeveling 27

Geef in de toelichting op de wet meer duidelijkheid over het gebruik van gegevens van derden die via artikel 45 en/of 54 worden verworven.

Het gebruik en de uitwisseling van slachtofferdata valt niet onder de verwerving maar onder de verwerking van gegevens. In hoofdstuk 9 wordt aanbevolen om de ex-ante toets door de TIB beperken tot verwervende bevoegdheden en hierbij geen verwerkingsaspecten te betrekken. Dit leent zich bij uitstek voor het (dynamische) toezicht door de CTIVD. De CTIVD kan in haar

reguliere toezichtsrol ook toezien of een inzet niet (on)bedoeld wordt gebruikt om de TIB-toets te omzeilen.

7.4 Strategische operaties

De diensten maken vooral gebruik van bevoegdheden, zoals de hackbevoegdheid, om gegevens te verwerven voor het beantwoorden van onderzoeksvragen. De focus van de Wiv 2017 lijkt dan ook op deze verwerving van gegevens te liggen. Bevoegdheden zoals de hackbevoegdheid kunnen ook worden ingezet in het kader van 'strategische operaties'. Bij strategische operaties gaat het niet zozeer om het verwerven van gegevens voor het beantwoorden van een concrete vraag of op basis van een acute dreiging, maar vooral om het opbouwen van een strategische positie zodat de diensten zich op toekomstige ontwikkelingen kunnen voorbereiden. Te denken valt aan het verkrijgen van toegang tot kennis over de versleuteling van communicatie zodat op een later moment gebruik gemaakt kan worden van deze toegang. Strategische operaties komen niet alleen bij hackoperaties voor, maar ook binnen andere disciplines van de diensten. In het kader van *human intelligence* (HUMINT) worden bijvoorbeeld ook over langere periode netwerken van relaties met informanten opgebouwd, waarmee later informatie verkregen kan worden. Het gaat hierbij om de verwerving van capaciteiten, kennis of bronnen die hier kortweg *assets* worden genoemd (zie hieronder).

Assets

"Any resource – person, group, instrument, installation, or technical system – at the disposal of an intelligence organization."[198]

De Wiv 2017 regelt de bevoegdheden van de diensten om gegevens te verwerven en verwerken voor de uitvoering van hun taken, zoals de hackbevoegdheid, OOG-interceptie of de informantenbevoegdheid. Deze bevoegdheden worden op hoofdlijnen omschreven, maar er is een grote verscheidenheid aan manieren hoe deze bevoegdheden (technisch) ingevuld kunnen worden. Bij de hackbevoegdheid kan bijvoorbeeld gebruik gemaakt worden van een *zeroday* die een kwetsbaarheid in een systeem uitbuit, of een sleutel waarmee berichten of apparaten kunnen worden ontcijferd. Dit zijn vormen van (technische) *assets*, evengoed als een informant of agent een *asset* kan zijn.

Assets kunnen gedurende langere tijd en voor meerdere onderzoeken worden gebruikt. Door de evolutie van een bepaalde technologie, de ontwikkeling van een bepaalde trend of de introductie van een nieuwe militaire doctrine of wapensysteem kunnen bestaande *assets* die de diensten hebben in de toekomst niet meer voldoen. Dit is de reden dat de diensten soms strategische operaties overwegen, om nieuwe *assets* te creëren en vroegtijdig te anticiperen op ontwikkelingen. Samenwerking met buitenlandse partners speelt hierbij vaak een belangrijke rol. Vanwege de complexiteit van strategische operaties is een verscheidenheid aan kennis en capaciteiten nodig waarover de Nederlandse diensten alleen niet altijd beschikken. Dergelijke operaties en samenwerkingsrelaties lopen doorgaans meerdere jaren.

[198] Central Intelligence Agency. (15 juni 1978). *Glossary of Intelligence Terms and Definitions*. p. 9. Beschikbaar via **https://www.cia.gov/library/readingroom/docs/CIA-RDP86B00269R001200130001-3.pdf**.

Voor de ontwikkeling en het verkrijgen van een *asset* kunnen bijzondere bevoegdheden worden ingezet. Daarvoor geldt de gebruikelijke toestemmingsprocedure bij die bevoegdheid. Zo kan met de hackbevoegdheid een bepaalde toegang (*asset*) worden verkregen. Als een *asset* dan vervolgens wordt gebruikt bij verwerving van gegevens via een bijzondere bevoegdheid, zal daarvoor opnieuw een toestemmingsaanvraag moet worden ingediend, met de waarborgen die daarbij horen.

De toelichting op de wet lijkt in algemene zin ruimte te bieden voor de inzet van bijzondere bevoegdheden voor strategische operaties. In de toelichting op het toepassingsbereik wordt gesteld dat bijzondere bevoegdheden kunnen worden ingezet "in het kader van een goede taakuitvoering van de diensten".[199] De toelichting biedt echter weinig duidelijkheid over hoe strategische operaties passen binnen de taakstelling van de diensten. De nadruk ligt op de verwerving van gegevens met de inzet van bijzondere bevoegdheden. Dit levert voor de diensten en voor de TIB soms een ongemakkelijke situatie op waarin enerzijds de behoefte van de diensten wordt erkend, maar waar anderzijds de wet onvoldoende aanknopingspunten lijkt te geven voor de weging van de TIB.

In het licht van het bovenstaande constateert de Evaluatiecommissie dat de wet wel ruimte biedt voor strategische operaties, maar hier onvoldoende expliciet over is. De Evaluatiecommissie heeft daarom begrip voor de aarzelingen die de TIB soms heeft bij het afwegen van de reikwijdte van dergelijke potentieel gevoelige operaties. Om de situatie te verlichten, zou de wetgever in de toelichting op de wet duidelijker kunnen zijn over haar bedoelingen en de redenen waarvoor de diensten bijzondere bevoegdheden kunnen inzetten. Ook moeten in de toelichting op de wet voorbeelden worden opgenomen van de inzet van bevoegdheden voor strategische operaties. Zo wordt de TIB meer handvatten geboden om bij de invulling van de normen te differentiëren.

Aanbeveling 28

Ga in de toelichting op de wet in op het gebruik van bijzondere bevoegdheden voor strategische operaties door middel van voorbeelden om de TIB meer handvatten te bieden voor differentiatie bij de invulling van normen.

7.5 Conclusie

Door het toenemend gebruik van computers is de hackbevoegdheid een essentiële bevoegdheid voor de diensten. Tegelijkertijd is de hackbevoegdheid één van de meest indringende bevoegdheden, omdat computers steeds meer informatie over het privéleven van personen bevatten. Met de hackbevoegdheid kan heimelijk in computers worden binnengedrongen.

Over het algemeen wordt geconstateerd dat de wet redelijk functioneert, maar op een aantal specifieke punten aanpassingen vergt. Het eerste punt betreft het toestemmingsniveau voor het verkennen van een geautomatiseerd werk, dat moet worden verlaagd van ministerieel niveau naar diensten intern. Dit bevordert de kwaliteit en gerichtheid van de toestemmingsaanvragen voor het binnendringen van een geautomatiseerd werk, die *wel* langs de minister gaan. Het

[199] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 43 (MvT Wiv 2017).

tweede punt is dat artikel 54, waarmee gegevensbestanden kunnen worden opgevraagd bij aanbieders van telecommunicatie- en opslagdiensten, voorzien moet worden van een bijschrijfmogelijkheid. Beide punten worden ondersteund door zowel de diensten als de TIB.

Verder is gebleken dat de toelichting op artikel 45 op sommige punten onvoldoende aansluit bij de snelheid en complexiteit van de hackbevoegdheid. Bij de omschrijving van technische risico's voor de TIB-toets is het gewenst meer richting te geven over de mate van detail waaraan de beschrijving moet voldoen; de vraag wanneer een geautomatiseerd werk in gebruik is bij een actor moet nader toegelicht worden; de voorwaarden waaronder via artikel 45 verworven gegevens van derden gebruikt kunnen worden moeten worden verduidelijkt en; de wetgever moet meer helderheid bieden over het toepassingsbereik van artikel 45 in het kader van strategische operaties.

Tot slot concludeert de Evaluatiecommissie dat de TIB een belangrijke waakfunctie vervult voor de inzet van een zware bevoegdheid als de hackbevoegdheid. Tegelijkertijd kan de snelheid en complexiteit – en daaruit voortvloeiende onvoorzienbaarheid – van cyberoperaties in sommige gevallen wringen met de ex-ante toets door de TIB. In deze gevallen ziet de Evaluatiecommissie in het dynamisch toezicht door de CTIVD een geschiktere vorm van toezicht op de uitvoering van hackoperaties.

8 Internationale samenwerking

8.1 Inleiding

Samenwerking met de inlichtingen- en veiligheidsdiensten van andere landen is essentieel voor het goed functioneren van de AIVD en de MIVD. De dreigingen die de diensten onderzoeken, lopen uiteen van ongewenste inmenging door andere staten in Nederland, spionage, sabotage, proliferatie en terrorisme tot dreigingen ten aanzien van internationale vredesoperaties waar Nederland aan deelneemt. Deze dreigingen zijn veelal internationaal van aard. Om deze dreigingen en risico's voor de Nederlandse samenleving en krijgsmacht goed te onderkennen en om ongekende dreigingen tijdig te herkennen, zijn de diensten in grote mate afhankelijk van samenwerking met buitenlandse diensten. Internationale partners kunnen cruciale informatieposities of inlichtingenmiddelen hebben ten aanzien van bepaalde dreigingen. Bovendien kan een samenwerking op het ene moment de onderhandelingspositie van de Nederlandse diensten op een ander moment weer verbeteren. Daarom is het voor de diensten van belang om samen te werken met internationale partners die het speelveld beheersen.

Internationale samenwerking kan bestaan uit enkel wederzijdse verstrekking van gegevens of het verlenen van ondersteuning aan buitenlandse diensten en *vice versa*, maar ook uit deelname aan een multilateraal samenwerkingsverband of het gezamenlijk uitvoeren van een operatie. Internationale samenwerking is in de afgelopen decennia enorm toegenomen. Onder meer vanwege de technologische ontwikkelingen zijn de interne en externe veiligheid steeds meer met elkaar verbonden geraakt. Daarmee heeft ook de hoeveelheid gegevens die internationaal wordt uitgewisseld een grote vlucht genomen. De samenleving heeft daarom begrijpelijkerwijs blijvende aandacht voor – en in sommige gevallen ook onbehagen over – de internationale uitwisseling van grote hoeveelheden gegevens. Zodra gegevens zijn verstrekt aan een buitenlandse dienst hebben de Nederlandse diensten immers geen directe controle meer over deze gegevens en het gebruik hiervan.

De commissie Dessens merkte op dat artikel 59 van de Wiv 2002 betreffende de samenwerking tussen diensten niet meer voldeed en dat het wettelijk kader heroverweging behoefde.[200] De commissie formuleerde daarbij als uitgangspunt voor de nieuwe Wiv-bepalingen betreffende internationale samenwerking dat de activiteiten van de diensten blijvend dienen te voldoen aan de eisen die zowel nationaal- als internationaalrechtelijk worden gesteld, in het bijzonder waar het gaat om de uitwisseling van persoonsgegevens. De Evaluatiecommissie bevestigt en hanteert dit uitgangspunt ook bij deze evaluatie.

Voor deze evaluatie heeft de Evaluatiecommissie zich in het licht van het voorgaande gericht op de vraag of de bevoegdheden en waarborgen rond het internationale samenwerkingsproces in balans zijn. Enerzijds of er voldoende waarborgen zijn rond het stelsel zelf, de mate van samenwerking en de aard van de gegevens die worden uitgewisseld, en anderzijds of er knelpunten zijn waartegen de diensten bij de internationale samenwerking zijn aangelopen.[201]

Bij het beantwoorden van deze vragen wordt in dit hoofdstuk specifiek gekeken naar relevante internationale en Europese ontwikkelingen, het wettelijk kader en de wegingsnotities, het verstrekken van persoonsgegevens door de diensten aan buitenlandse inlichtingen- en veilig-

[200] Samenwerking met buitenlandse diensten werd door de commissie Dessens behandeld in §6.3 als onderdeel van een breder hoofdstuk over samenwerking. Zie: Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*. p. 117.

[201] *Kamerstukken I* 2019/20, 34 588, nr. M (Kamerbrief Evaluatie Wiv 2017).

heidsdiensten, internationale ondersteuning en meer specifiek het ontvangen van gegevens en multilaterale samenwerking en toezicht.

8.2 Internationale en Europese ontwikkelingen

De eisen die in dit verband op internationaalrechtelijk niveau worden gesteld, zijn steeds duidelijker dankzij de zich ontwikkelende jurisprudentie van het EHRM in Straatsburg, baanbrekende uitspraken van nationale rechters en ontwikkelingen binnen het EU-recht op het gebied van bescherming van persoonsgegevens (zie §3.4 en §4.2). Voor dit hoofdstuk is met name de reeds besproken *Big Brother*-zaak relevant, waarbij het gaat om internationale samenwerking tussen de Britse en Amerikaanse diensten en meer specifiek het delen van bulkdata.[202] Het ging hierbij om het ontvangen van persoonsgegevens, niet het verstrekken daarvan. Van belang is dat het EHRM in deze zaak het verwerven of delen van bulkdata in het licht van de terroristische dreiging als zodanig niet als disproportioneel heeft aangemerkt. Specifiek met betrekking tot het uitwisselen van persoonsgegevens heeft het Hof het volgende gesteld:

> *"Faced with such a threat, the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts (see Othman, cited above, §183). Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world. As, in the present case, this 'information flow' was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was 'necessary in a democratic society'."*[203]

Het Hof kijkt dus met name naar de wettelijke context voor een rechtmatigheidsoordeel, waarbij van belang is dat er stevige waarborgen tegen misbruik bestaan. Nationale wetgeving dient hierbij duidelijk en voorzienbaar te zijn.[204] Het Hof benadrukt verder dat verzoeken aan buitenlandse diensten niet gedaan mogen worden om eisen die gelden voor de diensten zelf te omzeilen.

Ook nationale rechters in Europa hebben hierover richtinggevende uitspraken gedaan. In zijn uitspraak van 20 mei 2020 betreffende de grondwettigheid van bepaalde aspecten van de Duitse wet op de inlichtingen- en veiligheidsdiensten was het *Bundesverfassungsgericht* (het Duitse Constitutionele Hof; BVerfG) op onderdelen concreter dan het Straatsburgse Hof. Het Constitutionele Hof stelt dat de Duitse grondwet aan internationale samenwerking niet in de weg staat, ook niet waar het het delen van ongeëvalueerde bulkdata betreft, mits dit plaatsvindt op basis van wettelijke bepalingen die de bescherming van grondrechten waarborgen. Het Hof benadrukt zelfs dat goed functionerende informatie-uitwisseling van belang is om de Duitse overheid in staat te stellen de grondwettelijk garandeerde bescherming van haar burgers en ingezetenen te waarborgen. Maar het Hof stelt ook dat Duitsland een verplichting heeft om burgers en ingezetenen te beschermen tegen illegale *surveillance* van andere staten. Vanuit die

[202] Zoals reeds in hoofdstuk 4 aangegeven wordt onder bulkdata verstaan: een omvangrijke verzameling van gegevens waarvan het merendeel betrekking heeft op personen en/of organisaties die niet in onderzoek zijn van de diensten en dit ook nooit zullen worden.
[203] EHRM 13 september 2018, (*Big Brother Watch)*, para. 446.
[204] EHRM 13 september 2018, (*Big Brother Watch)*, paras. 424-444.

verplichting destilleert het Hof een inspanningsverplichting om gegevens van Duitse burgers en ingezetenen ten aanzien van zoektermen, treffers en in het bijzonder ook bij het verstrekken van ongeëvalueerde/ongeselecteerde bulkgegevens, te filteren. Het Hof stelt ook dat aan partnerdiensten moet worden gevraagd toe te zeggen dataverkeer met Duitse burgers of ingezetenen onmiddellijk te verwijderen als dat tijdens de analyse als zodanig wordt geïdentificeerd. Speciale verplichtingen gelden ook voor mensen die bijzondere risico's lopen, zoals dissidenten, klokkenluiders en advocaten en journalisten. Tot slot stelt het Hof dat toezeggingen moeten worden verkregen dat de verstrekte gegevens niet langer dan zes maanden worden bewaard.[205]

In zijn uitspraak heeft het Duitse Hof de Duitse wet op de inlichtingendiensten getoetst aan de Duitse grondwet. De uitspraak is derhalve niet direct van toepassing op de Wiv 2017 of de Nederlandse praktijk. De uitspraak geeft echter wel een beeld hoe in Duitsland wordt omgegaan met vragen betreffende het werk van inlichtingen- en veiligheidsdiensten, en specifiek met vragen die rijzen bij het gebruik en de uitwisseling van bulkdata. De uitspraak geeft ook een bepaalde visie weer die aansluit bij brede ontwikkelingen in Europees verband. De uitspraak kan dan ook bijdragen aan de geleidelijke totstandkoming van gedeelde (Europese) normen.

Een andere in dit kader relevante uitspraak is de in §3.4 genoemde zaak Schrems II van het HvJEU. In deze zaak van 16 juli 2020 heeft dit Hof het adequaatheidsbesluit van de Europese Commissie voor de doorgifte van persoonsgegevens door bedrijven of organisaties naar de Verenigde Staten op basis het zogenaamde '*Privacy Shield*' ongeldig verklaard. Daarnaast overwoog het Hof dat de standaardbepalingen van de Europese Commissie voor de doorgifte van persoonsgegevens naar derde landen (*Standard Contractual Cases*, SCC's) niet per definitie een passend beschermingsniveau waarborgen en dat het beschermingsniveau van een land per geval beoordeeld moeten worden (is er een "*adequate level of protection*").[206]

Deze uitspraken laten dus ontwikkelingen zien met betrekking tot de beoordeling van de rechtmatigheid van internationale samenwerking tussen diensten die ook voor de Nederlandse praktijk van belang zijn.

8.3 De Wiv 2017 en internationale samenwerking

8.3.1 Het wettelijke kader

De commissie Dessens kwam tot de conclusie dat het wettelijk kader voor internationale samenwerking heroverweging behoefde. In de Wiv 2017 is daarom een nieuw kader met waarborgen ten aanzien van internationale samenwerking vastgelegd, waarbij met name de wettelijke verplichting om te werken met wegingsnotities een belangrijke toevoeging was. In artikel 88 van de wet is geregeld dat de diensten bij een operationele behoefte een samenwerkingsrelatie met

[205] 1 BvR 2835/17, ECLI:DE:BVerfG:2020:rs20200519.1bvr283517, Het Hof stelt, "*Zu den von den ausländischen Diensten einzuholenden Zusagen gehört hier überdies, dass die gesamthaft übermittelten Daten nicht für einen längeren Zeitraum als sechs Monate bevorratend gespeichert werden.*" De termijn van zes maanden betreft derhalve de volledig verstrekte bulkdataset en niet per se door de ontvangende dienst uit die bulkdata geselecteerde gegevens.

[206] HvJEU 16 juli 2020, (*Schrems II*), r.o, 184 en r.o. 83, 86 en 93; HvJEU 6 oktober 2020, (*Quadrature du Net and others*); HvJEU 6 oktober 2020, (*Privacy International*) *("although it is for the Member States to define their essential security interests and to adopt appropriate measures to ensure their internal and external security, the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law") en 104 ("national legislation which requires providers of electronic communications services to retain traffic and location data for the purposes of protecting national security and combating crime, ..., falls within the scope of Directive 2002/58.").*

buitenlandse diensten mogen aangaan. Hiervoor moet de betreffende buitenlandse dienst eerst op een aantal in artikel 88, lid 3, neergelegde criteria worden beoordeeld. Dit wordt vastgelegd in een wegingsnotitie.

De wet geeft verder aan hoe deze samenwerkingsrelatie kan worden vormgegeven. Dat kan bestaan uit het uitwisselen van geëvalueerde en ongeëvalueerde gegevens (artikel 89, lid 1 en 2) of het verlenen van technische ondersteuning (artikel 89, lid 4). Daarnaast kunnen de diensten andere diensten verzoeken om technische en andere vormen van ondersteuning (artikel 90, lid 1) of om het verrichten van een handeling die overeenkomt met de uitoefening van een bijzondere bevoegdheid (artikel 90, lid 3). In bijzondere gevallen – als er sprake is van een dringende en gewichtige reden – kunnen de diensten op basis van artikel 64 ook gegevens verstrekken aan diensten waarmee geen samenwerkingsrelatie bestaat. Dit mag alleen gebeuren na toestemming van de minister. Als het gaat om ongeëvalueerde gegevens moet de CTIVD hierover worden geïnformeerd.

Artikel 65, lid 2, bepaalt in combinatie met artikel 62, lid 1, sub d, dat diensten alleen gegevens verstrekken op voorwaarde dat de ontvangende dienst deze gegevens niet aan anderen mag verstrekken (‘*third party rule*’). Daarnaast wordt in artikel 62, lid 1, sub d, en artikel 63 ook gerefereerd aan verstrekking van gegevens aan buitenlandse diensten.

De diensten zijn in de uitvoering van de wettelijk taken vaak afhankelijk van gegevens die worden ontvangen van buitenlandse partners. Afspraken over samenwerking en de uitwisseling van gegevens worden vaak in een algemeen *Memorandum of Understanding* tussen de Nederlandse dienst en de buitenlandse dienst vastgelegd. Vervolgens worden concrete gegevens over een specifiek onderwerp vanuit het buitenland verstrekt nadat de Nederlandse dienst daartoe een verzoek heeft ingediend (een *request for information)*. In de Wiv 2017 ontbreekt echter een expliciete grondslag voor een dergelijk verzoek. Dit gebeurt op basis van zowel artikel 39 (de informantenbevoegdheid) als artikel 62.

8.3.2 Algemene bevindingen

In de nieuwe wet valt op dat de samenwerking met buitenlandse diensten pas in §6.2 aan bod komt, ondanks het grote belang van deze samenwerking voor het functioneren van de diensten. Daarnaast valt op dat het thema internationale samenwerking op een summiere en gefragmenteerde manier in de wet is geregeld. Naast de drie artikelen van deze §6.2, zijn bijvoorbeeld ook artikel 62, lid 1, onder d, artikel 64 en artikel 65 van direct belang.[207] Daarnaast is de grondslag waarop informatie wordt opgevraagd aan buitenlandse partners zoals hierboven beschreven niet duidelijk in de wet verwoord. Dit zou een eigen grondslag in de wet moeten krijgen ten behoeve van de uniformiteit en de voorzienbaarheid.

De vraag dringt zich op of deze manier van reguleren voldoende recht doet aan het centrale belang van internationale samenwerking en de maatschappelijke aandacht voor dit thema. Als de Wiv 2017 in de toekomst fundamenteel wordt herzien, verdient het aanbeveling om het thema van internationale samenwerking op een prominentere en meer systematische wijze te regelen.

[207] Zie ook het advies van de RvS op dit punt en meer in het bijzonder de aanbeveling om de overdracht van gegevens aan buitenlandse diensten op een plek in de wet te regelen: *Kamerstukken II* 2016/17, 34 588, nr. 4, p. 24, 40-43.

De belangrijkste observatie betreffende dit thema is dat de normering van internationale samenwerking moet worden uitgebreid en versterkt, zodat deze beter is gespecificeerd en wettelijk verankerd.

Aanbeveling 29

Voorzie in een eenduidig wetsartikel als grondslag voor het bevragen van internationale partners en het ontvangen van gegevens van deze partners.

8.4 De waarborg van de wegingsnotities

De belangrijkste wijziging van de Wiv 2017 op het terrein van internationale samenwerking is de introductie van de wettelijke verplichting om wegingsnotities op te stellen voordat een samenwerkingsrelatie wordt aangegaan. Op basis van de notitie wordt bepaald of kan worden overgegaan tot samenwerking en wat de aard en intensiteit van deze samenwerking mag zijn. In het kader van een samenwerkingsrelatie kunnen de diensten gegevens uitwisselen voor zover deze niet strijdig zijn met de belangen van de eigen diensten en ze de goede taakuitvoering niet belemmeren (art. 89, lid 1). In de regel werken de diensten samen met inlichtingen- en veiligheidsdiensten van andere landen op basis van artikel 88. De wet biedt alleen geen expliciete basis voor internationale samenwerking met niet-statelijke groeperingen, zoals bijvoorbeeld groeperingen die niet als vertegenwoordigers van een staat zijn erkend maar die wel bepaalde statelijke activiteiten uitoefenen. Hierdoor is het onduidelijk of de wet voorziet in samenwerking met deze niet-statelijke groeperingen. Als de wetgever dit wil toestaan, dan is een expliciete wettelijke basis en een duidelijke verplichting tot het opstellen van een wegingsnotitie voor zo'n samenwerking nodig.[208]

Een samenwerkingsrelatie met buitenlandse diensten zal alleen maar worden aangegaan als de samenwerking operationeel toegevoegde waarde heeft. Als dat het geval is, zal een dienst moeten worden 'gewogen' om te bezien of hij wel voldoet aan de Nederlandse standaarden. De weging vindt plaats op basis van de volgende wettelijke criteria: (a) democratische inbedding, (b) de eerbiediging van de mensenrechten, (c) professionaliteit en betrouwbaarheid, (d) de wettelijke bevoegdheden en mogelijkheden en (e) het niveau van gegevensbescherming. Daarnaast beoordelen de diensten of de mate van samenwerking bevorderlijk is voor de taakuitvoering en wordt bezien of samenwerking wenselijk is in verband met internationale verplichtingen.[209] Tegelijkertijd wordt er ook gekeken of er sprake is van een juiste balans in de samenwerking ('*quid pro quo*').

[208] Het is hierbij van belang dat de grenzen van het internationale recht in acht worden genomen. Zie bijvoorbeeld: CAVV/AIV. (25 juni 2020). *Advies inzake het leveren en financieren van niet-letale steun aan niet-statelijke gewapende groepen in het buitenland*.

[209] Mandaatbesluit AIVD ten aanzien van samenwerking met inlichtingen- en veiligheidsdiensten van andere landen 2020, *Stcrt*. 2020, nr. 38474., (Mandaatbesluit AIVD ten aanzien van samenwerking met inlichtingen- en veiligheidsdiensten van andere landen 2020).

De wegingsnotitie bepaalt of er sprake is van enig risico en welke voorwaarden daarom aan de samenwerking gesteld moeten worden. Bij weging van buitenlandse diensten hanteren de diensten drie verschillende categorieën:

Categorie 1 Samenwerking onder standaard voorwaarden
Categorie 2 Samenwerking onder aanvullende voorwaarden
Categorie 3 Samenwerking onder strikte voorwaarden

Als de diensten gegevens willen verstrekken, wordt gekeken naar de risico's zoals vastgelegd in de wegingsnotities. Op basis daarvan kan worden besloten geen gegevens te verstrekken, of kunnen er voorwaarden worden verbonden aan de samenwerking. Het doel van deze voorwaarden is om risico's bij verstrekking zo veel als mogelijk te beperken. Dat kan dus betekenen dat aan twee diensten binnen dezelfde categorie toch verschillende voorwaarden worden gesteld. Elke weging en elke samenwerking is maatwerk, het hanteren van de voorwaarden logischerwijs dus ook. In de wegingsnotities kan bijvoorbeeld zijn opgenomen dat een bepaald type gegevens of gegevens over een specifiek onderwerp niet worden verstrekt, dat alleen samenwerking mogelijk is nadat daarvoor toestemming is gegeven door de minister of dat nadere afspraken worden gemaakt over de inzet van bevoegdheden om het risico op zogeheten U-bochtconstructies te voorkomen.

Of de bovengenoemde categorieën op juiste (rechtmatige) wijze worden gebruikt, is geen onderdeel van deze evaluatie. Dat is bij uitstek aan de CTIVD. Zij heeft aangekondigd een onderzoek te gaan doen naar de rechtmatigheid van het verstrekken van persoonsgegevens door de AIVD en MIVD aan buitenlandse diensten met een verhoogd risicoprofiel.[210] Hierbij zal worden gekeken of de diensten per geval een rechtmatige afweging maken en daar de juiste voorwaarden aan verbinden.

De introductie van de wegingsnotities heeft disciplinerend gewerkt. De bewustwording bij de diensten van de risico's van internationale samenwerking is erdoor vergroot. Het werken met de wegingsnotities is redelijk uniek in vergelijking met andere landen. Nederland lijkt hiermee internationaal voorop te lopen. De Evaluatiecommissie benadrukt dan ook het belang van de wegingsnotities, en beschouwt het als een belangrijke waarborg bij internationale samenwerking. Wel wordt opgemerkt dat de introductie van de wegingsnotities een extra administratieve last legt bij de diensten. Met de inwerkingtreding van de Wiv 2017 moesten in korte tijd voor de meest hechte samenwerkingsrelaties wegingsnotities zijn opgesteld.[211] Het opstellen en het up-to-date houden van deze notities kost de diensten veel capaciteit.

Eén van de criteria die worden gewogen bij het aangaan van een samenwerkingsrelatie is 'democratische inbedding' van de buitenlandse dienst. Impliciet wordt hierbij ook de positie en de effectiviteit van de toezichthoudende autoriteit in het desbetreffende land meegenomen. Gelet echter op de Europeesrechtelijke ontwikkelingen waarin het belang van effectief en onafhankelijk toezicht op gegevensbescherming wordt benadrukt[212], verdient het de voorkeur 'toezicht' als separaat wegingscriterium in de wet op te nemen zodat de diensten daaraan ook nadrukkelijker aandacht besteden. Hierbij is het ook van belang dat buitenlandse toezicht-

[210] CTIVD. (2020). *Aankondiging onderzoek naar het verstrekken van persoonsgegevens door de AIVD en de MIVD aan buitenlandse diensten met een verhoogd risicoprofiel*. Beschikbaar via **https://www.ctivd.nl/actueel/nieuws/2020/06/25/index**.
[211] CTIVD. (2019). *Toezichtsrapport 60 over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners*. p. 8.
[212] HvJEU 16 juli 2020, (*Schrems II*), r.o. 104.

houders soms een beperkter mandaat hebben, met name ook voor wat betreft het toezicht op buitenlandse persoonsgegevens.

Aanbeveling 30

Als de wetgever samenwerking met niet-statelijke groeperingen wil toestaan, dan moet in de wet een expliciete wettelijke basis komen met de verplichting tot het opstellen van een wegingsnotitie voor deze samenwerking.

Aanbeveling 31

Neem 'de inrichting en effectiviteit van het toezicht' op als apart wegingscriterium.

In het kader van een goede taakuitvoering zijn de diensten op grond van artikel 64, lid 1, bevoegd om op grond van 'dringende en gewichtige redenen' gegevens te verstrekken aan buitenlandse diensten waar geen samenwerkingsrelatie mee bestaat. De Evaluatiecommissie heeft begrip voor deze wettelijke uitzondering maar benadrukt dat dit stringente uitzonderingskarakter van deze bepaling ten zeerste gerespecteerd dient te worden en dat de toezichthouder hierop toeziet. Het druist immers in tegen de waarborgen die de wegingsnotities bieden.

8.5 Nadere waarborgen bij de verstrekking van gegevens aan buitenlandse diensten

Naast de systematiek van de wegingsnotities biedt de wet ten aanzien van de feitelijke verstrekking van gegevens aan een buitenlandse dienst weinig aanknopingspunten. Naast de algemene bepalingen voor gegevensverwerking, gelden specifiek voor deze verstrekkingen eigenlijk de '*third party rule*' van artikel 65 en de plicht om aantekening te houden (artikel 70). Hoewel uit deze algemene bepalingen al de nodige waarborgen volgen, verdient het de aanbeveling om dit algemene kader te specificeren en te codificeren.

Dit is van belang omdat in geval van het verstrekken van persoonsgegevens aan buitenlandse partnerdiensten inbreuk wordt gemaakt op de privacy van de betrokken perso(o)n(en). Een dergelijke verstrekking kan bovendien (indirect) leiden tot schending van andere mensenrechten, waaronder bijvoorbeeld de vrijheid van meningsuiting, het recht op een eerlijk proces, of zelfs het recht om niet te worden gefolterd en het recht op leven.

8.5.1 Meer inhoudelijke waarborgen

In de samenleving bestaan de nodige zorgen over internationale gegevensverstrekking tussen de diensten. Daarom moeten inhoudelijke voorwaarden, die nu al vaak een staande praktijk zijn en in beleidsregels of anderszins zijn gespecificeerd, van een directe wettelijke grondslag in de Wiv worden voorzien. Zo beveelt de Evaluatiecommissie aan om de regel in de wet op te nemen dat er geen gegevens worden gedeeld als er een reëel risico bestaat dat gebruik door de ontvan-

gende dienst een flagrante schending oplevert van het internationaal recht, en in het bijzonder van de mensenrechten en internationaal humanitair recht.[213]

Een ander voorbeeld van een inhoudelijke norm die duidelijker en explicieter wettelijk verankerd moet worden betreft het delen van bulkdata. In overeenstemming met de reeds bestaande praktijk dat de diensten geen register-bulkdata van Nederlandse medeoverheden – zoals het kentekenregister van de RDW of het register van de KvK – met buitenlandse partners delen, beveelt de Evaluatiecommissie aan dit als een verbodsbepaling op te nemen in de wet. Dit levert geen inperking op ten opzichte van huidige situatie omdat de diensten in de praktijk nu ook geen register-bulkdata delen,[214] maar biedt wel een wettelijke waarborg en garantie voor Nederlandse burgers en ingezetenen.

Voor gedrag-bulkdata geldt dat deze in beginsel niet in Nederland en specifiek over Nederlandse burgers en ingezetenen wordt verworven als er ook een lichter middel bestaat om de benodigde gegevens te verzamelen (zie §4.3.3). Dit komt voort uit het subsidiariteitsprincipe. Soms bestaan deze lichtere middelen niet. Dit zal in de praktijk met name gelden in het buitenland maar het kan soms voorkomen dat er ook in Nederland geen lichtere mogelijkheid is om noodzakelijke gegevens te verwerven. Hierdoor is het mogelijk dat er gegevens van Nederlandse burgers of ingezetenen onderdeel uitmaken van de verworven bulkdata. Daarom beveelt de Evaluatiecommissie aan om in de wet een inspanningsverplichting voor de diensten op te nemen om – waar technisch haalbaar en uitvoerbaar – bij het verstrekken van bulkdata te filteren op specifieke Nederlandse kenmerken, om op deze wijze Nederlandse burgers en ingezetenen passende waarborgen te bieden. Op welke kenmerken wordt gefilterd, hangt af van de context.

In dit kader kan verwezen worden naar het *Bundesverfassungsgericht*, dat heeft geoordeeld dat Duitsland een verplichting heeft om Duitse burgers en ingezetenen te beschermen tegen illegale *surveillance* van andere staten. Vanuit deze verplichting destilleerde het Duitse Hof een inspanningsverplichting ten aanzien van filtering van gegevens van Duitse burgers en ingezetenen, in het bijzonder ook bij het verstrekken van bulkdata. Het Hof stelde dat speciale verplichtingen ook kunnen gelden ten aanzien van mensen die bijzondere risico's lopen, zoals dissidenten, klokkenluiders, advocaten en journalisten.

Op grond van de Nederlandse Grondwet en internationale mensenrechtenverplichtingen kan worden betoogd dat ook Nederland zich moet inspannen om de persoonlijke levenssfeer en de lichamelijke integriteit van bepaalde groepen personen te beschermen.[215] De Wiv 2017 benoemt twee 'bijzondere categorieën personen': journalisten en advocaten (artikel 30). Journalisten en advocaten hebben in een democratische samenleving een bijzondere rol en daarom is een inzet op deze twee beroepsgroepen in de wet met meer waarborgen omkleed.[216] Ook andere groepen zoals klokkenluiders en dissidenten kunnen grotere risico's lopen. Een wettelijke inspanningsverplichting voor de diensten om, waar relevant en van toepassing, te filteren op specifieke (Nederlandse) kenmerken van bijzondere categorieën personen en speciale groepen, vertaalt deze verplichting naar de concrete context van de Wiv 2017. Op welke kenmerken gefilterd

[213] CTIVD. (2019). *Toezichtsrapport 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD*. Bijlage II, para. 5.3.2.

[214] Eventueel kan een uitzondering op het verbod in geval van dwingende noodzaak worden opgenomen voor nu nog niet te voorziene situaties.

[215] Zie over positieve verplichtingen in deze context ook HvJEU 6 oktober 2020, (*Quadrature du Net and others*), r.o. 126, 128.

[216] *Kamerstukken II* 2016/17, 34 588, nr. 3. p. 242 (MvT Wiv 2017).

dient te worden, zal afhangen van de situatie en de technische haalbaarheid, en vereist derhalve maatwerk. De Evaluatiecommissie beveelt daarom aan in de wet een *algemene* verplichting tot filtering – waar technisch haalbaar en uitvoerbaar - van kenmerken van bijzondere categorieën personen en speciale groepen op te nemen. Deze verplichting is grotendeels al een reflectie van een reeds bestaande praktijk en geldende beleidsregels.

Een ander punt betreft het standpunt van het Duitse Hof dat aan partnerdiensten moet worden gevraagd toe te zeggen dataverkeer met Duitse burgers of ingezetenen onmiddellijk te verwijderen als ze tijdens de analyse als zodanig worden geïdentificeerd en deze verder niet relevant zijn voor het onderzoek. Dit Duitse standpunt sluit aan bij de internationale inlichtingenpraktijk waarbij het gebruikelijk is om de ontvangende dienst te verzoeken bij ontdekking van gegevens over hun burgers, die onbedoeld zijn verstrekt, deze alsnog te verwijderen. De Evaluatiecommissie beveelt aan om een dergelijke norm ook in de Nederlandse wet op te nemen. Hiermee worden de diensten verplicht om bij verstrekking van gegevens de ontvangende dienst te verzoeken gegevens over Nederlandse burgers en ingezetenen, die voorafgaand aan verstrekking niet waren onderkend en verder niet direct relevant zijn voor het onderzoek, bij eventuele ontdekking te vernietigen. Dit draagt bij aan een geleidelijke totstandkoming van gedeelde (Europese) normen en bovendien benadrukt een dergelijke wettelijke norm het belang dat de wetgever hecht aan bescherming van Nederlandse burgers en ingezetenen.

Het Duitse Hof stelde ook de voorwaarde dat de partnerdienst de ontvangen gegevens binnen een bepaalde termijn vernietigt, namelijk zes maanden. De Nederlandse diensten kennen een dergelijk vernietigingsverzoek niet. De Evaluatiecommissie beveelt aan om in de wet op te nemen dat de diensten bij verstrekking van gegevens verplicht zijn de buitenlandse dienst te verzoeken de gegevens te vernietigen als deze niet (meer) worden gebruikt voor het inlichtingenproces. Het ligt niet voor de hand een termijn expliciet in de wet op te nemen. Termijnen die de diensten eventueel zelf kunnen stellen, zullen nauw samenhangen met de aard van de gegevens en de risico's die voortvloeien uit de wegingsnotities en zijn niet goed in absolute, wettelijk te verankeren, getallen te vangen.

Aanbeveling 32

Leg de volgende inhoudelijke normen in de wet vast die gelden bij het verstrekken van gegevens aan buitenlandse diensten:

a) De regel dat er geen gegevens worden gedeeld als er een reëel risico bestaat dat gebruik door de ontvangende dienst een flagrante schending oplevert van het internationaal recht, en in het bijzonder van de mensenrechten en internationaal humanitair recht.
b) Het verbod op het delen van register-bulkdata van Nederlandse medeoverheden.
c) De inspanningsverplichting om – waar technisch haalbaar en uitvoerbaar – bij het verstrekken van bulkdata te filteren op specifieke Nederlandse kenmerken.
d) De algemene inspanningsverplichting – waar technisch haalbaar en uitvoerbaar – tot het filteren van bijzondere categorieën personen, met name journalisten en advocaten, en andere specifieke groepen personen, zoals klokkenluiders en dissidenten.
e) De verplichting om bij verstrekking van gegevens de ontvangende dienst te verzoeken gegevens over Nederlandse burgers en ingezetenen, die voorafgaand aan verstrekking niet waren onderkend en verder niet direct relevant zijn voor het onderzoek, bij eventuele ontdekking te vernietigen.

f) De verplichting om bij verstrekken van gegevens de ontvangende dienst te verzoeken de gegevens te vernietigen als deze niet (meer) worden gebruikt voor het inlichtingenproces.

8.5.2 Het onderscheid geëvalueerd/ongeëvalueerd

De Wiv maakt een onderscheid tussen geëvalueerde en ongeëvalueerde gegevens – zonder dit nader te definiëren – waarbij ministeriële toestemming en een meldplicht bij het CTIVD gelden voor het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten. Deze extra waarborgen legden druk op de exacte afbakening van het begrip 'ongeëvalueerd', waarbij met name de koppeling in de wetsgeschiedenis[217] aan het begrip relevantie, en de praktijk van relevantiebepaling op hoog abstractieniveau heeft geleid tot verschillende standpunten betreffende de juiste interpretatie van het begrip 'ongeëvalueerd'.

In §4.4.5 is hier al uitvoerig op ingegaan en zijn de bevindingen van de Evaluatiecommissie voorzien van de aanbeveling dat in de wet wordt opgenomen dat bulkdatasets pas verstrekt mogen worden aan een buitenlandse dienst nadat de verantwoordelijke minister hiervoor toestemming heeft verleend. Het wettelijk onderscheid tussen geëvalueerd en ongeëvalueerd kan hiermee worden losgelaten.

8.5.3 Het toezichtstelsel bij verstrekking van persoonsgegevens aan buitenlandse diensten

De uitwisseling van persoonsgegevens met buitenlandse diensten vraagt om een constante afweging van belangen en risico-inschattingen tot welke grens die verstrekking geoorloofd is. Met de intrede van nieuwe technologieën zijn die grenzen opgeschoven.[218] Des te relevanter is dan ook de vraag of het toezicht op internationale samenwerking, en meer specifiek op het uitwisselen van gegevens met buitenlandse diensten, voldoet aan de eisen die voortvloeien uit de zich ontwikkelende internationale en Europese jurisprudentie van zowel het EHRM als het HvJEU. Een andere belangrijke vraag betreft de werkbaarheid van het systeem. Uit de bestaande jurisprudentie van het EHRM volgt dat voor een oordeel over de rechtmatigheid van internationale gegevensuitwisseling het systeem van waarborgen en toezicht in zijn totaliteit dient te worden beschouwd.

De CTIVD speelt een belangrijke rol bij het toezicht op internationale samenwerking. De aandacht van de CTIVD voor internationale samenwerking blijkt ook uit het grote aantal rapporten dat specifiek ingaat op dit thema en concrete onderdelen daarvan. Ingevolge de beleidsregels Wiv 2017 geldt voor het verstrekken van ongeëvalueerde gegevens dat de minister toestemming dient te geven en bestaat een meldplicht aan de CTIVD. De aanstaande wetswijziging van de Wiv 2017 zorgt voor een wettelijke verankering van deze beleidsregels. De tijdelijke bulkregeling[219] inzake verdere verwerking van bulkdatasets Wiv 2017 (zie §4.4) breidt de meldplicht aan de CTIVD uit naar alle (dus ook geëvalueerde) bulkdata.

De Evaluatiecommissie heeft zich ook de vraag gesteld of de TIB een formele rol moet krijgen bij internationale samenwerking en meer specifiek de verstrekking van gegevens. Bij de behan-

[217] "Ongeëvalueerd is als gegevens nog niet op hun relevantie voor de taakuitvoering van de diensten zijn onderzocht." *Kamerstukken II* 2016/17, 34 588, 18, p. 18 (Nota naar aanleiding van het Verslag Wiv 2017).
[218] CTIVD. (2009). *Toezichtsrapport 22a over de samenwerking van de AIVD met buitenlandse inlichtingen en veiligheidsdiensten*. p. 28.
[219] Regeling van 5 november 2020, *Stcrt*. 2020, 56482.

deling van het wetsvoorstel tot wijziging van de Wiv 2017 in de Tweede Kamer is het amendement Buitenweg verworpen.[220] Dit amendement strekte ertoe om een verstrekking van ongeëvalueerde gegevens aan buitenlandse partners te laten toetsen door de TIB. Een toetsing van de TIB zou volgens de indiener onder andere kunnen voorkomen dat gegevens van bijzondere categorieën personen onbedoeld verstrekt worden aan buitenlandse partners. Daarnaast is de TIB van oordeel dat zij thans reeds een rol heeft bij de beoordeling van internationale samenwerking. Als de diensten bij een verzoek om toestemming tot de inzet van een bijzondere bevoegdheid al het oogmerk hebben de te verwerken gegevens te delen met buitenlandse diensten, dient dit naar het oordeel van de TIB in het verzoek te worden opgenomen en wordt het door de TIB in de toetsing meegenomen. Daarmee heeft de TIB een beoordelingscriterium ingevoerd dat pas bij verwerking aan de orde is en niet bij verwerving. Deze benadering doorkruist het onderscheid betreffende verwerving en verwerking van gegevens, zoals onderstreept in het hoofdstuk 9 betreffende het stelsel van toezicht.

De Evaluatiecommissie acht een rol van de TIB bij internationale samenwerking niet aangewezen. Zoals in hoofdstukken 4 en 9 wordt toegelicht, moet de TIB-toets worden beperkt tot verwerving. De daaropvolgende verwerking van gegevens, inclusief het eventueel verstrekken aan buitenlandse diensten, is bij uitstek onderworpen aan toezicht door de CTIVD. De CTIVD houdt reeds toezicht op de wegingsnotities en kan bovendien toezicht houden op de verschillende verplichtingen die de Evaluatiecommissie eerder heeft aanbevolen, bijvoorbeeld ten aanzien van filtering. De Evaluatiecommissie acht het niet opportuun om het toezicht op internationale samenwerking te verspreiden over verschillende toezichthouders. Bovenstaande kent één uitzondering. Wanneer de inzet van bijzondere bevoegdheden door de diensten (mede) ten behoeve van een buitenlandse dienst plaatsvindt, kan de verstrekking van gegevens door de TIB worden betrokken in haar toets. Dit volgt uit het feit dat het delen van gegevens hierbij het *doel* is van de inzet.

Aanbeveling 33

De CTIVD houdt toezicht op internationale samenwerking, en specifiek ook het verstrekken van (bulk)gegevens. Internationale samenwerking en meer specifiek verstrekking van gegevens/bulkdata worden niet getoetst door de TIB. De TIB heeft alleen een rol bij internationale samenwerking waar het de inzet van door de TIB te toetsen bijzondere bevoegdheden (mede) ten behoeve van een buitenlandse dienst betreft.

8.6 Het verlenen en ontvangen van internationale ondersteuning

De diensten zijn bevoegd in het kader van de goede taakuitvoering internationale ondersteuning te bieden aan een buitenlandse dienst (artikel 89, lid 4) of die ondersteuning te krijgen (artikel 90). Het krijgen van ondersteuning kan op twee manieren worden gerealiseerd. De diensten kunnen door een buitenlandse dienst worden geholpen bij de uitoefening van een bevoegdheid (artikel 90, lid 2), dan wel de buitenlandse dienst verricht de beoogde inzet van de bevoegdheid helemaal zelf (artikel 90, lid 3).

[220] *Kamerstukken II* 2019/20, 35 242, nr. 9 (amendement Buitenweg).

In beide gevallen kan het gaan om de inzet van een bijzondere bevoegdheid. Daarvoor moet de minister eerst toestemming geven. In het eerste geval moet deze toestemming ook worden getoetst door de TIB. Dat geldt niet voor het tweede geval omdat de diensten de inzet niet (deels) zelf uitoefenen, dit doet de buitenlandse dienst. Uit de toelichting op de wet lijkt te volgen dat dit verschil voortvloeit uit het feit dat de bevoegdheid in het tweede geval niet door de diensten wordt uitgeoefend en niet binnen de Nederlandse jurisdictie plaatsvindt. Enerzijds is dat logisch. De buitenlandse dienst kent immers eigen procedures en waarborgen waar de TIB niet op kan toetsen. Anderzijds is het ook onlogisch; als de diensten diezelfde bevoegdheid zelf zouden inzetten, eventueel met behulp van de partner, is de rechtmatigheidstoets door de TIB wel van toepassing. Om een mogelijke onwelwillende TIB-toets te vermijden óf om een door de TIB afgewezen aanvraag alsnog rechtmatig te kunnen uitvoeren, zouden de diensten gebruik kunnen maken van een U-bochtconstructie die de wet onbedoeld lijkt te faciliteren en niet expliciet verbiedt. Het is van belang dat de wet preciseert dat een dergelijke U-bochtconstructie verboden is. Dit is dus breder dan het verbod zoals neergelegd in artikel 90, lid 5. De CTIVD kan hierop toezien binnen de reeds bestaande bevoegdheden. Een rol voor de TIB bij de toepassing van artikel 90, lid 3, ligt niet in de rede, omdat dit er in de praktijk op neer zou komen dat de TIB de rechtmatigheid van toekomstige handelingen van een buitenlandse dienst zou moeten gaan toetsen. Dit is juridisch en technisch complex maar ook in een internationale context onwenselijk.

Daarnaast is in de wet niet duidelijk neergelegd welke andere waarborgen er gelden bij de verwerking van gegevens verkregen door de inzet van een buitenlandse dienst. Te denken valt bijvoorbeeld aan het datareductiestelsel, aangezien de gegevens formeel niet afkomstig zijn uit de inzet van een bijzondere bevoegdheid. De diensten hebben aangegeven artikel 27, lid 2, overeenkomstig toe te passen op gegevens die niet door de diensten zelf zijn verworven. Met andere woorden, vertrouwelijke communicatie tussen advocaat en cliënt wordt dezelfde waarborgen toegekend, ongeacht wie die communicatie heeft verworven. Ook blijkt niet of de relevantiebeoordeling uit artikel 27, lid 1, onverkort van toepassing is wanneer de inzet van de bijzondere bevoegdheid is verricht door een partnerdienst. Ook dit zou duidelijker en transparanter in de wet kunnen worden gecodificeerd. In de tijdelijke regeling inzake verdere verwerking van bulkdatasets Wiv 2017 worden gelijke waarborgen toegekend aan bulkdatasets die verkregen zijn van buitenlandse diensten als aan bulkdatasets die diensten zelf hebben verworven. Dit volgt ook uit de aanbeveling uit §4.4.5 om te komen tot één uniform verwerkingsregime voor *alle* bulkdata, inclusief bulkdata verkregen van buitenlandse diensten. Daarnaast geldt voor het ontvangen van bulkdata dat de minister eerst akkoord moet gaan met de bulkbehoefte, alvorens de bulkdata mag worden gebruikt voor het inlichtingenproces. Zo wordt het ontvangen van bulkdata meer in lijn gebracht met de aanbevolen procedure voor het zelf verwerven van bulkdata (zie §4.3.4).

Aanbeveling 34

Leg in de wet vast dat het uniforme verwerkingsregime voor bulkdata óók geldt voor bulkdata ontvangen van buitenlandse diensten.

Aanbeveling 35

Leg in de wet vast dat voor bulkdata ontvangen van een buitenlandse dienst de minister eerst akkoord moet gaan met de bulkbehoefte alvorens deze bulkdata mag worden gebruikt voor het inlichtingenproces.

Aanbeveling 36

Leg in de wet vast dat een U-bocht constructie ten aanzien van internationale samenwerking verboden is.

8.7 Multilaterale samenwerking

Zoals ook gesignaleerd door de CTIVD, neemt multilaterale samenwerking steeds verdergaande vormen aan.[221] Voorbeelden zijn langdurige samenwerkingsverbanden in het kader van terrorismebestrijding of juist geografisch georiënteerde verbanden die gekoppeld zijn aan militaire missies.

8.7.1 Multilaterale "overzichtsnotities"

Langdurige samenwerkingsvormen kennen thans geen eigen weging van het samenwerkingsverband als geheel. Deze wordt gebaseerd op afzonderlijke wegingsnotities van de deelnemende diensten (zie §8.4), waarbij 'de zwakste schakel' veelal het niveau van samenwerking bepaalt. Gezien het grote belang van deze samenwerking en de eigen dynamiek ervan ligt het in de rede om, indachtig de wettelijke eis van weging van artikel 88, lid 2 en 3, ook voor langdurige multilaterale samenwerkingsvormen waarbinnen persoonsgegevens worden uitgewisseld na te denken over een 'zelfstandige cumulatieve overzichtsnotitie'. Een dergelijke notitie, die een andere status kan hebben dan de individuele wegingsnotities, biedt overzicht. Het specificeert hoe de individuele wegingsnotities van de partnerdiensten binnen het grotere samenwerkingsverband dienen te worden begrepen en toegepast. In een dergelijke notitie kunnen ook overwegingen met betrekking tot toezicht worden opgenomen.

Aanbeveling 37

Stel voor langdurige multilaterale samenwerking aparte overzichtsnotities op.

8.7.2 Internationaal toezicht

Door de toename van multilaterale samenwerkingsverbanden rijst ook de vraag naar multilateraal toezicht. Diensten werken soms op locatie fysiek samen of maken gebruik van gezamenlijke systemen. Zo doen zij samen aan gegevensverwerking. De CTIVD kan maar beperkt

[221] CTIVD. (2019). *Toezichtsrapport 60 over de wegingsnotities van de AIVD en de MIVD voor de internationale samenwerking met de Counter Terrorism Group- en sigint-partners.*

toezicht houden als op een systeem wordt gewerkt dat niet eigendom is van de diensten.[222] Bij multilaterale gegevensverwerking is het domein van de toezichthouder onduidelijk, want welke toezichthouder ziet toe op de gegevens en verwerking van deze gegevens?

De wet beperkt de CTIVD niet om samen te werken met toezichthouders op buitenlandse diensten. Momenteel worden er tussen zes toezichthouders in Europa ervaringen en methoden uitgewisseld. De wet biedt de CTIVD echter niet de ruimte om zonder tussenkomst van de verantwoordelijk minister staatsgeheime informatie te delen met andere toezichthouders.[223] Dat maakt het houden van toezicht in de praktijk lastig.

De minister van BZK heeft aangegeven internationale samenwerking van toezichthouders toe te juichen, maar daarbij ook benadrukt dat het weinig effect heeft wanneer de Nederlandse toezichthouder de bevoegdheid krijgt staatsgeheime informatie te delen terwijl andere toezichthouders die ruimte niet hebben.[224]

De voortrekkersrol die de CTIVD heeft ingenomen moet worden aangemoedigd en waar mogelijk gefaciliteerd. Daarnaast moet nagedacht worden over de vraag hoe bij de steeds verdergaande samenwerking van diensten ook verdergaande samenwerking van toezichthouders kan worden ingevuld en vormgegeven.

Ook kan nog worden overwogen om internationaal een voorbeeld te stellen en in de wet een bepaling op te nemen dat de CTIVD expliciet de bevoegdheid geeft om zich open te stellen voor verzoeken van niet-Nederlandse toezichthouders om onderzoek te doen, naar bijvoorbeeld de vraag hoe Nederlandse diensten met persoonsgegevens zijn omgegaan die zij van buitenlandse partners hebben ontvangen. Hiervoor is het verstrekken van staatsgeheime informatie niet noodzakelijk. Tegelijkertijd bevordert het de betrouwbaarheid van de Nederlandse diensten als samenwerkingspartner en zou hiervan een voorbeeldfunctie uit kunnen gaan.

Aanbeveling 38

Moedig de CTIVD aan en faciliteer haar in de voortrekkersrol die zij op zich heeft genomen ter bevordering van internationaal toezicht.

Aanbeveling 39

Geef de CTIVD de wettelijke bevoegdheid om onderzoek te doen naar aanleiding van een verzoek van een toezichthouder van een buitenlandse partnerdienst.

---

[222] CTIVD. (2018). *Toezichtsrapport 56 over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*.
[223] CTIVD. (2018). *Joint Statement: Strengthening Intelligence Oversight Cooperation*. Beschikbaar via **https://english.ctivd.nl/latest/news/2018/11/14/index**.
[224] *Kamerstukken II*, 2018/19, 34 588, nr. 82.

8.8 Conclusie

Internationale samenwerking is van belang voor de diensten omdat dreigingen veelal internationaal van aard zijn. Tegelijkertijd moet deze samenwerking wel met voldoende waarborgen zijn omkleed. De belangrijkste observatie van de Evaluatiecommissie ten aanzien van internationale samenwerking is dat de normering van deze samenwerking moet worden uitgebreid en versterkt, zodat deze beter is gespecificeerd en wettelijk verankerd.

De Evaluatiecommissie ziet de introductie van de wegingsnotities in de Wiv 2017 als een belangrijke versterking van deze waarborgen. Hierdoor worden eventuele risico's bij internationale samenwerking beter inzichtelijk en kunnen de juiste maatregelen worden getroffen om deze risico's te mitigeren. De Evaluatiecommissie doet een aantal aanbevelingen die zien op de wegingsnotities, waaronder het opnemen van de inrichting en effectiviteit van het toezicht als een apart wegingscriterium in de wet. Ook beveelt de Evaluatiecommissie aan om – als de wetgever dit wil toestaan – een expliciete grondslag op te nemen voor samenwerking met niet-statelijke groeperingen in het buitenland.

Daarnaast beveelt de Evaluatiecommissie aan om een aantal meer inhoudelijke normen in de wet te specificeren en te verankeren. Het gaat hierbij onder meer om een verbod op het delen van register-bulkdata van Nederlandse medeoverheden, een inspanningsverplichting tot het filteren – waar technisch haalbaar en uitvoerbaar – van kenmerken van bijzondere categorieën personen uit te verstrekken gegevens en van Nederlandse kenmerken uit te verstrekken bulkdata en de verplichting om de ontvangende dienst te verzoeken persoonsgegevens van Nederlandse burgers of ingezetenen, die voorafgaand aan verstrekking niet waren onderkend en verder niet direct relevant zijn voor het onderzoek, te verwijderen bij ontdekking. Ook moet in de wet worden opgenomen dat er geen gegevens worden gedeeld als er een reëel risico bestaat dat gebruik door de ontvangende dienst een flagrante schending oplevert van het internationaal recht, en in het bijzonder de mensenrechten en internationaal humanitair recht. Deze normen sluiten enerzijds aan bij bestaande (inter)nationale jurisprudentie, normen en praktijken en kunnen anderzijds bijdragen aan het ontwikkelen van gedeelde (Europese) normen ten aanzien van internationale samenwerking tussen inlichtingen- en veiligheidsdiensten.

Het is de Evaluatiecommissie tenslotte gebleken dat de CTIVD intensief toezicht houdt op internationale samenwerking. Dit is van groot belang gezien de risico's die hierbij bestaan. Vanwege de toenemende internationalisering en het ontstaan van multilaterale samenwerkingsverbanden beveelt de Evaluatiecommissie aan internationale samenwerking tussen toezichthouders zo veel als mogelijk te faciliteren. Nu de CTIVD algeheel toezicht houdt, ook bijvoorbeeld op het ontstaan en de inhoud van de wegingsnotities, ligt het niet in de rede de TIB een rol te geven bij de internationale verstrekking van gegevens of andersoortige vormen van internationale samenwerking, uitgezonderd waar het de inzet van door de TIB te toetsen bijzondere bevoegdheden (mede) ten behoeve van een buitenlandse dient betreft.

9 Stelsel van toezicht

9.1 Inleiding

Zoals in hoofdstuk 1 opgemerkt, is de opdracht van de Evaluatiecommissie voor een belangrijk deel gericht op evaluatie van het functioneren van het in de Wiv 2017 neergelegde stelsel van toezicht. De vraag of het toezicht thans op de juiste wijze is ingericht en of er bij de toepassing van de wet knelpunten op dit vlak zijn opgekomen, is niet goed te beantwoorden zonder op de in de Wiv 2017 gestelde normen in te gaan. In voorgaande hoofdstukken zijn de meer technische open normen van de wet behandeld, zoals relevantiebeoordeling en GDA. Dit hoofdstuk gaat in op de open normen die de rechtmatigheidstoets invullen. Kunnen de toezichthouders, gelet op de inhoud van de normen, effectief toezicht uitoefenen?

Evaluatie van het toezicht op zichzelf heeft, los van die vraag, een wezenlijke op zichzelf staande functie. Gelet op de politieke inbedding, de belangen van de nationale veiligheid en de geheimhouding van de activiteiten van de diensten, is de organisatie daarvan afwijkend van het gewone bestuurlijke en rechterlijke toezicht dat in een democratische rechtsstaat voor alle maatschappelijke activiteiten functioneert. Deze afwijkingen staan internationaal, maar met name ook in Europa, constant ter discussie, zoals blijkt uit nationale en Europese rechterlijke uitspraken sinds de inwerkingtreding van de Wiv 2017. Onderdeel van de evaluatie is dus in hoeverre die afwijkingen binnen het thans in Nederland bestaande stelsel (nog steeds) gerechtvaardigd zijn.[225]

Een hiermee samenhangend fundamenteel aspect is dat het toezicht de belangen van de burgers in het systeem moet vertegenwoordigen. Zeker omdat zij bij de dynamische ontwikkeling van de datatechnologie steeds minder zelf kunnen doen, aangezien zij in beginsel onwetend zullen zijn over het feit of hun gegevens in een massale dataverzameling zijn betrokken en daarom daar ook niet tegen kunnen ageren. Zoals uit §3.3 blijkt, is de verschuiving van individuele rechtsuitoefening naar collectieve belangenbehartiging en toezicht een trend die zich in het algemene privacyrecht voordoet. In het domein van de diensten is dat in verdubbelde mate het geval. Zo heeft bijvoorbeeld de notificatieplicht[226] bij de huidige stand van massale dataverzameling steeds minder betekenis en functioneerde de klachtenafdeling van de CTIVD de laatste jaren voornamelijk op het niveau van de individuele veiligheidsonderzoeken.

In dit hoofdstuk bespreekt de Evaluatiecommissie verschillende aspecten van het stelsel van toezicht, en doet zij aanbevelingen. Allereerst (§9.2) wordt ingegaan op de inrichting van het toezicht waarbij ook de bevoegdheden en positionering van de partijen worden besproken. Vervolgens (§9.3) wordt meer specifiek ingegaan op de invulling van de ex-ante toetsing door de TIB om in §9.4 de samenhang van deze ex-ante toetsing met het dynamisch toezicht van de CTIVD te bespreken. Daarna (§9.5) kijkt de Evaluatiecommissie vanuit een breder perspectief naar de balans in het gehele stelsel van toezicht. Tenslotte (§9.6) behandelt de Evaluatiecommissie de huidige benoemingsprocedure en de bezetting van de TIB en CTIVD.

---

[225] Zoals in hoofdstuk 3, §3.4 over Europees recht werd opgemerkt is de Europese rechtspraak een belangrijke drijfveer voor het maken van de WIV geweest; Oerlemans, J.J. (November 2020). *Grenzen stellen aan de datahonger*. p. 14 (noot 40). Oratie beschikbaar via **https://www.uu.nl/sites/default/files/UU%20oratietekst%20Jan-Jaap%20Oerlemans%2016%2011%202020.pdf**.

[226] De notificatieplicht (artikel 59 Wiv 2017) houdt in dat personen jegens wie de bijzondere bevoegdheid van het openen van het briefgeheim (artikel 44, lid 1), gerichte interceptie (artikel 47, lid 1) of binnentreden van een woning zonder toestemming (artikel 58, lid 1) is ingezet, hierover vijf jaar na beëindiging van de inzet worden genotificeerd.

9.2 Inrichting van het toezicht onder de Wiv 2017

9.2.1 Inleiding

De Wiv 2017 is een wet die de bevoegdheden van de diensten regelt om gegevens te verwerven, te bewerken en te bewaren met betrekking tot organisaties en personen die, kort gezegd, een gevaar vormen voor het voortbestaan van de democratie of de veiligheid van de staat. De wet regelt de taken, doelstelling en bevoegdheden van de AIVD en MIVD, en hoe die bevoegdheden mogen en moeten worden uitgeoefend. Daarop wordt algemeen toezicht uitgeoefend door de CTIVD die daarover niet-bindende rechtmatigheidsoordelen uitspreekt in de vorm van speciale en algemene rapporten. De betrokken ministers sturen deze rapporten en hun reactie vervolgens aan de Staten-Generaal. Dit toezicht van de CTIVD is tijdens uitoefening van bevoegdheden door de diensten (ex-nunc) en achteraf (ex-post).

Naast het toezicht door de CTIVD is met de Wiv 2017 ook toezicht vooraf geïntroduceerd door de instelling van de TIB. Dit is één van de meest in het oog springende wijzigingen van de Wiv 2017 ten opzichte van de Wiv 2002.[227] Het merendeel van de bijzondere bevoegdheden mag pas worden ingezet als de toestemming van de betrokken minister door de TIB als externe toetsende instantie (de ex-ante-toets) rechtmatig is bevonden. De oordelen van de TIB zijn bindend. Als de TIB oordeelt dat de toestemming van de betrokken minister onrechtmatig is, dan mag de dienst die bevoegdheid dus niet inzetten. Het invoeren van bindende autorisatie op de inzet van bijzondere bevoegdheden heeft de waarborgen fors versterkt. Dat is goed en belangrijk, vanwege de grote inbreuk die deze bevoegdheden kunnen maken op de privacy. De introductie van de TIB is het gevolg van kritische reacties op het wetsvoorstel in de internetconsultatie en kritiek in de *Privacy Impact Assessment* (PIA) (zie §2.1). Met het toevoegen van een onafhankelijke en bindende ex-ante toets streeft de wetgever ernaar om te voldoen aan de eisen van het EVRM.[228]

Het stelsel van toezicht bestaat hiermee uit twee onafhankelijke instanties: de TIB en de CTIVD. Hierbij heeft de TIB een rol in de autorisatiefase voorafgaand aan de inzet van (bepaalde) bijzondere bevoegdheden en de CTIVD bij het toezicht op het handelen van de diensten tijdens de uitvoering en achteraf. Bij de totstandkoming van de Wiv 2017 is gekozen voor de introductie van de TIB naast de CTIVD, omdat er sprake zou zijn van een 'slager die zijn eigen vlees keurt'[229] als de autorisatie, het toezicht en de klachtbehandeling in één hand zouden zijn. Dan zou er volgens de wetgever geen sprake meer zijn van onafhankelijkheid.[230] De wet zwijgt over de precieze relatie tussen de TIB en de CTIVD; uitgangspunt is dat het gaat om twee onafhankelijke instanties die naast elkaar bestaan en niet ondergeschikt aan elkaar zijn.[231] Om de onafhankelijkheid van zowel de TIB als de CTIVD te waarborgen, gelden zware benoemingsregels voor de leden van deze commissies.

---

[227] Wiv 2002 kende alleen een ex-ante toets voor het briefgeheim en later de inzet jegens advocaten en journalisten: Artikel 23, lid 1 van de Wiv 2002 bepaalde dat de rechtbank Den Haag voor het openen van brieven en geadresseerde zendingen, zonder goedvinden van de afzender of de geadresseerde, een rechterlijke last moest afgeven. Daarnaast gold ook per 1 januari 2016 per tijdelijke regeling een onafhankelijke toetsing op de inzet van bijzondere bevoegdheden jegens journalisten en advocaten door een tijdelijke toetsingscommissie.

[228] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 173 (MvT Wiv 2017).

[229] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 52 en 234 (MvT); *Handelingen I* 2016/17, 35, nr. 8, p. 3.

[230] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 234 (MvT). *Kamerstukken* II 2016/17, 34 588, nr. 18, p. 47 (Nota naar aanleiding van het Verslag Wiv 2017).

[231] *Kamerstukken I* 2016/17, 34 588, C, p. 24.

Toezicht en controle in brede zin

Met het toezicht en de controle op de inlichtingen- en veiligheidsdiensten zijn in Nederland verschillende instanties belast. Elk van deze instanties beziet de taakuitvoering van de diensten vanuit haar eigen optiek. Zo wordt er een rechtmatigheidstoets door de TIB uitgevoerd op de toestemming voor de inzet van de belangrijkste bijzondere bevoegdheden en verleent de rechtbank Den Haag toestemming voor de inzet van bijzondere bevoegdheden jegens journalisten en advocaten. Verder is er sprake van algemeen rechtmatigheidstoezicht op de uitvoering van de wet door de afdeling toezicht van de CTIVD en vindt klachtbehandeling plaats door de afdeling klachtbehandeling van de CTIVD.

Het beroep op de bestuursrechter is behoudens specifieke gevallen uitgesloten. Wel is er de mogelijkheid voor eenieder een klacht in te dienen tegen optreden van de betrokken ministers en de diensten zelf bij de afdeling klachtenbehandeling van de CTIVD, die daarover bindende beslissingen kan nemen. Daarnaast is er de gang naar de burgerlijke rechter om een rechtsvordering uit onrechtmatige daad tegen de staat in te dienen wegens vermeend onrechtmatig handelen van de betrokken ministers, de diensten of de toezichthouders.

Naast toezicht op rechtmatigheid verricht de Algemene Rekenkamer doelmatigheidsonderzoek met betrekking tot de diensten en voert zij de controle uit op de financiële huishouding van de diensten. Tenslotte vindt er parlementaire controle plaats door de Vaste Kamercommissies voor Defensie en voor Binnenlandse Zaken en Koninkrijksrelaties op openbare aspecten en controle door de Commissie op de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer op het geheime deel van het werk van de diensten. De commissie Dessens heeft in het kader van de evaluatie van de Wiv 2002 het gehele stelsel van toezicht tegen het licht gehouden. In het onderhavige rapport beperkt de Evaluatiecommissie zich – daarbij aansluitend bij de aan de commissie verstrekte opdracht – tot aanbevelingen met betrekking tot de rechtmatigheidstoets door de TIB en het rechtmatigheidstoezicht door de CTIVD alsmede de klachtbehandeling door de CTIVD.

In de volgende paragrafen wordt nader ingegaan op de inrichting van het stelsel door stil te staan bij zowel de TIB als de CTIVD inclusief haar afdeling klachtbehandeling. Hierop volgt de analyse en daaruit voortvloeiende conclusie van de Evaluatiecommissie ten aanzien van de inrichting van het stelsel.

9.2.2 TIB

Voorafgaand aan de inzet van een groot aantal bijzondere bevoegdheden moet de verleende toestemming van de minister voor deze inzet door de TIB worden getoetst (artikel 32, lid 2). In de toestemmingsaanvragen moeten de diensten aangeven welke bevoegdheid zij waarvoor willen inzetten. Daarbij moeten zij onderbouwen waarom die inzet volgens de diensten voldoet aan de vereisten van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid (artikel 26). Na toestemming van de minister voor de inzet wordt deze toestemming door de drie leden van de TIB getoetst op rechtmatigheid. Soms stellen zij daartoe aanvullende vragen. Als de TIB de verleende toestemming als onrechtmatig beoordeelt, mag de dienst die bevoegdheid niet inzetten (bindende ex-ante-toets). De door de minister verleende toestemming voor de inzet vervalt dan van rechtswege.

De Evaluatiecommissie is onder meer gevraagd zich te buigen over het vraagstuk van ministeriële verantwoordelijkheid in relatie tot de rol van de TIB als toetser van de ministeriële toestemming. Duidelijk is dat de bindende toets door de TIB een beperking van de ministeriële zeggenschap, en daarmee van de ministeriële verantwoordelijkheid, oplevert. Dit is echter een bewuste en staatsrechtelijk aanvaardbare keuze. Hoewel volledige ministeriële verantwoordelijkheid uitgangspunt is bij het vormgeven van de overheidsorganisatie, is het de wetgever toegestaan om in verband met de in het geding zijnde bevoegdheden, gemotiveerd een uitzondering op dat uitgangspunt te maken.[232] Gelet op de aard en strekking van de hier in het geding zijnde bevoegdheden, is een bindende toets door een toezichthouder goed verdedigbaar.

9.2.3 CTIVD afdeling toezicht

De afdeling toezicht van de CTIVD (hierna: de CTIVD) bestond al onder de Wiv 2002, en houdt in brede zin toezicht op de rechtmatigheid van het handelen van de diensten. Dat is in artikel 97, lid 3, vastgelegd in twee regels: a. toezicht op de rechtmatigheid van de uitvoering 'van hetgeen bij of krachtens de wet is gesteld,' en b. het gevraagd of ongevraagd inlichten en adviseren van de ministers over de 'geconstateerde bevindingen' van de CTIVD. Doorgaans doet de CTIVD dit in de vorm van openbare rapportages (eventueel met geheime bijlage), die door de ministers inclusief reactie aan de Staten-Generaal worden gezonden. Voor haar onderzoek heeft de CTIVD direct (fysieke) toegang tot alle relevante informatie en de systemen van de diensten. De medewerkers van de diensten zijn verplicht vragen van de CTIVD te beantwoorden.

Ondanks dat de CTIVD niet de bevoegdheid heeft om bindende oordelen te geven, is het toezicht bijzonder effectief. De aanbevelingen in de rapportages worden in de praktijk door de ministers vrijwel altijd overgenomen (zie kader §9.2.5). De CTIVD heeft de mogelijkheid om haar toezicht op rechtmatigheid naar eigen inzicht in te vullen. Een deel van het toezicht vult de CTIVD in als ex-post toezicht, waarbij na afronding van een bepaalde operatie de rechtmatigheid van het handelen van de diensten wordt onderzocht. Dit onderzoek kan ook *gedurende* de operatie al plaatsvinden, waardoor er ook sprake is van ex-nunc toezicht. Hierbij heeft de CTIVD zich de afgelopen jaren toegelegd op het houden van dynamisch toezicht waarbij de CTIVD streeft om zoveel mogelijk *real-time* mee te kijken met bepaalde handelingen. Een ander deel van het toezicht richt zich op algemene doelen, zoals de verbetering van de organisatie in het naleven van de Wiv 2017, in het bijzonder de zorgplicht, en het inschatten van kansen in de toekomst dat er (voortgaand of verminderd) sprake van onrechtmatig handelen is.

9.2.4 CTIVD afdeling klachtbehandeling

Naast de afdeling toezicht heeft de CTIVD ook een aparte klachtenafdeling (hierna: de afdeling klachtbehandeling). Deze afdeling is organisatorisch onderdeel van de CTIVD, maar functioneert onafhankelijk van de afdeling toezicht van de CTIVD. De afdeling klachtbehandeling beoordeelt of de dienst in een bepaald geval behoorlijk heeft gehandeld en doet daar bindende uitspraken over (artikel 124, lid 1). Deze afdeling behandelt in de praktijk vooral bejegeningsvraagstukken in individuele gevallen.

Onder de Wiv 2002 was de klachtenbehandeling nog neergelegd bij de Nationale ombudsman. Hierbij had de CTIVD wel een adviserende rol, de minister was namelijk verplicht om over een klacht advies te vragen aan de CTIVD. Na reactie van de minister richting de klager, had de klager de mogelijkheid om een klacht bij de Nationale ombudsman in te dienen (art. 83, Wiv 2002). De

[232] Vgl. het recente ongevraagde advies van de Afdeling advisering van de Raad van State over ministeriële verantwoordelijkheid (Bijlage *Kamerstukken II 2019/20*, 35 300, 78).

Nationale ombudsman kon hierover niet-bindende oordelen geven. Mede naar aanleiding van het advies van de commissie Dessens heeft de wetgever ervoor gekozen om deze procedure aan te passen en de CTIVD als onafhankelijke klachtinstantie aan te wijzen. In deze opzet treedt de CTIVD niet langer als interne klachtenadviescommissie op, maar geeft zij bindende oordelen. De rol als onafhankelijk klachtbehandelaar zou beter passen bij de positie van de CTIVD en zou bovendien leiden tot efficiënte behandeling van klachten vanwege de aanwezige expertise.[233] Met de Wiv 2017 is een aparte afdeling binnen de CTIVD aangewezen als klachtinstantie. De Nationale ombudsman heeft in de Wiv 2017 geen (rest)taak meer.[234]

9.2.5 Analyse van de inrichting van het stelsel van toezicht

Het stelsel van toezicht is met de Wiv 2017 op een aantal belangrijke punten gewijzigd. De Evaluatiecommissie is gevraagd het integrale stelsel te bezien, inclusief de inrichting van de TIB en de positionering van de klachtbehandeling bij de CTIVD. Naar aanleiding van gesprekken met de CTIVD heeft de Evaluatiecommissie zich ook gebogen over het al dan niet toekennen van een bindende bevoegdheid aan de afdeling toezicht van de CTIVD.

TIB

Ten aanzien van de inrichting van de TIB concludeert de Evaluatiecommissie dat de introductie van deze toezichthouder van grote meerwaarde is voor het toezichtstelsel. De ex-ante-toets is een belangrijke waarborg die aan het systeem is toegevoegd.

De TIB heeft enorm veel werk verzet in korte tijd. Zij heeft zich razendsnel operationeel weten te maken en is in staat gebleken om de aanvragen vanaf het begin snel en grondig te beoordelen. Er is terecht veel waardering voor haar werk. De diensten hebben mede door de toetsing door de TIB de vorm en inhoud van de aanvragen voor het inzetten van bijzondere bevoegdheden naar een professioneler niveau getild. Dit heeft het aantal onrechtmatigheidsverklaringen uit de eerste periode drastisch verminderd, zodat thans nog ongeveer 1,7% (AIVD) resp. 3,1% (MIVD) van de lasten onrechtmatig wordt verklaard.[235] Dit zijn in het algemeen de complexe zaken waarover tussen de diensten, de ministeries en de toezichthouders (soms diepgaande) verschillen van opvatting bestaan, zoals hierna nader zal worden toegelicht. Dat de cyclus van toestemmingsaanvragen zonder grote onderbreking heeft kunnen continueren, is een prestatie van formaat. De TIB heeft haar autorisatietaak zeer serieus opgevat en is na twee jaar zeker niet te kwalificeren als 'alibi'[236] of 'stempelmachine'[237], waarvoor bij de totstandkoming van de wet werd gevreesd. De openbare jaarverslagen van de TIB dragen bovendien bij aan de voorzienbaarheid voor het publiek en de parlementaire toetsing op het werk van de diensten.[238]

De TIB speelt verder een belangrijke rol in het scherp houden van de diensten in hun overwegingen om bijzondere bevoegdheden in te zetten. Niet alleen heeft dit tot verbeteringen van de interne procedures van de diensten geleid,[239] de Evaluatiecommissie ziet ook het belang van de rol van de TIB in het maatschappelijke debat. De openbare jaarverslagen dragen in belangrijke mate bij aan de transparantie en publieke verantwoording over het werk van de diensten. De beoogde doelstelling van de wet is voor wat dit betreft gehaald. Om deze redenen vindt de

[233] Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen.* p. 145- 152.
[234] *Kamerstukken II* 2016/17, 34 588, 3, p. 181-183 (MvT Wiv 2017).
[235] TIB. (2020). *Jaarverslag 2019-2020.*
[236] *Kamerstukken II* 2016/17, 34 588, nr. 4, p.16.
[237] *Handelingen II* 2016/17, 50-10, p. 5, 37, 61.
[238] TIB. (2018). *Voortgangsbrief TIB*; TIB. (2019). *Jaarverslag 2018-2019*; TIB. (2020). *Jaarverslag 2019-2020.*
[239] Zie de TIB-jaarverslagen. TIB. (2019). *Jaarverslag 2018-2019*; TIB. (2020); *Jaarverslag 2019-2020.*

Evaluatiecommissie dat de TIB moet blijven bestaan als orgaan dat in de autorisatiefase de rechtmatigheid van de toestemming voor de inzet van bepaalde bijzondere bevoegdheden bindend toetst. Wel is er een aantal aspecten van de toetsing door de TIB dat bijzondere aandacht behoeft. Dit wordt besproken onder §9.3.

CTIVD, afdeling toezicht

De inrichting van de afdeling toezicht van de CTIVD is zoals reeds gezegd niet nieuw ten opzichte van de Wiv 2002. Met de Wiv 2017 is niet gekozen voor een fundamentele wijziging van de inrichting van deze toezichthouder. De commissie Dessens deed de aanbeveling om de CTIVD de mogelijkheid te geven om een bindend rechtmatigheidsoordeel uit te spreken, in plaats van een preventieve (ex-ante-)toets op de inzet van bijzondere bevoegdheden.[240] Het kabinet en de Kamer besloten uiteindelijk voor het omgekeerde: introductie van de TIB en géén bindende rechtmatigheidsoordelen van de CTIVD. In reactie op het rapport van commissie Dessens gaf het kabinet aan dat de ministers volledig verantwoordelijk zouden moeten blijven voor het opereren van de diensten en dat het daarom niet wenselijk was om over te gaan tot het mogelijk maken van bindende oordelen door de afdeling toezicht van de CTIVD.[241] De introductie van de TIB volgde later.

De Evaluatiecommissie ziet het toezicht van de CTIVD op de diensten als een zeer belangrijke waarborg. De CTIVD heeft de benodigde kennis en expertise om haar toezichtstaken zorgvuldig uit te voeren. De toezichthouder heeft zich de afgelopen jaren doorontwikkeld op technisch vlak, onder meer door de oprichting van de ICT-unit.[242] De Evaluatiecommissie ziet grote meerwaarde in deze technische expertise. Sinds de inwerkingtreding van de Wiv 2017 heeft de CTIVD met haar voortgangsrapportages over de implementatie van de wet bovendien een belangrijke bijdrage geleverd aan het politieke en publieke debat. De kritische oordelen van de CTIVD over de implementatie van de wet hebben er mede toe geleid dat de diensten veel verbeteringen hebben doorgevoerd, met name op organisatorisch en ICT-gebied zoals de professionalisering van de systemen voor gegevensverwerking. Dit ziet de Evaluatiecommissie als een belangrijke ontwikkeling, omdat dit bijdraagt aan het systeemtoezicht door de CTIVD.

Interne controle en zorgplicht bij de diensten

Een belangrijk onderdeel van het wettelijke stelsel van toezicht is het interne toezicht door de diensten zelf. Dit vloeit voort uit de zogeheten zorgplicht (artikel 24) voor de diensten om technische, personele en organisatorische maatregelen te nemen om te komen tot een rechtmatige gegevensverwerking. Deze zorgplicht is een belangrijke interne waarborg op het werk van de diensten. Op basis van deze zorgplicht moeten de diensten controle hebben op de gegevensverwerking en hier ook verantwoording over kunnen afleggen. Dit vraagt om een juist instrumentarium dat zicht geeft op de werking van processen en systemen van gegevensverwerking.[243]

---

[240] Evaluatiecommissie Dessens (2013). *Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*. p. 99-106.

[241] *Kamerstukken II* 2013/14, 33 820, nr. 2, p. 6.

[242] Zie onder meer **https://www.ctivd.nl/over-ctivd/ict-unit-en-technisch-onderzoek**. **https://www.ctivd.nl/over-ctivd**

[243] Zie ook de behandeling van het thema zorgplicht in de vier voortgangsrapportages van de CTIVD.

Sinds de inwerkingtreding hebben de diensten hierop grote stappen gezet.[244] De Evaluatiecommissie beschouwt de inbedding van zorgplicht en controle op de gegevensverwerking als cruciaal voor effectieve interne controle door de diensten zelf en effectief dynamisch- en systeemtoezicht door de CTIVD. De Evaluatiecommissie moedigt een verdere versterking van interne controlemechanismen op gegevensverwerking dan ook aan. De Evaluatiecommissie benadrukt het belang van een hoogwaardige datahuishouding voor deze (interne) controle op de gegevensverwerking. De ingezette ontwikkeling richting een gezamenlijke datahuishouding van de AIVD en MIVD is belangrijk. Tegelijkertijd kosten deze doorontwikkelingen van het ICT-landschap de nodige tijd en middelen.

Op ICT-gebied bleek bij de invoering van de Wiv 2017 dat de wet op technisch vlak vele malen lastiger uit te voeren was dan op voorhand was voorzien. De invoering van de Wiv 2017 heeft dan ook veel gevraagd van de ICT-capaciteit van beide diensten, mede door de achterstand in de ontwikkeling van het ICT-landschap bij de MIVD.[245] Ondertussen moeten de diensten ook blijven draaien. In het vervolg zou een ICT-uitvoeringstoets bij wijzigingen van de wet dan ook verstandig zijn.

De Evaluatiecommissie heeft zich gebogen over de vraag of de rechtmatigheidsoordelen van de afdeling toezicht van de CTIVD een bindend karakter zouden moeten krijgen. Hierbij is gekeken naar de vereisten die volgen uit Europeesrechtelijke ontwikkelingen en de mate van effectiviteit van het huidige toezicht van de CTIVD. Voorop moet worden gesteld dat Europa zeer uiteenlopende stelsels van toezicht kent, waardoor een vergelijking tussen stelsels niet makkelijk is.[246] Voor een beoordeling van het vereiste van effectief toezicht moet de doeltreffendheid van het stelsel als geheel worden beschouwd.[247] In het kader hieronder wordt uiteengezet dat het internationale recht daartoe ook niet noopt.

Internationaal recht

Dataprotectieverdrag C-108

Op 10 oktober 2018 is het protocol tot wijziging van het dataprotectieverdrag C-108 van de Raad van Europa door Nederland ondertekend (zie ook §3.3.2). Met het protocol, ook wel 'Conventie 108+' genoemd, wordt het verdrag gemoderniseerd en meer in lijn gebracht met EU-privacywetgeving.

Eén van de wijzigingen is dat het niet meer mogelijk is voor landen om bepaalde vormen van dataverwerking, zoals in het kader van de nationale veiligheid, op voorhand uit te sluiten.[248] Uit het protocol volgt onder meer dat er in de lidstaten sprake moet zijn van

[244] CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 8-9.
[245] Zie de verschillende voortgangsrapportages van de CTIVD.
[246] Zie onder meer de verschillende rapportages van de *European Union Agency for Fundamental Rights* (FRA), via **https://fra.europa.eu/en/publication/2017/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies-eu**.
[247] *Kamerstukken II* 2016/17, 34 588, nr. 4, p. 22 en 41.
[248] Council of Europe. *The modernised Convention 108: novelties in a nutshell*. Beschikbaar via **https://rm.coe.int/modernised-conv-overview-of-the-novelties/16808accf8**.

effectief toezicht op inlichtingen- en veiligheidsdiensten. In het protocol zijn de nodige uitzonderingsmogelijkheden op de normale regels die gelden voor dataprotectie opgenomen. Die zien onder meer op de bevoegdheden van de toezichthouders in het kader van nationale veiligheid.

De ratificatie van het protocol tot wijziging van het verdrag voor Nederland is in voorbereiding. Goedkeuring zal plaatsvinden bij wet. Het is op dit moment nog niet bekend of en zo ja, welke uitzonderingen en beperkingen op het verdrag door de Nederlandse wetgever zullen worden ingeroepen en welke keuzes daarbij zullen worden gemaakt. De goedkeuringswet voor het verdrag zal zo nodig in implementatiebepalingen voorzien. Die bepalingen zullen in de behandeling van het wetsvoorstel onderwerp van debat zijn tussen de regering en de Staten-Generaal. Aan het inroepen van een uitzondering of beperking stelt het verdrag de voorwaarde dat deze noodzakelijk en evenredig moet zijn in een democratische samenleving. De vraag of daarvan sprake is, zal door de wetgever in het democratisch proces moeten worden beantwoord.

Het protocol codificeert de lijnen die volgen uit de Europese jurisprudentie ten aanzien van artikel 8 en 13 van het EVRM. Het gaat dan in het bijzonder om de criteria die het EHRM heeft geformuleerd in §3.4.1 over het Europese recht en toezicht.[249] Het EHRM toetst het stelsel van toezicht als geheel op effectiviteit. Door verschillende gesprekspartners is tijdens de evaluatie naar voren gebracht dat de uitzonderingsclausule zo beperkt is geformuleerd, dat Nederland verplicht zou zijn om over de gehele linie (zowel ex-ante als ex-post) bindend rechtmatigheidstoezicht in te voeren. De Evaluatiecommissie deelt, alles afwegende, die mening niet. De vereiste beoordeling van het systeem als geheel noopt tot de conclusie dat effectief ex-ante toezicht bindend moet zijn, maar in het ex-post toezicht effectiviteit beter langs een andere weg kan worden bereikt. Wel is de Evaluatiecommissie van oordeel dat het uiteindelijke bindende oordeel over de rechtmatigheid van de inzet van bevoegdheden bij de onafhankelijke rechter moet liggen. Daarvoor doet de Evaluatiecommissie in §9.5 over de balans van het stelsel afzonderlijke voorstellen.

Het HvJEU

Voor zover het HvJEU zich in recente jurisprudentie[250] uitspreekt over eisen die aan het toezicht moeten worden gesteld, zoals een bindende ex-ante toets bij verplichtingen aan aanbieders van communicatiediensten[251], zijn deze reeds verankerd in de Wiv 2017 en vormen zij op deze wijze effectieve waarborgen. Dat ligt mogelijk anders voor de verplichting ex artikel 55 Wiv 2017 tot *real time collection* van metadata, waarvoor in de huidige wet geen bindende ex-ante toets geldt.[252] Zie voor een meer uitgebreide duiding van deze rechtspraak §3.4 en §4.3.1.

Bij het beoordelen van de effectiviteit van het toezicht moet allereerst een scherp onderscheid worden gemaakt tussen ex-ante en ex-post toezicht. Effectief ex-ante toezicht is niet goed denkbaar als het niet bindend is. Er moet een *go/no-go* beslissing worden genomen. Bij ex-post toezicht is dat niet zonder meer vanzelfsprekend. Daarbij moet naar het oordeel van de

[249] EHRM 4 december 2015, (*Roman Zakharov*), r.o. 249, 267, 285.
[250] HvJ EU 6 oktober 2020, (*Quadrature du Net and others*).
[251] Zie artikelen 53, lid 2, 54, lid 2, en 57, lid 2, Wiv 2017.
[252] HvJEU 6 oktober 2020, (*Quadrature du Net and others*), r.o. 192.

Evaluatiecommissie de aard en intensiteit van het toezicht en de specifieke rol van de verschillende spelers in acht worden genomen. De Evaluatiecommissie is van oordeel dat niet-bindend toezicht daar effectiever kan zijn. In de praktijk blijkt dat het toezicht van de CTIVD bijzonder effectief is. De aanbevelingen van de CTIVD worden door de ministers vrijwel zonder uitzondering overgenomen. Als zij ervoor kiezen dat naast zich neer te leggen, dan kan het parlement de ministers ter verantwoording roepen. Sinds de inwerkingtreding van de Wiv 2017 zijn vier aanbevelingen van de CTIVD niet door de ministers overgenomen (zie kader hierna). Het gaat hierbij om verschillen van opvatting over de uitleg van wetsbepalingen. Het is in de ogen van de Evaluatiecommissie de vraag of dat probleem door het bindend maken van de aanbevelingen niet erger wordt gemaakt.

Niet door de ministers overgenomen aanbevelingen van de CTIVD

Sinds inwerkingtreding van de Wiv 2017 heeft de CTIVD acht openbare toezichtsrapporten uitgebracht die betrekking hadden op activiteiten van de diensten onder de Wiv 2017.[253] In deze acht rapporten deed de CTIVD in totaal 74 aanbevelingen.[254]

De betrokken ministers hebben alle aanbevelingen overgenomen, met uitzondering van de volgende vier aanbevelingen uit twee rapporten:

1. CTIVD rapport nr. 65: dezelfde aanbeveling voor zowel de AIVD als de MIVD om de definities van ongeëvalueerd en geëvalueerd in beleid en werkinstructies overeenkomstig het toetsingskader van de CTIVD aan te passen.[255] De betrokken ministers reageren dat zij op dit punt van inzicht verschillen en dat de door hen gehanteerde uitleg van de begrippen aansluit bij de wet en parlementaire behandeling (zie ook §5.4.4).[256]
2. CTIVD rapport nr. 70: twee aanbevelingen tot vernietiging van desbetreffende bulkdatasets. Naast vernietiging van één bulkdataset vanwege ontbreken geldige toestemming wordt ook aanbevolen de betreffende bulkdatasets te vernietigen vanwege het onrechtmatigheidsoordeel van het als integraal relevant aanmerken van deze bulkdatasets.[257] De betrokken ministers reageren dat de beoordeling op relevantie een open norm is en dat de wijze waarop de diensten hieraan invulling hebben gegeven past binnen het huidige wettelijk kader. De ministers gaan niet over tot vernietiging van de betreffende bulkdatasets (zie ook §5.4.4). Ten aanzien van de ontbrekende toestemming zijn de

[253] In juni 2018 heeft de CTIVD het toezichtsrapport nr. 58 uitgebracht over de uitvoering van inzageverzoeken bestuurlijke aangelegenheden door de AIVD en de MIVD. Dit rapport kwam uit na inwerkingtreding van de Wiv 2017 maar heeft betrekking op een periode onder de Wiv 2002. Eén van de in totaal 21 aanbevelingen is niet overgenomen door de betrokken minister. Zie: *Kamerstukken II*, 2017/18, 29 924, nr. 166.

[254] Het gaat om de toezichtsrapporten nrs. 60, 63, 64, 65, 67, 68, 70 en 71. In totaal worden er 74 aanbevelingen gedaan, ten aanzien van beide diensten (eventueel gezamenlijk) of ten aanzien van één van de twee diensten. Zie ook **https://www.ctivd.nl/onderzoeken**. Daarnaast heeft de CTIVD ook vier voortgangsrapportages gepubliceerd over de invoering van de Wiv 2017. In deze rapportages worden geen aanbevelingen gedaan maar rapporteert de CTIVD over de risico's op onrechtmatig handelen.

[255] CTIVD. (2019). *Toezichtsrapport 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD*. p. 23-24.

[256] *Kamerstukken* 2020/21, 29 924, 193, p.2-3 (Beleidsreactie CTIVD rapport nr. 65).

[257] CTIVD. (2020). *Toezichtsrapport nr. 70 over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD*. p. 24-25.

ministers het niet eens met de juridische duiding van de CTIVD en wordt daarom ook niet overgegaan tot vernietiging.[258]

In beide gevallen is de discussie terug te voeren op de invulling van het wettelijke vereiste om gegevens uit bijzondere bevoegdheden op relevantie te beoordelen. Dit heeft ten aanzien van bulkdata geleid tot verschillende interpretaties over de wijze waarop deze beoordeling dient plaats te vinden (zie §4.4.4).

Het afdwingen van aanbevelingen door middel van boetes zoals bij regulier markttoezicht het geval is, ziet de commissie niet als een oplossing gezien de bijzondere aard van het toezicht op de diensten. Dit toezicht is zeer intensief op één partij gericht (beide diensten) waarbij het zich ook heeft doorontwikkeld tot *real-time* toezicht. Hierbij kan het afdwingen van aanbevelingen zelfs nadelig werken. Dit sluit bovendien niet aan op het reguliere stelsel van strafrecht en punitief bestuursrecht, waar de Staat immuun is en andere openbare lichamen dat ook zijn voor zover zij een publieke taak behartigen.[259] Het is juist de huidige constructieve dialoog tussen de diensten en de CTIVD die van grote meerwaarde is voor het waarborgen van een goede taakuitoefening door de diensten. Hierbij nemen de diensten en de CTIVD – ieder vanuit de eigen rol – deel aan nuttige overleggen over onder meer de implementatie van de Wiv 2017. Ook bezien de CTIVD en diensten gezamenlijk de mogelijkheid voor het uitbreiden van toezichtsfunctionaliteiten in bijvoorbeeld applicaties, ten behoeve van het dynamisch toezicht van de CTIVD. Juist vanwege de complexe (technologische) en gevoelige aard van de materie, brengt een dergelijke dialoog een hoge mate van effectiviteit van het toezicht met zich. Introductie van bindende te sanctioneren oordelen van de CTIVD heeft als risico dat deze constructieve dialoog wordt geschaad. Bovendien vindt de Evaluatiecommissie het ook principieel niet passend dat een toezichthouder het laatste woord heeft over de uitleg van wetsbepalingen (zie §9.5). Op dit punt doet de Evaluatiecommissie dus geen aanbevelingen tot aanpassing.

CTIVD, afdeling klachtbehandeling

De afdeling klachtbehandeling van de CTIVD behandelt klachten over het optreden van de diensten. Daarnaast is zij belast met de behandeling van meldingen inzake vermoedens van misstanden. In het kader van haar opdracht heeft de Evaluatiecommissie bezien of de positionering van de klachtbehandeling bij de CTIVD vanuit het burgerperspectief het indienen van klachten belemmert.[260] De behandeling van klachten door de afdeling klachtbehandeling lijkt goed te verlopen. De afdeling heeft zelfstandig toegang tot informatie en medewerkers van de diensten en korte lijnen bij interventies. Daarnaast beschikt de afdeling over veel expertise, niet alleen ten aanzien van klachtbehandeling maar ook over de diensten en de Wiv 2017. De Evaluatiecommissie heeft de indruk dat de afdeling zorgvuldig tot haar bindende oordelen komt.

In de evaluatie is gebleken dat door zowel de afdeling klachtbehandeling als de Nationale ombudsman vanuit het perspectief van de burger geen verhoogde drempel voor het indienen van klachten wordt gezien. Qua hoeveelheid klachten die in de tweede lijn worden behandeld, zijn er nauwelijks verschillen waar te nemen tussen de situatie onder de Wiv 2002 en de huidige

[258] *Kamerstukken* 2020/21, 29 924, 203, p.3 (Beleidsreactie CTIVD rapporten nr. 70 en 71).
[259] HR 6 januari 1998, ECLI:NL:HR:1998:AA9342, (*Pikmeer II*); *NJ* 1998/367 m.nt. JdH, *AB* 1998/45 m.nt. ThGD; *JB* 1998/4, *AB- klassiek,* 7e druk, Deventer: Kluwer 2016 nr. 24 m.nt. T. Barkhuysen en M.L. van Emmerik.
[260] *Kamerstukken II* 2019/20, 34 588, nr. 84 (Kamerbrief opdracht evaluatie).

situatie. In beide gevallen ging/gaat het om enkele klachten per jaar. Meldingen van vermoedens van misstanden zijn door de afdeling klachtbehandeling tot op heden niet ontvangen.

Ook is gebleken dat de interne klachtbehandeling bij de diensten goed op orde is. De afdeling klachtbehandeling van de CTIVD verwijst burgers die niet eerst bij de diensten hebben aangeklopt met hun klacht terug naar de diensten. Het blijkt dat veel klachten daar behoorlijk en naar tevredenheid van de klager worden behandeld. De Evaluatiecommissie vindt dit een belangrijk en positief signaal.

De Evaluatiecommissie constateert dat de afdeling klachtbehandeling tot nu toe geen klachten van maatschappelijke organisaties met een collectief karakter heeft behandeld. Daarop wordt in §9.6 verder ingegaan. In dit verband is een relevant verschil met de situatie van voor de Wiv 2017 dat de Nationale ombudsman de bevoegdheid had om onderzoek uit eigen beweging te doen, waar de afdeling klachtbehandeling van de CTIVD dat niet heeft. De afdeling klachtbehandeling kan alleen naar aanleiding van een klacht een onderzoek starten. Dat is ook begrijpelijk vanwege de bevoegdheid om bindende uitspraken te doen die de afdeling klachtbehandeling heeft en de Nationale ombudsman niet. Van deze mogelijkheid is in de Wiv 2017 afgezien omdat dit spanning zou opleveren met de bevoegdheid van de afdeling toezicht van de CTIVD om wel uit eigen beweging onderzoek te starten waarbij géén bindende oordelen kunnen worden uitgesproken.[261]

De Evaluatiecommissie ziet geen reden om een aanbeveling te doen met betrekking tot de inrichting van de huidige klachtbehandeling of de behandeling van meldingen inzake vermoedens van misstanden. De keuze van de wetgever om de afdeling klachtbehandeling niet de bevoegdheid te geven onderzoek uit eigen beweging te starten is begrijpelijk. Hiermee zou overlap ontstaan met de afdeling toezicht van de CTIVD die reeds over deze bevoegdheid. Wel komt de Evaluatiecommissie tot aanbevelingen met betrekking tot de toegang voor maatschappelijke organisaties tot de klachtbehandeling (zie §9.5.4).

9.2.6 Aanbevelingen

De Evaluatiecommissie vindt dat het stelsel van toezicht zich in twee jaar tijd goed heeft gezet en dat het toezicht op het handelen van de diensten hiermee stevig is ingebed. De TIB is van grote meerwaarde gebleken en de kwaliteit en toegankelijkheid van de klachtbehandeling zijn, bezien vanuit het burgerperspectief, niet veranderd. Daarnaast wordt het toezicht door de CTIVD zorgvuldig en effectief ingevuld en vormt het daarmee een belangrijke waarborg in het stelsel. De Evaluatiecommissie ziet dan ook, mede gelet op de korte evaluatieperiode, geen noodzaak om op dit moment inhoudelijke aanbevelingen te doen met betrekking tot de juridische structuur van het toezicht.

Aanbeveling 40

De TIB blijft in haar huidige vorm bestaan met behoud van de bevoegdheid om bindend ex-ante te toetsen.

[261] *Kamerstukken II 2016/17*, 34 588, nr. 3, p. 182 (MvT Wiv 2017).

Aanbeveling 41

De CTIVD afdeling toezicht blijft in haar huidige vorm bestaan met behoud van de huidige bevoegdheden.

Aanbeveling 42

De afdeling klachtbehandeling van de CTIVD blijft in haar huidige vorm bestaan met behoud van het bindend oordeel.

Ondanks bovenstaande constateringen meent de Evaluatiecommissie dat er belangrijke punten bij de invulling van het toezicht zijn die aandacht behoeven. Dit raakt zowel de inhoud van de normstelling als de toepassingspraktijk van de ex-ante toets. Discussie hierover heeft geleid tot spanningen binnen het stelsel die in de volgende paragraaf worden besproken. Een complicerend aspect in het stelsel van toezicht is dat de relatie ex-ante en ex-post toezicht bij de invoering van het stelsel niet goed is doordacht. Dit wordt in §9.4 geanalyseerd. Ten slotte ziet de Evaluatiecommissie het als een gemis dat in het systeem een duidelijke geschiloplossing door de rechter over interpretatievragen ontbreekt. Daarover doet zij een aanbeveling (zie §9.5). Een ander tekort in het stelsel is dat bij de huidige stand van de techniek de burger (ook niet in de vorm van algemeen belang behartigende organisaties) in het stelsel is ondervertegenwoordigd. Hoewel de klachtenafdeling van de CTIVD hiervoor bevoegd is, heeft zij op dit vlak in de sinds de inwerkingtreding van de Wiv 2017 geen rol gespeeld. Het voorstel van mogelijke rechterlijke toetsing ziet ook op dit aspect.

9.3 De invulling van de ex-ante-toets door de TIB

9.3.1 Inleiding

Bij de rechtmatigheidstoets kijkt de TIB naar de vereisten van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid. Dit betreft een volle toets.[262] In de praktijk is te zien dat de TIB een brede invulling geeft aan de rechtmatigheidstoets die zij uitvoert. Zo betrekt de TIB bij de toets op de rechtmatigheid van het verzamelen van gegevens (verwerving) soms ook aspecten van wat de diensten met die gegevens gaan doen (verwerking), zoals het oogmerk om gegevens te delen met buitenlandse partners. Deze aspecten neemt zij mee in haar weging, bijvoorbeeld om te bezien of de inzet proportioneel is. Op basis van de voorgenomen verwerking van gegevens wordt een toestemming soms als onrechtmatig beoordeeld, of worden er voorwaarden gesteld aan de inzet. Ook weegt de TIB soms in detail mee *hoe* de inzet van een bevoegdheid plaatsvindt en bijvoorbeeld welke bepaalde (technische) risico's daarmee gepaard gaan.

Tegelijkertijd is de toets door de TIB per definitie een statische toets doordat deze voorafgaand aan de daadwerkelijke inzet plaatsvindt. Zeker bij technisch meer complexe operaties zoals de inzet van de hackbevoegdheid is op voorhand niet altijd in detail aan te geven hoe de inzet er precies uit gaat zien (zie §7.3). Ook is het inzicht in de aard van te verwerven gegevens vooraf

[262] *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 39 (Nota naar aanleiding van het Verslag Wiv 2017).

beperkt, waardoor de wijze van verwerking nog niet bekend is. Hetzelfde geldt voor de bulkverwerving. Wel heeft de TIB een toetsende rol bij verlengingsverzoeken van deze bijzondere bevoegdheden. Dit heeft een andere dynamiek omdat bij verlengingen wel bekend is hoe de inzet is verlopen. Zo worden dynamische aspecten van het toezicht bij de toets op verlenging geïntroduceerd.

De brede invulling van de TIB enerzijds en de wrijving tussen de statische aard van de toets en de dynamische uitvoering van de bevoegdheid anderzijds, behoeft aandacht omdat zij in de praktijk tot patstellingen leiden. De Evaluatiecommissie licht in de volgende paragrafen deze knelpunten toe en doet hierop aanbevelingen.

9.3.2 Het stellen van voorwaarden

Het komt in de praktijk voor dat de TIB bepaalde voorwaarden verbindt aan een rechtmatigheidsoordeel.[263] Dat betekent dat de TIB een toestemming van de minister als rechtmatig beoordeelt, mits aan een aantal voorwaarden wordt voldaan bij de uitvoering. De dienst kan dan toch verder met de inzet maar moet hierbij wel de voorwaarden in acht nemen. Het stellen van voorwaarden is niet in de wet voorzien. De Evaluatiecommissie is gevraagd zich te buigen over deze 'geclausuleerde goedkeuring'.[264]

Vooropgesteld staat dat het aan de minister is om toestemming te verlenen voor een bepaalde operatie en daaraan voorschriften en voorwaarden te verbinden voor het vervolgtraject van die operatie. Die voorwaarden kunnen bijvoorbeeld voortvloeien uit de zorgplicht van de diensten. Welke regels van toepassing zijn, moet duidelijk worden vastgelegd in de toestemmingsaanvraag. De TIB toetst die toestemming met inachtneming van de door de minister gestelde voorschriften en voorwaarden en geeft aan of die toestemming wel of niet rechtmatig is.

De wet voorziet niet in een mogelijkheid voor de TIB om voorwaarden te stellen aan de toestemming van de minister en daarmee een geclausuleerd rechtmatigheidsoordeel te geven. Een dergelijke voorwaardelijke toestemming verdraagt zich ook niet met het karakter van deze rechtsfiguur. Het roept namelijk de vraag op wat het rechtsgevolg is van het niet naleven van de voorwaarden: vervalt dan de toestemming (ex-nunc of met terugwerkende kracht)? Of blijft de toestemming bestaan, en is alleen het niet naleven van de voorwaarden onrechtmatig? En wat als een gedeelte van de voorwaarden wel, en een gedeelte niet wordt nageleefd? Het is dan ook een kernelement van preventief toezicht dat de toezichthouder alleen 'ja' of 'nee' kan zeggen tegen het besluit. Daarom is dit toezicht ook bindend. Dit wordt ook wel aangeduid met de metafoor van de slagboom: óf de slagboom blijft naar beneden, en de auto kan niet verder, of de slagboom gaat omhoog, en dan rijdt de auto verder. Half omhoog gaat niet.[265] De Evaluatiecommissie heeft opgemerkt dat de TIB aan de hand van verlengingen van eerder, onder voorwaarden verleende,

---

[263] Zie onder andere het TIB-jaarverslag 2018-2019, p. 14 (geclausuleerd rechtmatigheidsoordeel ten aanzien van kabelinterceptie) en TIB-jaarverslag 2019-2020, p. 10 (geclausuleerd rechtmatigheidsoordeel ten aanzien van GDA artikel 50, eerste lid onder b).

[264] *Kamerstukken II* 2019/20, 35 242, 6, p. 6 (Nota naar aanleiding van het Verslag Wijziging Wiv 2017).

[265] In dit kader is het nuttig om te kijken naar de Algemene wet bestuursrecht (Awb). Alhoewel de Awb niet van toepassing is op de Wiv 2017, biedt deze wet op basis van algemene leerstukken van bestuursrecht goede aanknopingspunten voor de vraag hoe om te gaan met goedkeuring. Artikel 10:25 Awb definieert goedkeuring als: de voor de inwerkingtreding van een besluit van een bestuursorgaan vereiste toestemming van een ander bestuursorgaan. Bij de procedure van de TIB gaat het formeel niet om goedkeuring in de zin van deze bepaling, maar alleen omdat de TIB ingevolge artikel 1:1, lid 2, Awb geen bestuursorgaan is. *Materieel* is de procedure wel als goedkeuring te beschouwen. Artikel 10:29 Awb bepaalt uitdrukkelijk dat de goedkeuring niet onder voorwaarden kan worden verleend.

toestemmingen toeziet op de naleving van die voorwaarden. De ex-ante rol wordt hiermee diffuus.

De Evaluatiecommissie ziet het gebruik van geclausuleerde goedkeuringen als een uiting van spanning binnen het stelsel van toezicht. Deze spanning is het gevolg van het gebrek aan een duidelijke afbakening van rollen en een helder omschreven toetsingskader. De Evaluatiecommissie vindt dat gebruik van geclausuleerde goedkeuring niet past bij de autoriserende rol van de TIB. Niet alleen verhoudt dit zich niet tot de beginselen van preventief toezicht, ook is het aan de minister om vanuit diens verantwoordelijkheid voor de uitvoering door de diensten voorwaarden te stellen aan deze uitvoering. De TIB toetst vervolgens de rechtmatigheid van de toestemming inclusief deze voorwaarden als zodanig.

Aanbeveling 43

Maak het gebruik van de figuur van de geclausuleerde toestemming niet mogelijk.

9.3.3 Object en normstelling TIB-toets

De Evaluatiecommissie constateert dat de TIB een volle rechtmatigheidstoets uitvoert, en dat ook moet doen.[266] De belangen die door de TIB-toets worden beschermd vragen om een volle rechtmatigheidstoets, waaronder de volle evenredigheidstoets. De wijze waarop de TIB toetst, wordt door de diensten soms ervaren als een doelmatigheidstoets, waarvan zij menen dat die het domein is van de ministeriële verantwoordelijkheid. Het gaat hier echter om een schijntegenstelling. Inderdaad dient de TIB niet te beoordelen of daadwerkelijk sprake is van een gevaar voor de veiligheid van de staat of één van de andere, door de Wiv 2017 omschreven belangen. Maar een evenredigheidstoets houdt wel in dat, gegeven het betrokken gevaar, wordt getoetst of de gekozen middelen niet zwaarder zijn dan het belang rechtvaardigt, of er minder zware middelen zijn om hetzelfde doel te bereiken, en of die inzet zo gericht mogelijk is. Dit vergt wel degelijk een vorm van doelmatigheidstoets. Deze volle toets past bij de in het geding zijnde belangen en is in lijn met de jurisprudentie op andere delen van het bestuursrecht.[267] De invulling van de evenredigheidstoets moet primair worden bepaald door de in het geding zijnde belangen: hoe ingrijpender de bevoegdheden en hoe groter het belang van de burger, hoe indringender de toetsing.

Wel is het van belang dat duidelijk is wat het object van deze volle toets is en welke interpretatie wordt gegeven aan de normstelling. Binnen deze kaders vindt vervolgens een volle toets op rechtmatigheid plaats door de TIB. De Evaluatiecommissie meent dat aandacht moet worden besteed aan het object en de normstelling zoals die worden toegepast in de praktijk.

Object: OOG-interceptie

In de Wiv 2017 is bepaald dat de TIB de toestemming van de minister voor de inzet van bepaalde bijzondere bevoegdheden toetst op rechtmatigheid (artikel 32, lid 2). De wetgever heeft deze bevoegdheden onderworpen aan de TIB-toets omdat deze potentieel als het meest inbreukmakend worden gezien.[268] Met uitzondering van drie bijzondere bevoegdheden – namelijk

[266] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 53-54 (MvT Wiv 2017).
[267] Hirsch Ballin, E.M.H. (2015). 'Dynamiek in de bestuursrechtspraak', in: *Rechtsontwikkeling door de bestuursrechter*, VAR-reeks nr. 154, Den Haag: BJu 2015.
[268] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 53 (MvT Wiv 2017).

search gericht op selectie (artikel 49, lid 2), selectie (artikel 50, lid 1, onder a) en geautomatiseerde data-analyse (GDA) (artikel 50, lid 1, onder b) – zien deze bevoegdheden op verwerving van (nieuwe) gegevens.[269]

In de toelichting op de Wiv 2017 staat dat de TIB bij haar toets kijkt naar de toepassing van de eisen zoals neergelegd in artikel 26: subsidiariteit, proportionaliteit en noodzakelijkheid.[270] Dit zal nader worden toegelicht in het kader van de normstelling. Voor het *object* van de toets is het van belang dat artikel 26 ziet op het *verzamelen* van gegevens. De eisen worden niet gekoppeld aan de *verwerking* van gegevens. Dit is opvallend omdat de TIB tegelijkertijd wel toetst op een aantal verwerkingsbevoegdheden. Met het voorstel tot wijziging van de Wiv 2017 (dat momenteel in behandeling is bij de Eerste Kamer) wordt aan artikel 26 bovendien het gerichtheidsvereiste toegevoegd. Volgens de toelichting op dit voorstel is het vereiste daarmee van toepassing op bevoegdheden tot gegevens*verzameling*.[271] Hieruit volgt dat de wetgever de TIB-toets heeft ingesteld voor bevoegdheden tot *verwerving (verzamelen)*. De hiervoor genoemde bevoegdheden van *search* gericht op selectie, selectie en GDA (artikel 50, lid 1, onder b) vallen buiten dit systeem omdat het gaat om verwerkingsbevoegdheden.

Dit betekent dat de wetgever de TIB op een kernelement van de wet in een hybride positie heeft geplaatst doordat de TIB vooraf statische beslissingen moet geven op de meest dynamische verwerkingsfase: het analyseren, duiden en met elkaar in verband brengen van gegevens om zo een steeds completer beeld te krijgen van een dreiging. Dit is een complex vraagstuk dat zowel de inhoud van de norm, de rechtstoepassing als de aanpassing van de inrichting van het toezicht raakt. De Evaluatiecommissie vindt de statische aard van de ex-ante toets niet passend bij deze dynamische verwerkingsfase.

Object: verloop van het project

Daarnaast constateert de Evaluatiecommissie dat de TIB bij haar rechtmatigheidstoets op de inzet van verwervende bevoegdheden soms ook de wijze betrekt waarop de diensten deze gegevens ná verwerving willen verwerken. De TIB geeft aan dat "(E)lke redelijkerwijs voorzienbare vorm van gegevensverwerking van betekenis [kan] zijn voor de rechtmatigheidstoets door de TIB"[272]. Hierbij gaat het specifiek om het delen van gegevens aan buitenlandse partners. Als dit voorzienbaar is, dan vindt de TIB dit van belang voor haar toets. In het meest recente jaarverslag schrijft de TIB dat zij de voorgenomen wijze van gegevensverwerking meer in het algemeen betrekt in de rechtmatigheidstoets.[273] Soms neemt de TIB voorschriften over de verwerking op als clausulering (zie §9.3.2). Soms wijst de TIB een toestemmingsverzoek af vanwege aspecten van verwerking die zij als onrechtmatig beoordeelt.[274] De betrokken ministers vinden dat de verwerking van gegevens die zijn verkregen door de inzet van bijzondere bevoegdheden buiten de rechtmatigheidstoets door de TIB vallen. Zij zien een rol voor de TIB in het autorisatieproces en niet in hetgeen daarop volgt.[275] Dit is eveneens van belang bij de toets

[269] Search gericht op interceptie (artikel 49, lid 1) is een essentieel onderdeel van de verwerving door middel van OOG-interceptie en wordt daarom door de Evaluatiecommissie als een op de verwerving gerichte bevoegdheid gezien (zie verder hoofdstuk 6 over OOG-interceptie).
[270] *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 40, 51, 53 (MvT Wiv 2017).
[271] *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4 (MvT wijziging Wiv 2017).
[272] *Kamerstukken II* 2018/19, 29 924, nr. 173, p. 2 (brief rechtseenheidsoverleg iz. reikwijdte en GDA).
[273] TIB. (2020). *Jaarverslag 2019-2020.* p. 13.
[274] Ibidem. p. 10.
[275] Bijlage bij *Kamerstukken II*, 2018/19, 29 924, nr. 179, p. 3.

door de TIB op toestemmingen voor verlenging van een bepaalde inzet. Hierbij betrekt de TIB bijvoorbeeld ook de opbrengst van de inzet omdat dit van invloed is op de proportionaliteit.[276]

Het betrekken van de (voorziene) wijze van verwerking in de toets door de TIB stuit volgens de Evaluatiecommissie op dezelfde bezwaren als die voor de TIB-toets op de inzet van verwerkingsbevoegdheden zelf. Dat zijn bij uitstek handelingen van de diensten waar de CTIVD toezicht op houdt. Door dit ook bij de TIB-toets te betrekken, wordt de rolverdeling tussen TIB en CTIVD diffuus, hetgeen de Evaluatiecommissie niet wenselijk vindt. Het past bovendien niet bij de statische ex-ante-toets om dergelijke dynamische (toekomstige) processen vooraf te omschrijven en af te bakenen. Ook bij verlengingsverzoeken, waarbij de diensten aangeven wat de opbrengst is geweest ter onderbouwing van de verlenging, zou de toets niet moeten zien op de wijze waarop deze opbrengst is verwerkt. De mate van opbrengst kan op zichzelf wel worden betrokken in de weging. De enige uitzondering hierbij betreft de inzet van bijzondere bevoegdheden (mede) ten behoeve van een buitenlandse dienst, gezien het feit dat het delen van gegevens (verwerking) hierbij het *doel* is van de inzet.

Al de hier geschetste problemen moeten naar het oordeel van de Evaluatiecommissie niet leiden tot vermindering van toezicht op deze dynamische processen, maar tot een betere aansluiting tussen het ex-ante en ex-post toezicht. Dit wordt in §9.4 behandeld.

Normstelling

Naast het diffuse object van toetsing heeft de wet geen scherp toetsingskader gesteld voor de ex-ante toets door de TIB. De TIB toetst aan de vereisten van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid. Deze open normen vormen de toespitsing van één van de kernbeginselen van behoorlijk bestuur, te weten de materiële zorgvuldigheid (artikel 3:4 Algemene wet bestuursrecht (Awb)). Kort gezegd mag een bevoegdheid alleen worden ingezet als zij in de omstandigheden van het geval (waaronder de ernst van de dreiging) mede in aanmerking nemend de andere beschikbare bevoegdheden voor 'de betrokkene' het minste nadeel oplevert (subsidiariteit). Daarbij blijft de uitoefening achterwege als deze onevenredig nadeel voor 'de betrokkene' oplevert en moet de inzet evenredig zijn aan het beoogde doel (proportionaliteit). De uitoefening moet tenslotte zo gericht mogelijk zijn, waarbij verwerving van gegevens die niet noodzakelijk zijn voor het onderzoek tot een minimum worden beperkt.[277] Doet zich bij de uitoefening een minder belastend alternatief voor, dan wordt de meer belastende uitoefening 'onmiddellijk gestaakt'.[278] De noodzakelijkheid volgt indirect uit artikel 26 maar wordt expliciet als vereiste van een toestemmingsaanvraag genoemd in artikel 29, lid 2, onder f.

Op het eerste gezicht kan iedereen zich goed voorstellen wat met deze open normen wordt bedoeld. Het hanteren van open normen is ook begrijpelijk, omdat de invulling hierdoor kan meegroeien met (technologische) ontwikkelingen. Deze open normen zijn gaandeweg door de CTIVD en TIB nader ingevuld. Zij zijn gevat in openbare brieven aan de Tweede Kamer[279] maar ook in vertrouwelijke stukken van de TIB aan de betrokken ministers. Soms gaat de interpretatie van open normen door de toezichthouders ook gepaard met het stellen van bovenwettelijke eisen. In de praktijk blijkt dat de interpretatie van open normen door de TIB en CTIVD niet altijd

[276] TIB. (2020). *Jaarverslag 2018-2019*. p. 17.
[277] *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 4-5 (MvT wijziging Wiv 2017).
[278] Artikel 26 van de Wiv 2017 en artikel 2 Beleidsregels Wiv 2017 (*Stcrt.* 2018, 24397).
[279] *Kamerstukken II 2018/19*, 29 924, nr. 173, p. 2 (brief rechtseenheidsoverleg iz. reikwijdte en GDA); TIB. (2019). *Jaarverslag 2018-2019*; TIB. (2020).

wordt gedeeld door de ministers en diensten. Hierover heeft in het publieke domein maar zeer beperkte discussie plaatsgevonden. De Evaluatiecommissie vindt dit een gemis.

De evaluatie leert dat betwijfeld moet worden of onder alle omstandigheden dezelfde aspecten moeten worden meegewogen bij de invulling die wordt gegeven aan de open normen van artikel 26. Een vaste interpretatie van die normen met vaste elementen lijkt zich niet goed te verhouden met de dynamiek van het werk van de diensten en de technologische ontwikkelingen. Kort gezegd houdt dit in dat de normen te veel zijn toegesneden op in 'individuele' gevallen te maken afwegingen. Dit is de kern van het klassieke privacyrecht. Als het gaat om persoonsgegevens die onderdeel vormen van zeer grote databestanden gaan algemene proportionaliteitsmaatstaven een rol spelen. De handhaving van de rechten van het individu komt in handen te liggen van een publieke toezichthouder en/of een collectief belangorganisatie. De TIB heeft aangegeven bij haar toetsing sterk te kijken naar de wet en de bijbehorende toelichting. Deze geeft in de praktijk niet altijd voldoende aanknopingspunten.

In die toelichting op de wet staat een aantal voorbeelden dat niet altijd rechtdoet aan de complexiteit en diversiteit van de praktijk. Hierbij wordt volgens de Evaluatiecommissie te veel uitgegaan van 'individuele' *targets* en bekende dreiging. In de praktijk is ook onderzoek naar nog verborgen dreiging, waarbij bijvoorbeeld nog niet bekend is wie de *targets* zijn, een belangrijke taak van de diensten. Bij de inzet die is gericht op deze verborgen dreiging zijn de omstandigheden doorgaans anders dan bij gekende dreigingen. Zo zijn er bijvoorbeeld geen specifieke individuele *targets* of vindt de inzet in het buitenland plaats waar de diensten zijn aangewezen op minder gerichte bevoegdheden dan in Nederland (zie §8.5.1). Dit vergt 'collectieve' afwegingen (in vaak complexe internationale situaties) waarbij aan de inhoud van begrippen als 'zo gericht mogelijk' en 'onevenredige benadeling' en de 'evenredigheid in relatie tot het doel' een andere inhoud moet worden gegeven dan bij in het algemeen overzichtelijke individuele gevallen.

Het belang van afwegingen die gericht zijn op de waarborgen van de verzameling, inrichting, toegankelijkheid en tijdsduur van het bestand, komt duidelijk naar voren bij de invulling van het gerichtheidscriterium bij bulkverwerving. Bulkdata heeft niet alleen meerwaarde voor gekende dreiging en gekende *targets*, maar juist ook voor verborgen dreiging. De invulling van het gerichtheidscriterium gaat uit van gekende *targets* waarop de inzet kan worden gericht. Voor bulkverwerving is deze invulling niet passend vanwege een minder eenduidige doelbinding. Zo kan het bijvoorbeeld noodzakelijk zijn om bulkdata te verwerven waarbij pas bij de verwerking duidelijk wordt wat de specifieke gebruiksdoelen zijn (zie §4.2.4). Het is evenwel belangrijk om zo gericht mogelijk te verwerven. Daarom heeft de Evaluatiecommissie al belangrijke aanbevelingen gedaan voor een passende invulling van het gerichtheidsvereiste bij bulkverwerving. Voor de eis van noodzakelijkheid verwacht de Evaluatiecommissie dat de aanbevolen introductie van de bulkbehoefte de TIB in staat stelt de noodzakelijkheid van bulkverwerving beter te kunnen betrekken bij het toetsen van de inzet van een bijzondere bevoegdheid (zie §4.3.4).

Ook ten aanzien van de overige normen voor toetsing beveelt de Evaluatiecommissie aan om bij een wetswijziging in de toelichting op de wet meer aandacht te besteden aan deze verschillende omstandigheden. De bestaande toelichting biedt voor de TIB nog te weinig aanknopingspunten om te differentiëren in de toetsing. Het gaat hierbij niet alleen om bulkverwerving maar bijvoorbeeld ook om voorbeelden van technologische complexe omstandigheden en de complexiteit van het doen van onderzoek naar verborgen dreiging en inzet in het buitenland. Zo moet in de toelichting worden opgenomen dat de mate van detail van de toets door de TIB ook moet passen bij de statische aard van de ex-ante toets. Bij een nieuwe, complexe hackoperatie

volstaat bijvoorbeeld een mindere mate van detail in de omschrijving van technische risico's (zie §7.3.3). Daarnaast kunnen ook voorbeelden van de inzet van bijzondere bevoegdheden voor het verkrijgen van *assets* (bij strategische operaties) meer handvatten bieden aan de TIB voor differentiatie (zie §7.4).

Hierbij kan ook worden overwogen om de verschillende wettelijke taken van de diensten (artikelen 8 en 10) een rol te laten spelen in de weging. Zo zal de weging van de inzet in het kader van de veiligheidstaak (de a-taak in artikel 8 van de wet) van de AIVD – waarbij personen en organisaties worden onderzocht die aanleiding geven tot een ernstig vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor veiligheid of andere gewichtige belangen van de staat – anders zijn dan die in het kader van de d-taak (AIVD) en e-taak (MIVD) in de artikelen 8 en 10 van de wet. Hierbij verrichten de diensten 'onderzoek betreffende andere landen', door inlichtingen over het buitenland in te winnen. Bepaalde landen en regio's, die zijn vastgelegd in de Geïntegreerde Aanwijzing, worden op verzoek van de regering onderzocht. Het gaat hierbij onder andere om inlichtingen over politieke intenties van andere landen die de Nederlandse regering kunnen gebruiken bij het bepalen van standpunten over buitenlands beleid.[280] Waar bij de a-taak (AIVD) sneller sprake zal zijn van een (ernstig vermoeden van) *concrete* dreiging voor de nationale veiligheid, hoeft dit niet zo te zijn voor de d-taak (AIVD) en de e-taak (MIVD). Deze inlichtingentaken zijn in het belang van de nationale veiligheid, maar er is niet altijd sprake van *concrete* dreiging. Bij de inlichtingentaak spelen urgentie en dreiging een andere rol bij de weging van de inzet van een bevoegdheid. Het onderscheid is niet altijd zwart-wit, maar deze benadering biedt wel aanknopingspunten voor een andere invulling van de normen bij de veiligheidstaak, dan bij de inlichtingentaak waar niet altijd sprake is van een (ernstig vermoeden van) direct gevaar. Het is dan vervolgens aan de diensten om in de toestemmingsaanvraag helder te onderbouwen in het kader van welke taak een inzet moet worden getoetst.

Aanbeveling 44

Verduidelijk de wet en toelichting zodat duidelijk is dat de TIB alleen bij de inzet van verwervende bevoegdheden een rol heeft, niet bij bevoegdheden voor verwerking. Specificeer hierbij ook dat bij deze TIB-toets op de inzet van verwervende bevoegdheden de verwerking van de te verwerven gegevens geen rol speelt.

Aanbeveling 45

Neem in de toelichting op de wet voorbeelden op van verschillende omstandigheden aan de hand waarvan de TIB de invulling van de normen bij de toets kan differentiëren. Hierbij kan de aard van de verschillende wettelijke taken van de diensten een rol spelen.

[280] Geintegreerde aanwijzing Inlichtingen en Veiligheid 2019-2022 van 23 november 2018, *Stcrt.* 68088, p. 2.

9.4 Samenhang binnen het stelsel van toezicht

9.4.1 Inleiding

Zoals besproken onder §9.3 beveelt de Evaluatiecommissie aan om de TIB-toets te beperken tot verwervende bevoegdheden en niet te laten zien op de daaropvolgende verwerking van de verworven gegevens. Vanwege de dynamische aard van de verwerkingsfase, leent deze fase zich beter voor het toezicht dat de CTIVD op de diensten houdt. Hierbij is het van belang dat er geen verkokering plaatsvindt binnen het gehele stelsel van toezicht. Juist de aansluiting tussen de toetsende rol van de TIB en de toezichthoudende rol van de CTIVD vormt een belangrijke waarborg, zo meent de Evaluatiecommissie. Deze aansluiting moet worden versterkt. Dit past in de door de CTIVD tijdens het onderzoek uitgesproken doelstelling te komen tot goed geïntegreerd toezicht.

In dat kader moet de inhoud van het ex-ante toezicht scherp worden gedefinieerd. Zoals hiervoor gesteld: de TIB toetst een toestemming van de minister. Ervanuit gaande dat de TIB niet (voorwaardelijk) toezicht kan houden op het vervolgtraject moet zij wel inzicht hebben in de concretisering van de waarborgen die in de toestemming zijn verwerkt. De wettelijke kapstok is artikel 24 van de Wiv dat bepaalt dat de hoofden van dienst zorgdragen voor de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming met de wet.

9.4.2 Samenwerking binnen het stelsel

Waar de TIB voorafgaand de toestemming voor inzet van bijzondere bevoegdheden toetst, houdt de CTIVD dus toezicht op het daaruit voortkomende handelen van de diensten over de gehele linie. Zoals gezegd kan dit achteraf (nadat een operatie is afgelopen) maar ook tijdens. In de verschillende fases van een operatie kan de focus van het toezicht ook verschuiven. Dit wordt ook wel ‘dynamisch toezicht’ genoemd.

De TIB-toets is een statische ex-ante toets. De TIB neemt in deze toets ook de voorwaarden mee die de minister aan de toestemming heeft verbonden (inclusief de onderbouwing van de noodzakelijkheid van bulkverwerving). Bij deze toets kan het zicht op de inzet van de bevoegdheid beperkt zijn, bijvoorbeeld bij een meer complexe en dynamische hackoperatie. Juist zo’n operatie leent zich voor dynamisch en geïntegreerd toezicht door de CTIVD. Volgens artikel 97, lid 3, onder a, ziet de CTIVD toe op de rechtmatigheid van de uitvoering van de wet. Dat ziet dus ook op de rechtmatigheid van de uitvoering van de bijzondere bevoegdheid, waarvan de toestemming ex-ante door de TIB is getoetst. De CTIVD kan de ministers gevraagd en ongevraagd inlichten en adviseren over haar bevindingen over de rechtmatigheid van de uitvoering van een (bijzondere) bevoegdheid. Als de CTIVD meent dat sprake is van een (dreigende) onrechtmatigheid, dan kan zij de minister daarover informeren (artikel 97, lid 3, onder b). De minister moet dan actie ondernemen.

Langs deze weg kan dynamisch toezicht worden gecreëerd dat de autonomie van de TIB en de CTIVD respecteert. Dit dynamisch toezicht kan bovendien worden versterkt door periodiek overleg tussen de TIB en de CTIVD over specifieke casuïstiek in de vorm van een ‘beleidseenheidsoverleg’. Hiervoor ziet de Evaluatiecommissie onder de huidige wet geen belemmeringen.

Aanbeveling 46

Intensiveer de samenwerking tussen de TIB en de CTIVD, waarbij casuïstiek wordt besproken in een beleidseenheidsoverleg. De huidige wet vormt hiervoor geen belemmering.

9.4.3 Rechtseenheidsoverleg

In het verlengde van de vorige aanbeveling rijst de vraag hoe het verder moet met het rechtseenheidsoverleg tussen de TIB en de CTIVD. De Evaluatiecommissie is gevraagd zich hierover te buigen, en over de vraag of dit overleg inderdaad leidt tot voldoende rechtseenheid.[281]

De TIB en de CTIVD (zowel de afdeling toezicht als de afdeling klachtbehandeling) voeren rechtseenheidsoverleg met als doel om tot nadere invulling van een norm te komen. Dat overleg leidt tot openbare brieven die naar de betrokken ministers en de Tweede Kamer worden verstuurd. Daarnaast bestaat er informeel contact tussen de TIB en de rechtbank Den Haag, die oordeelt over mogelijke inzet van bijzondere bevoegdheden jegens advocaten en journalisten, om tot een gelijke vorm van toetsing te komen. Dat de TIB en de CTIVD elkaar hebben opgezocht in de wens bepaalde begrippen eenduidig uit te leggen is begrijpelijk en het heeft de voorspelbaarheid en consistentie van het toezicht vergroot. Het is goed dat er eenheid van opvattingen bestaat tussen de toezichthouders. De vraag is wel wat de juridische betekenis van de (uitkomsten van) het rechtseenheidsoverleg is, ook vanwege de verschillen in bevoegdheden tussen beide toezichthouders.

Het rechtseenheidsoverleg heeft geleid tot eenheid in standpunten van de TIB en CTIVD, zowel op de meer technische open normen zoals GDA als ook op de open normen voor toetsing. Zoals benoemd in §9.3 zijn deze standpunten deels in openbare brieven gevat. De Evaluatiecommissie ziet geen duidelijke juridische basis voor en in ieder geval geen bindende status van deze standpunten. In de praktijk hebben de bevindingen van het rechtseenheidsoverleg wel gezag omdat zij, als waren zij wetsinterpreterende beleidsregels[282], aangeven hoe de TIB en de CTIVD hun toezichtsbevoegdheden uitoefenen. Vanwege de bindende toets door de TIB worden deze interpretaties door de ministers en de diensten soms als een ‘dictaat’ ervaren. Tegelijkertijd hebben de ministers en diensten hier niet proactief een andere interpretatie tegenover gezet. In §9.6 wordt hierop teruggekomen.

De Evaluatiecommissie constateert dat het onwenselijk is dat de afdeling klachtbehandeling van de CTIVD onderdeel uitmaakt van het rechtseenheidsoverleg. De afdeling klachtbehandeling moet onafhankelijk van de afdeling toezicht kunnen oordelen. Daarom past het niet om gezamenlijk overleg te voeren. Voor zover de rechtbank Den Haag deel zou uitmaken van het rechtseenheidsoverleg, vindt de Evaluatiecommissie dat om dezelfde reden onwenselijk.

Geen aanbevelingen ten aanzien van het rechtseenheidsoverleg, met dien verstande dat daaraan alleen de TIB en de afdeling toezicht van de CTIVD deelnemen.

[281] *Kamerstukken II* 2019/20, 34 588, nr. 84 (Kamerbrief opdracht evaluatie).

[282] Vgl. artikel 1:3, vierde lid, Awb, dat beleidsregel definieert als een bij besluit vastgestelde algemene regel, niet zijnde een algemeen verbindend voorschrift, omtrent de afweging van belangen, de vaststelling van feiten *of de uitleg van wettelijke voorschriften* bij het gebruik van een bevoegdheid van een bestuursorgaan (curs. Evaluatiecommissie).

9.5 Balans in het stelsel

9.5.1 Inleiding

De aanbevelingen uit dit hoofdstuk hebben betrekking op de inrichting van het toezicht, de invulling van de ex-ante toets door de TIB en de verhouding en samenhang tussen de statische ex-ante toets en dynamisch toezicht. Deze hangen bovendien samen met de aanbevelingen over de invulling van wettelijke begrippen uit hoofdstuk 4 en 5. De Evaluatiecommissie verwacht dat het stelsel van toezicht hierdoor beter zal kunnen functioneren. De Evaluatiecommissie meent echter dat het stelsel nog op één punt een weeffout bevat.

De TIB en de CTIVD zijn in het leven geroepen om toezicht te houden op de rechtmatigheid van de uitoefening van bevoegdheden door de diensten. Zij doen dat door de wettelijke normen van proportionaliteit, subsidiariteit en 'zo gericht mogelijk' toe te passen op concrete casus. In dat kader moeten zij niet alleen zelf bepalen wat zij in die casus proportioneel, subsidiair en 'zo gericht mogelijk' vinden, maar ook wat deze criteria inhouden, en hoe indringend zij daaraan moeten/mogen toetsen. Daarnaast moeten zij de wettelijke begrippen (bulkdatasets, GDA, verwerking, etc.) toepassen en nader uitleggen. Nu zal iedere toezichthouder in eerste instantie invulling moeten geven aan wettelijke normen en begrippen, maar in het stelsel zoals de wetgever dat heeft gecreëerd, hebben de toezichthouders niet alleen het laatste woord in een concrete casus, maar (behoudens ingrijpen door de wetgever) ook wat betreft de uitleg van de wettelijke begrippen en criteria, en de wijze waarop zij hieraan toetsen.

Het is de Evaluatiecommissie gebleken dat de ministers en de diensten zich niet hebben gerealiseerd dat dit het gevolg kon zijn van het stelsel dat de wetgever met de Wiv 2017 heeft gecreëerd. Dat er discussie zou kunnen ontstaan over de wijze van toepassing van de wettelijke begrippen en criteria is wel verondersteld, maar niet dat de algemene invulling daarvan ook in laatste instantie aan de toezichthouder werd gelaten, en wat daarvan de gevolgen zouden zijn.

9.5.2 Knelpunten in de praktijk

Dit systeem heeft de afgelopen jaren verschillende malen tot knelpunten geleid. De toezichthouders hebben een rechtseenheidsoverleg opgezet, waarvan de juridische status onduidelijk is (zie §9.4.3). De ministers van hun kant hebben een regeling op basis van artikel 16 van de wet vastgesteld die een invulling geeft aan de wijze waarop de diensten met bulkdata om moeten gaan (zie hoofdstuk 4). Hiermee geven de ministers een interpretatie van de wettelijke beoordelingscriteria, terwijl die interpretatie volgens het *huidige* systeem aan de toezichthouders is. In de praktijk heeft dit bijvoorbeeld geleid tot een patstelling over de relevantiebeoordeling van bulkdatasets en het al dan niet vernietigen van deze sets (zie §4.4.4).

Tijdelijke bulkregeling op basis van artikel 16

Tijdens deze evaluatie heeft er een discussie gespeeld tussen de CTIVD en de ministers en diensten over de omgang met bulkdatasets (zie §4.4.4). In dat verband hebben de ministers een Tijdelijke regeling op basis van artikel 16 van de Wiv 2017 uitgevaardigd. Uit deze regeling komt de suggestie[283] naar voren dat het hier gaat om algemeen verbindende voorschriften, dat wil zeggen voorschriften die niet alleen de diensten maar ook de toezichthouder binden.

Naar de mening van de Evaluatiecommissie geeft artikel 16 van de Wiv 2017 geen basis voor extern (dus ook de toezichthouders) bindende algemeen verbindende voorschriften, maar is het artikel een – in het licht van artikel 44 Grondwet juridisch overbodige – grondslag voor het stellen van interne regels voor de interne 'organisatie en werkwijze' van de diensten. Daarmee is artikel 16 geen grondslag voor het stellen van algemeen verbindende voorschriften die de uitoefening van bijzondere bevoegdheden zelf raken.

Zoals gezegd meent de Evaluatiecommissie met een aantal aanbevelingen inhoudelijke verbeteringen in de wet en toepassing van de wet te hebben voorgesteld, maar met het laatste woord voor de TIB en de CTIVD over de uitleg van de wet blijft het stelsel een weeffout bevatten. Het is niet ondenkbaar dat deze weeffout de komende jaren opnieuw tot problemen zal leiden, mede gelet op de snelle technologische ontwikkelingen. Immers, ook de verduidelijkingen van begrippen en verhelderingen van procedures zullen weer nieuwe vragen van afbakening kunnen oproepen. Dat geldt ook voor het object en normstelling van de TIB-toetsing; daar stelt de Evaluatiecommissie onder meer voor om verhelderende voorbeelden in de toelichting bij een eventuele wetswijziging op te nemen (zie §9.3.3). Het is belangrijk dat het stelsel hiermee tot op zekere hoogte een eigen probleemoplossend vermogen heeft, waarbij alle betrokkenen vanuit hun eigen rol en verantwoordelijkheid met elkaar in gesprek gaan. Dat betekent echter niet dat deze vragen zich niet op gezette tijden weer kunnen voordoen.

De Evaluatiecommissie vindt het niet alleen praktisch onwenselijk, maar ook principieel niet passend dat een toezichthouder het laatste woord heeft over de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen en de intensiteit van de toetsing. Dat is bij uitstek een rechterlijke taak, waarbij de toezichthouder, gegeven de rechterlijke overwegingen, gaat over de toepassing in concrete gevallen. De Evaluatiecommissie beveelt dan ook aan dat het stelsel van toezicht wordt aangevuld met een rol voor de rechter, die de grenzen van het speelveld bepaalt waarbinnen het toezicht op de bevoegdheidsuitoefening door de diensten plaatsvindt.

[283] De aanhef van de regeling verwijst uitsluitend naar artikel 16 Wiv 2017, en de artikelen van de regeling en de toelichting zijn zodanig geformuleerd dat de diensten geen ruimte lijken te hebben om van de voorschriften af te wijken. De Evaluatiecommissie meent dat het zuiverder zou zijn dergelijke regelingen als beleidsregels aan te merken, en artikel 16 Wiv 2017 te beperken tot het stellen van regels van interne beheersmatige en procedure aard. Opmerking verdient ook dat de – naar hun aard met dit besluit vergelijkbare - regels die de ministers naar aanleiding van het referendum van maart 2018 hebben vastgesteld (Besluit van 25 april 2018, *Stcrt.* 2018, 24397) niet op artikel 16 Wiv 2017 waren gebaseerd, maar het karakter van beleidsregels hadden.

Aanbeveling 47

Vul het stelsel van toezicht aan met een rol voor de rechter. Deze rechter bepaalt de grenzen van het speelveld van toezicht door de uitleg van wettelijke begrippen, de invulling van toetsingsnormen en de intensiteit van de toetsing.

9.5.3 Voor- en nadelen van aanvullende rol rechter

De aanvulling van het stelsel met een rol voor de rechter zorgt voor balans in het stelsel. Daarnaast zijn er andere belangrijke voordelen aan verbonden.

Allereerst is er in het huidige stelsel niet of nauwelijks ruimte voor inbreng van algemeen-belangenbehartigende organisaties. Deze organisaties hebben in het debat over de totstandkoming van de Wiv een belangrijke rol gespeeld en doen dat nog steeds in het huidige publieke debat. Gelet op het maatschappelijk belang is het gebrek aan ruimte voor inbreng van deze organisaties een gemis. Juist als het gaat om de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen of de intensiteit van de toetsing is het waardevol, zowel voor de kwaliteit als de maatschappelijke legitimatie van de uitkomst, dat algemeen-belangbehartigers zich hierover kunnen uitspreken. In de huidige situatie is dat ondenkbaar, omdat het in de toetsing door de toezichthouders steeds gaat om concrete, staatsgeheime vraagstukken. Bij een rechterlijke procedure kan dat anders liggen.

Daarnaast heeft het internationale en supranationale (EU-)recht een steeds belangrijker invloed op het werk van de diensten (zie §3.4). In het huidige stelsel ontbreekt de mogelijkheid om aan het EHRM of het HvJEU prejudiciële vragen te stellen over de verenigbaarheid van de Nederlandse wet met het EVRM en het Unierecht. Een rechter kan dat wel. In veel Europese stelsels heeft de rechter die mogelijkheid. In Nederland heeft de rechter die op papier misschien nog wel (vanwege de restfunctie van de burgerlijke rechter), maar in de praktijk niet.

Ten slotte zal een rol voor de rechter zoals hierboven beschreven mogelijk ook de behoefte aan het voeren van het rechtseenheidsoverleg tussen de TIB en CTIVD verkleinen. Zoals toegelicht in §9.4.3 past dit overleg niet goed in het wettelijk stelsel, en doet het verder afbreuk aan een goede verhouding tussen toezichthouders en diensten.

Ook elders in het bestuursrecht doen zich geschillen tussen toezichthouders en ondertoezichtgestelden voor. Dit wordt opgelost door de bestuursrechter de bevoegdheid te geven deze geschillen te beslechten. De bestuursrechter is bij uitstek geschikt om de rechtmatigheid van overheidshandelen te beoordelen: aan de hand van de beginselen van behoorlijk bestuur en met inachtneming van de bijzondere positie van de democratisch gelegitimeerde overheid.

Tegen deze oplossing zou kunnen worden ingebracht dat zij het probleem alleen maar verplaatst, maar de Evaluatiecommissie meent dat dit niet het geval is. Een rol voor de rechter zou het stelsel juist meer in balans brengen, omdat het eerder geschetste dilemma wordt doorbroken door het probleem daar neer te leggen waar het rechtsstatelijk gezien het beste thuishoort, namelijk de rechter.

9.5.4 De procedure op hoofdlijnen

Gelet op de in het geding zijnde belangen en omstandigheden (snel duidelijkheid, zo min mogelijk bekendheid van staatsgeheime informatie) beveelt de Evaluatiecommissie aan om de Afdeling bestuursrechtspraak van de Raad van State in eerste en enige instantie met bovengenoemde taken te belasten. Het gaat hierbij om een gesloten categorie van beroepsgerechtigden. In sommige gevallen zal moeten worden voorzien in een verkorte en vereenvoudigde procedure. Hieronder wordt – op hoofdlijnen – verder uitgewerkt op welke punten het beroep mogelijk zou moeten zijn, en hoe de rechtsgang eruit zou kunnen zien.

De Evaluatiecommissie ziet in de volgende situaties een rol voor de Afdeling bestuursrechtspraak weggelegd:

a) Minister/diensten zijn het niet eens met de wijze waarop de TIB in een concreet geval gebruik heeft gemaakt van haar toezichtsbevoegdheden;
b) Minister/diensten, CTIVD/toezicht, CTIVD/klachtbehandeling en/of TIB willen, al of niet naar aanleiding van een concrete zaak, een richtinggevende uitspraak over de uitleg van wettelijke begrippen en normen of de intensiteit van de toetsing;
c) Er is behoefte aan een prejudiciële beslissing van het EHRM of het HvJEU;
d) Minister/klager is het niet eens met een uitspraak van de afdeling klachtbehandeling van de CTIVD.

Ad a. Beroep tegen oordeel TIB

Eén van de situaties die zich kan voordoen en zich nu ook al voordoet, is dat er verschil van mening bestaat tussen toezichthouder – de TIB – en de diensten over de wijze waarop de toezichthouder een concrete casus beoordeelt. Dat kan gaan om de uitleg van een wettelijk begrip maar ook om de invulling van de toets door de TIB. Weliswaar is de evenredigheidstoets (culminerend in subsidiariteit, proportionaliteit en 'zo gericht mogelijk') die de TIB moet toepassen een volle toets, maar dat doet er niet aan af dat het primaat van afweging bij de diensten en de minister ligt. Zou de TIB in een bepaald geval in de ogen van de minister/diensten een (in het licht van het wettelijk systeem) té intensieve toets plegen, dan is er geen instantie die beslissend kan beoordelen of de toetsing door de TIB de juiste is. De hierdoor ontstane patstelling is in niemands belang.

In het hier geschetste stelsel kan de minister het oordeel van de TIB aan de Afdeling bestuursrechtspraak voorleggen. Deze zal kennis moeten nemen van de inhoud van de voorliggende last en de motivering daarvan. De Afdeling is al bekend met de beoordeling van zaken waarin staatsgeheime, vaak ook operationele, informatie van diensten aan de orde komt, zoals verzoeken om kennisgeving als bedoeld in §5.2 van d e Wiv en ambtsberichten van de AIVD die door andere bestuursorganen (ministers, burgemeesters) aan hun besluitvorming ten grondslag worden gelegd. Daarop zijn de bepalingen van hoofdstuk 8 van de Wiv 2017 met betrekking tot geheimhouding van toepassing. Ook in geschillen ingevolge de Wet veiligheidsonderzoeken treedt de Afdeling als hoogste bestuursrechter op.

Het feit dat de Afdeling kennis moet nemen van de concrete last waar het geschil over gaat, betekent niet dat de Afdeling het oordeel van de TIB volledig heroverweegt: het gaat hier immers om een rechter, niet een hogere toezichthouder. Wanneer het geschil ziet op de invulling van de toetsing door de TIB (toetsingsnormen en intensiteit), dan behelst de toetsing door de Afdeling of de TIB in redelijkheid tot het desbetreffende oordeel heeft kunnen komen. De wet zou dit

uitdrukkelijk kunnen bepalen. Wanneer het geschil ziet op een invulling van een wettelijk begrip, dan zal de Afdeling de gehanteerde wetsuitleg van de TIB wél vol moeten toetsen.

Vanwege de vereiste spoed bij een geschil over een concreet onrechtmatigheidsoordeel van de TIB, moet worden afgeweken van een aantal in het normale geval geldende procesregels. De bezwaarschriftprocedure moet worden uitgesloten, er moet een korte en vereenvoudigde procedure worden toegepast, de behandeling zal achter gesloten deuren moeten plaatsvinden en de Afdeling moet als in eerste en enige aanleg oordelende rechter worden aangewezen en zij moet aan een korte termijn worden gebonden.

Ad b. Verzoek om richtinggevende uitspraak
Een richtinggevende uitspraak over de interpretatie van centrale wettelijke begrippen en de invulling van de open toetsingsnormen (proportionaliteit, subsidiariteit, noodzakelijkheid, gerichtheid maar ook het object en de intensiteit van toetsing) kan worden gedaan op verzoek van de minister, de TIB of de CTIVD (daaronder ook begrepen de afdeling klachtafhandeling). Te denken valt aan een verzoekschriftprocedure of een vorm van prejudiciële beslissing. Bij het eerste hoeft niet voor een spoedprocedure te worden gekozen (al zal dat soms wel nodig zijn); bij een prejudicieel oordeel (als een concreet geval bij de TIB voorligt en de TIB of de minister willen een prejudicieel oordeel van de Afdeling) zal wel weer een spoedprocedure moeten worden gehanteerd.

Ad c. Prejudiciële vragen aan het EU Hof van Justitie en aan het EHRM
Het is duidelijk dat het terrein van de Wiv steeds meer vervlochten raakt met het Europees recht en dat de rol van de beide Europese hoven buitengewoon belangrijk is, en bij bepaalde elementen zelfs doorslaggevend wordt. In dat licht is het wenselijk dat aan de hoven prejudiciële vragen kunnen worden gesteld over de verenigbaarheid van het stelsel van de Wiv met het Europese recht. In de huidige situatie is dat onmogelijk, omdat dit alleen kan door een rechter, waarvoor de TIB en de CTIVD niet kwalificeren. Wordt gekozen voor introductie van een rol voor de Afdeling bestuursrechtspraak van de Raad van State zoals hiervóór geschetst, dan kan de Afdeling in alle gevallen prejudiciële vragen stellen, zowel over de uitleg van het Europese Unierecht aan het HvJEU als over de interpretatie van het EVRM aan het EHRM.

Ad d. Hoger beroep tegen een oordeel van de afdeling klachtbehandeling van de CTIVD
Op dit moment staat geen bestuursrechtelijk beroep open tegen een bindend oordeel van de afdeling klachtbehandeling van de CTIVD: de klager kan zich tot de burgerlijke rechter wenden, terwijl voor de minister geen voorziening open staat. Wordt gekozen voor een beroepsmogelijkheid bij de Afdeling bestuursrechtspraak van de Raad van State zoals hiervóór onder a geschetst, dan acht de Evaluatiecommissie het uit rechtstatelijk oogpunt wenselijk dat tegen een bindend oordeel van de afdeling klachtbehandeling zowel voor klager als minister beroep open staat op de bestuursrechter.

Expertise
De Evaluatiecommissie is zich ervan bewust dat het per jaar om weinig zaken zal gaan; sterker, wellicht dat het enkele bestaan van de procedure ertoe leidt dat partijen meer dan nu het geval is proberen er met elkaar uit komen. Dat betekent dat waar de Afdeling, naast de eerdergenoemde zaken waar zij nu al bevoegd is, geen expertise op dit terrein heeft, zij die ook niet snel zal kunnen opbouwen. De Evaluatiecommissie ziet dit probleem, maar meent alles afwegende dat toch voor deze procedure moet worden gekozen. Het gaat om bij uitstek bestuursrechtelijke vragen, waarbij een goede balans moet worden gezocht voor het algemeen, door het democra-

tisch gelegitimeerde bestuur behartigde belang, en de waarborgen voor de burger; vragen waar de bestuursrechter voor in het leven is geroepen. Voorts gaat het om vragen van wetsuitleg en rechtseenheid, beschermingsomvang van grondrechten, alle een kernactiviteit van een hoogste bestuursrechter. De Afdeling zal bij iedere zaak de (deskundige) mening kunnen vragen van de TIB, de CTIVD, de ministers en diensten en algemeen-belangorganisaties, en van eventuele andere deskundigen die zij wil raadplegen. Ten slotte is het zo dat de Afdeling ook de hoogste bestuursrechter in zaken van gegevensbescherming is.[284] De ontwikkelingen in de inter- en supranationale jurisprudentie[285] laten zien dat het recht betreffende de inlichtingen- en veiligheidsdiensten steeds meer onderhevig wordt aan in het inter- en supranationale recht erkende algemene beginselen van privacyrecht. Niet alleen betekent dit dat op een bepaalde manier al belangrijke expertise in huis is, deze vervlechting leidt ook tot een behoefte aan consistentie op het niveau van de rechtspraak. De procedure bij de Afdeling kan deze consistentie brengen.

In dit verband moet aandacht worden besteed aan een ander aspect van expertise, namelijk de kennis van en ervaring met de technische kant van het werk van de diensten. Is specialistische technische kennis nodig, dan kan de Afdeling zich allereerst richten tot de partijen in de procedure (ministers, TIB en CTIVD) en eventueel één of meer algemeen-belangorganisaties. Daarnaast kan zij zich van die kennis voorzien door een deskundige te benoemen. Voorts kan worden gedacht aan het benoemen van een materie-deskundige als staatsraad in buitengewone dienst.

Rol voor algemeen-belangenbehartigende organisaties

Zoals gezegd is in deze procedure ook ruimte voor een rol van algemeen-belangbehartigers, bijvoorbeeld in de vorm van '*amicus curiae*' (*friend of the court*).[286] Juist als het gaat om de uitleg van wettelijke begrippen of de intensiteit van de toetsing is het waardevol, zowel voor de kwaliteit als de maatschappelijke legitimatie van de uitspraak, dat algemeen-belangbehartigers zich hierover kunnen uitspreken. Het gaat op dit terrein uit de aard der zaak vaak om staatsgeheime informatie, waarvan derden (waaronder algemeen-belangorganisaties) vanzelfsprekend geen kennis kunnen nemen. Is die informatie noodzakelijk om een uitspraak op het verzoek te kunnen doen, dan zal een rol als *amicus curiae* niet mogelijk zijn.

Aanbeveling 48

Belast de Afdeling bestuursrechtspraak van de Raad van State in eerste en enige instantie met geschilbeslechting en het doen van richtinggevende uitspraken over de uitleg van wettelijke normen en begrippen.

[284] Zie bijvoorbeeld de uitspraken van de ABRvS 1 april 2020, AB 2020, 306-310 over een principiële uitleg van de AVG.
[285] HvJEU 6 oktober 2020, (*Quadrature du Net and others*); HvJEU 6 oktober 2020, (*Privacy International*); EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400, (*Weber en Saravia)*; EHRM 4 december 2015, (*Roman Zakharov)*, r.o. 249, 267, 285; EHRM 13 september 2018, (*Big Brother Watch);* EHRM 19 juni 2018, (*Centrum för Rättvisa)*.
[286] Zie het recentelijk ingediende wetsvoorstel waarbij wordt voorzien in een dergelijke figuur in het bestuursprocesrecht (*Kamerstukken II*, 2019/20, 35 550, nr. 2).

9.6 Benoeming en bezetting van TIB en CTIVD

9.6.1 Inleiding

De benoemingsprocedure voor de leden van de TIB en CTIVD[287] is ongewijzigd overgenomen uit de Wiv 2002, waarin de benoemingsprocedure voor de leden van de CTIVD was geregeld. De TIB is geïntroduceerd bij de Wiv 2017, zodat deze procedure voor deze commissie nieuw is. Met de introductie van de afdeling klachtbehandeling bij de CTIVD is deze procedure ook gaan gelden voor de benoeming van de leden van die afdeling.

De procedure is destijds opgezet naar analogie van artikel 2, lid 2, van de Wet Nationale ombudsman met het oog op de vereiste onafhankelijkheid van de CTIVD,[288] met dien verstande dat bij de benoeming van de Nationale ombudsman de regering niet betrokken is. De procedure start met een aanbeveling door de vice-president van de Raad van State, de president van de Hoge Raad en de Nationale ombudsman. Op basis van deze aanbeveling doet de Tweede Kamer per vacature een (openbare) voordracht van ten minste drie personen, waaruit de betrokken ministers hun keuze maken. Benoeming vindt plaats bij koninklijk besluit. Het lidmaatschap van de TIB en de CTIVD betreft een vertrouwensfunctie. De eindkandidaten worden, alvorens zij kunnen worden benoemd, aan een veiligheidsonderzoek onderworpen. De totale duur van de wervings- en selectieprocedure van de leden van de TIB en van de CTIVD was in de periode 2017/2018 gemiddeld zeven maanden.

9.6.2 Benoemingsprocedure leden TIB en CTIVD

De benoemingsprocedure van leden van de TIB en CTIVD is zeer zorgvuldig opgezet en alle staatsmachten zijn daarbij betrokken. Dat zorgt voor een breed draagvlak en past bij colleges met een dergelijke belangrijke taak, vergaande bevoegdheden en unieke positie. De voorzitters van de TIB en CTIVD hebben aandacht gevraagd voor het feit dat zij het als een gemis ervaren dat zij geen enkele rol in de benoemingsprocedure hebben, zelfs geen informele en raadgevende. Dit klemt temeer omdat het kleine colleges zijn en nauwe samenwerking noodzakelijk is.

De keerzijde van deze zorgvuldige procedure is dat deze gecompliceerd en tijdrovend is. Met name bij de TIB kan dit operationele gevolgen hebben als vervanging niet snel kan plaatsvinden. Aan dit bezwaar zou tegemoet kunnen worden gekomen door het in de wet mogelijk te maken in noodgevallen een tijdelijke waarnemer te benoemen via een lichtere procedure, zoals dat ook in de Wet Nationale ombudsman is geregeld.[289] Een andere en wellicht meer voor de hand liggende manier om dit knelpunt op te lossen is de benoeming van een aantal plaatsvervangende leden van de TIB, die de vaste leden bij verhindering of ontstentenis kunnen vervangen. Daartoe is een wetsvoorstel ingediend, dat momenteel aanhangig is bij de Eerste Kamer.[290] In dit wetsvoorstel is echter niet voorzien in een lichtere benoemingsprocedure van plaatsvervangende leden. Deze procedure is daarom even gecompliceerd en tijdrovend als de procedure voor de benoeming van de vaste leden. Dit pleit ervoor om in de toekomst voldoende plaatsvervangers te benoemen, waarop bij plotselinge uitval van een vast lid een beroep kan worden gedaan. Van het beschikbaar zijn van verschillende plaatsvervangers kan bovendien gebruik worden gemaakt als de TIB in bijvoorbeeld operationeel, technisch en juridisch zeer complexe operaties ook wil putten uit de kennis van plaatsvervangers.

---

[287] Artikel 99 jo. 33 Wiv 2017.
[288] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 81 e.v. (MvT Wiv 2017).
[289] Artikel 2, vijfde lid, Wet Nationale ombudsman.
[290] *Kamerstukken II* 2018/19, 35 242, nr. 2 (MvT Wijziging van de Wiv 2017).

Bij de huidige benoemingsprocedure blijkt het vaak niet mogelijk om voor elke vacature het wettelijk vereiste aantal van drie kandidaten voor te dragen. In de praktijk trekken mensen zich regelmatig terug, waardoor de openbare voordracht van drie personen vaak niet wordt gehaald. Dat is ook wel begrijpelijk vanuit het perspectief van de kandidaten die niet als eerste kandidaat worden voorgedragen. Gezien het feit dat de wet op dit punt regelmatig niet kan worden nageleefd, ligt het voor de hand om het wettelijk vereiste van drie kandidaten los te laten, zodat zo nodig kan worden volstaan met minder dan drie kandidaten. Dit zou kunnen worden opgelost door in de wet de woorden "ten minste drie kandidaten" te vervangen door "zo mogelijk drie kandidaten". Ook schuurt het dat de namen van de kandidaten bekend worden gemaakt voordat het veiligheidsonderzoek is afgerond (bij vertrouwensfuncties is het gebruikelijk dat dit pas gebeurt ná positieve afronding van het onderzoek). Dit pleit ervoor om de wet op deze punten aan te passen in die zin dat de voordracht van de te benoemen kandidaten geheim blijft totdat door de Ministerraad is beslist op de voordracht, inclusief succesvolle afronding van het veiligheidsonderzoek.

Aanbeveling 49

Behoud de benoemingsprocedure voor leden van de TIB en de CTIVD zoals deze nu is en neem daarbij een raadgevende rol van de voorzitter van het betreffende college op.

Aanbeveling 50

Maak ofwel een lichtere procedure mogelijk voor benoeming van een tijdelijke waarnemer voor de TIB op korte termijn ofwel benoem - na inwerkingtreding van het wetsvoorstel tot wijziging van de Wiv 2017 - voldoende plaatsvervangende leden van de TIB.

Aanbeveling 51

Laat het wettelijk vereiste vallen dat drie kandidaten voor de TIB en de CTIVD in het openbaar moeten worden voorgedragen en vervang "ten minste drie personen" door "zo mogelijk drie personen".

Aanbeveling 52

Maak de naam van de te benoemen kandidaten pas openbaar na (positieve) afronding van het veiligheidsonderzoek.

9.6.3 Rechtspositie TIB en CTIVD

In de Wiv 2017 is bepaald dat de bezoldiging, de aanspraken in geval van ziekte, alsmede de overige rechten en plichten met betrekking tot de rechtspositie van de leden van de TIB en de CTIVD bij algemene maatregel van bestuur (AMvB) worden geregeld. De Evaluatiecommissie acht het gezien de posities en de onafhankelijkheid van beide commissies passender om deze onderwerpen op hoofdlijnen in de Wiv te regelen, waarbij delegatie naar een AMvB mogelijk zal zijn.

Aanbeveling 53

Regel de rechtspositie van de TIB en de CTIVD op hoofdlijnen in de Wiv, met mogelijkheid van delegatie naar een AMvB.

9.6.4 Bezetting TIB

In deze evaluatie is duidelijk geworden dat de TIB in de huidige vorm een kwetsbare organisatie is vanwege het beperkt aantal leden. Dit brengt het risico met zich mee dat de TIB door uitvallen van leden haar rol in het operationele proces niet (effectief) kan vervullen. Daarnaast vragen de aan TIB voorliggende complexe vraagstukken om brede en specifieke expertise.

De TIB bestaat uit drie leden. Gedurende de onderzoeksperiode van deze evaluatie bestond de TIB slechts uit twee leden vanwege het vertrek van één lid, en de lange tijd die gemoeid gaat met benoeming van een opvolger. De ambtelijke ondersteuning bestaat uit een secretariaat bemenst door drie personen.

Om effectief te kunnen toetsen, moet de TIB voldoende bemenst zijn. De vereiste deskundigheid onder potentiële kandidaten is echter schaars, vooral op technisch vlak, en dat maakt de TIB kwetsbaar in geval dat er vervanging nodig is. Het is niet gemakkelijk om mensen te vinden met de juiste expertise op het hoge niveau dat voor het toezicht vereist is, én die voldoende tijd hebben om dit belangrijke werk te verrichten.

De leden en de ondersteuning van de TIB werken hard om hun taken zo snel en goed mogelijk te vervullen. Voor zover de Evaluatiecommissie kan beoordelen, is het operationele proces nooit in het gedrang gekomen door vertraging aan de zijde van de TIB. Dat is knap. Het risico dat zich dit in de toekomst wel zal voordoen, is echter aanwezig. Daarom is het goed dat er met het voorstel tot wijziging van de Wiv 2017 plaatsvervangers komen. Die plaatsvervangers krijgen naar de Evaluatiecommissie begrijpt echter alleen een rol om in te springen bij langdurige afwezigheid van de leden van de TIB, zo kan worden opgemaakt uit de toelichting op het wetsvoorstel.[291] De Evaluatiecommissie beveelt aan om de plaatsvervangende leden niet alleen een rol te geven in geval van langdurige afwezigheid, maar ook bij kortstondige afwezigheid. Daarnaast kan het gewenst zijn om in uitzonderlijke gevallen juist ook gebruik te maken van de expertise van plaatsvervangende leden door hen te betrekken bij de toetsing. De Evaluatiecommissie acht dit voorstelbaar in geval van technisch, juridisch en operationeel complexe operaties, waarin hun expertise van pas komt.

[291] *Kamerstukken II* 2018/19, 35 242, nr. 3, p. 8 (MvT Wiv 2017).

Bij de benoeming van plaatsvervangende leden moet wel rekening worden gehouden met de benodigde ervaring. De wet vereist dat een meerderheid van de TIB specifieke rechterlijke ervaring van ten minste zes jaar heeft (artikel 33, lid 2). Dit sluit ook aan bij de jurisprudentie van het EHRM waarin wordt verwezen naar het rechterlijk model. Daarbij worden overigens afwijkingen aanvaard, mits onder meer onafhankelijkheid en toepassing van proportionaliteitseisen zijn gegarandeerd.[292] Voor het derde lid van de TIB geldt dit benoembaarheidsvereiste niet; dat lid kan ook andere expertise hebben, zoals een technische achtergrond of kennis over het inlichtingenwerk.

De Evaluatiecommissie vindt het met het oog op de robuustheid van de TIB denkbaar en wenselijk om het aantal expertises binnen de TIB uit te breiden door plaatsvervangende leden met andere achtergronden te benoemen, naast (een of meer) plaatsvervangers met rechterlijke achtergrond ter vervanging van de twee vaste leden als bedoeld onder artikel 33, lid 2. Zo ontstaat er een groep van plaatsvervangende leden die niet alleen de vaste leden kunnen vervangen in geval van afwezigheid, maar ook kunnen worden geraadpleegd door de vaste leden in geval van een complexe operatie. Het dusdanig verbreden van expertise is mogelijk zonder te tornen aan het uitgangspunt dat de TIB primair de rechtmatigheid toetst en daarom voor de meerderheid uit (plaatsvervangende) leden met een rechterlijke achtergrond bestaat.

Ook zou de TIB gebruik moeten kunnen maken van een kenniskring, zoals de CTIVD ook heeft. Deze kenniskring kan een waardevolle aanvulling vormen op de reeds in de commissie aanwezige expertise. Voor het delen van staatsgeheime informatie zou wel een voorziening moeten worden getroffen.

Aanbeveling 54

Maak het de TIB mogelijk intensiever te werken met plaatsvervangers met verschillende achtergronden, zowel ter vervanging van een vast lid in geval van (langdurige) afwezigheid als ter aanvulling op de aanwezige expertise (in geval van technisch, juridisch en/of operationeel complexe operaties).

Aanbeveling 55

Maak het de TIB mogelijk gebruik te maken van een kenniskring.

[292] EHRM 6 september 1978, (*Klass en anderen tegen Duitsland)*, par. 55-56; EHRM 18 mei 2010, ECLI:CE:ECHR:2010:05 18JUD002683905, (*Kennedy tegen Verenigd Koninkrijk)*, par. 167 en 184–191; EHRM 12 januari 2016, (*Szabó en Vissy)*, par. 79.

9.7 Conclusies en aanbevelingen

De Evaluatiecommissie vindt dat het stelsel van toezicht zich in twee jaar tijd goed heeft gezet en dat het toezicht op het handelen van de diensten stevig is ingebed. De TIB is van grote meerwaarde gebleken en het toezicht van de CTIVD, wat in toenemende mate dynamisch wordt ingevuld, is een onverminderd belangrijke waarborg. Met de overheveling van de klachtbehandeling naar de CITVD is de toegankelijkheid voor de burger niet verminderd. De afdeling klachtbehandeling voert haar taken naar het oordeel van de Evaluatiecommissie zorgvuldig uit.

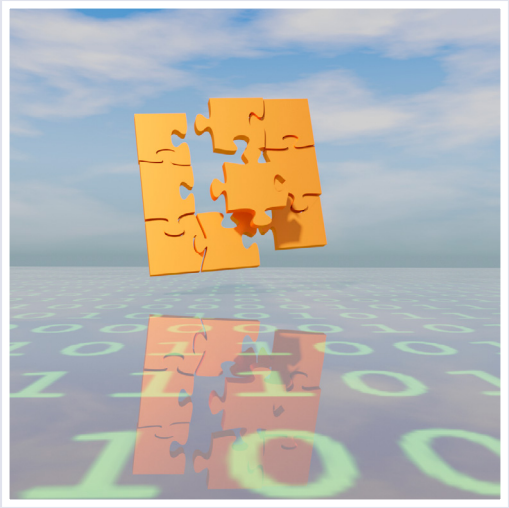
Wel ziet de Evaluatiecommissie dat er spanningen zijn ontstaan in het stelsel ten aanzien van het object van en de normstelling bij de ex-ante toets. Deze spanningen zijn het gevolg van een stelsel waarin de relatie tussen ex-ante en ex-post toezicht niet goed is doordacht. Zo heeft de wetgever de TIB niet alleen een rol toegewezen bij verwerving van gegevens – wat past bij de aard van de ex-ante toets – maar ook bij bepaalde bevoegdheden in de verwerkingsfase. Daarnaast bieden de wet en de wetsgeschiedenis onvoldoende aanknopingspunten voor differentiatie van de invulling van de open toetsingsnormen. De Evaluatiecommissie beveelt aan om de TIB-toets te beperken tot de fase van verwerving, waarbij de toets niet strekt tot aspecten van verwerking. Bij deze autoriserende rol past het niet om voorwaarden aan een rechtmatigheidsoordeel te verbinden.

Met deze aanpassingen wordt de relatie tussen het ex-ante en ex-post toezicht verduidelijkt en daarmee de diffuse rolverdeling binnen het stelsel van toezicht verhelderd. Wel benadrukt de Evaluatiecommissie dat aansluiting van de rol van de TIB en van de CTIVD een belangrijke voorwaarde voor effectief toezicht is. Door middel van het voeren van beleidseenheidsoverleg, waarin casuïstiek wordt besproken, kunnen de ex-ante toets en het ex-post toezicht elkaar versterken. Dit is een stap naar beter geïntegreerd toezicht.

De Evaluatiecommissie beveelt aan om balans aan te brengen in het stelsel van toezicht door een rechterlijke procedure mogelijk te maken in geval van geschillen over de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen en de intensiteit van de toetsing. De Afdeling bestuursrechtspraak van de Raad van State wordt aanbevolen als enige en hoogste rechter in deze geschillen. Deze procedure kan ook ruimte bieden aan algemeen-belangbehartigers, wat het maatschappelijke debat ten zal goede zal komen. Ook wordt met deze procedure de weg vrijgemaakt om prejudiciële vragen te stellen aan het EHRM of het HvJEU.

Tenslotte doet de Evaluatiecommissie voor de benoeming en de bezetting van zowel de TIB als de CTIVD verschillende aanbevelingen. Zo is het wenselijk de benoemingsprocedure van de leden van de TIB en CTIVD op enkele punten aan te passen en zou de TIB, onder meer vanwege de kwetsbaarheid, de mogelijkheid moeten krijgen om intensiever met plaatsvervangende leden te werken.

Deel III



10 Overige bevindingen

Tenslotte heeft de Evaluatiecommissie nog enkele bevindingen gedaan die niet goed passen binnen de drie overkoepelende thema's zoals behandeld in de voorgaande hoofdstukken, maar die wel belangrijk zijn om te worden weergegeven.

10.1 Overgangsrecht

De Wiv 2017 moest in korte tijd, zonder overgangsrecht, geïmplementeerd worden. Zoals toegelicht in hoofdstuk 9 betekende dit voor de TIB dat zij in zeer korte tijd de complexe materie eigen moest maken en de nodige organisatorische maatregelen moest treffen. Voor de diensten betekende de afwezigheid van overgangsrecht dat de implementatie van de wet van de een op de andere dag feit was terwijl 'de winkel open diende te blijven'. Dat dit niet altijd gemakkelijk was, blijkt uit meerdere voortgangsrapportages van de CTIVD.[293] Uit de laatste rapportage van de CTIVD kan worden opgemaakt welke stappen de diensten hebben gezet in het beperken van rechtmatigheidsrisico's.[294]

In de wet is niet voorzien in overgangsbepalingen en er is, met uitzondering van de PIA, geen voorafgaande impactanalyse uitgevoerd. Daardoor was niet precies duidelijk wat de invoering van de wet in praktische zin voor consequenties had en was de wet van het ene op het andere moment van kracht, zonder een tussentijds regime voor onder meer de al lopende toestemmingen voor de inzet van bevoegdheden. Tegelijk moest de TIB vanaf de eerste dag een nieuw toetsingskader hanteren. Het gebrek aan overgangsbepalingen en een impactanalyse heeft aan een soepele overgang van de Wiv 2002 naar de Wiv 2017 in de weg gestaan. De Evaluatiecommissie beveelt aan om bij een toekomstige wetswijziging tijdig aandacht te hebben voor de implementatie daarvan en bij iedere afzonderlijke wijziging te overwegen of overgangsrecht nodig is.[295] In het vervolg is ook een ICT-uitvoeringstoets bij wijzigingen van de wet aan te bevelen.

Aanbeveling 56

Bij een toekomstige wetswijziging moet tijdig aandacht zijn voor de implementatie daarvan en bij iedere afzonderlijke wetswijziging moet worden overwogen of overgangsrecht nodig is.

Aanbeveling 57

Doe een ICT-uitvoeringstoets bij wijzigingen van de wet.

[293] Zie de verschillende voortgangsrapportages van de CTIVD.
[294] CTIVD. (2020). *CTIVD nr. 69, Voortgangsrapportage IV over de implementatie van de Wiv 2017*. p. 14-15.
[295] Zie Aanwijzing 5.59 van de Aanwijzingen voor de regelgeving, die luidt: Bij een nieuwe regeling of wijziging van een regeling wordt overwogen of overgangsbepalingen noodzakelijk zijn.

10.2 Vestigingsklimaat

Naar aanleiding van een motie van Kamerlid Verhoeven (D66)[296] heeft de Evaluatiecommissie ook gekeken naar de effecten van de Wiv 2017 op het Nederlandse vestigingsklimaat. Tijdens de totstandkoming van de wet heeft een bedrijfseffectentoets uitgewezen dat de verwachte impact van de wet zeer gering zou zijn.[297] De Evaluatiecommissie heeft het externe onderzoeksbureau Verdonck, Klooster & Associates (VKA) gevraagd om te kijken in hoeverre deze verwachting is uitgekomen sinds de inwerkingtreding van de wet.

Binnen de verschillende invalshoeken van het onderzoek[298] zijn geen directe argumenten gevonden om te onderbouwen dat de inwerkingtreding van de Wiv 2017 enig negatief effect heeft gehad op het vestigingsklimaat in Nederland. Nederland scoort onverminderd hoog op internationale ranglijsten die zien op het vestigingsklimaat, digitalisering en rechtsorde en analyse van CBS-cijfers toont een groei van het aantal bedrijven in de ICT-telecommunicatiesector. Tijdens interviews met vertegenwoordigers van het bedrijfsleven, brancheorganisaties en relevante overheidsorganisaties zijn bovendien zelfs voorzichtig positieve geluiden gehoord over de verhoogde transparantie en aanvullende waarborgen. Hierdoor lijkt Nederland zich in positieve zin te onderscheiden.

10.3 Openbaarheid

De Evaluatiecommissie noemde in §2.3 al de complexiteit van de wet. Het vereist een grote inspanning om deze ingewikkelde en specialistische materie te doorgronden en eigen te maken. Dit draagt niet bij aan de kennis over het werk van de diensten. Om deze kennis te vergroten, kunnen de diensten zelf meer in de openbaarheid treden. Recentelijk heeft de Evaluatiecommissie hier een paar goede voorbeelden van gezien.[299] De Evaluatiecommissie moedigt de diensten aan om ook in de toekomst in de openbaarheid te blijven treden en – dit waar mogelijk gezien het soort werk van de diensten – uit te breiden. Hierdoor kan de samenleving beter inzicht krijgen in de aard en omvang van de dreigingen die spelen, waarom het nodig kan zijn bepaalde bevoegdheden in te zetten en waarom daar in het belang van de nationale veiligheid voor wordt gekozen.

Bovendien zou een volledig(er) beeld kunnen worden gegeven van de wijze waarop de diensten invulling geven aan hun zorgplicht. Het werk van de diensten wordt nu vaak in de openbaarheid gebracht door middel van rapporten van de toezichthouder. Daarin ligt de focus begrijpelijkerwijs over het algemeen op de zaken die *niet* goed gaan bij de diensten. Als de diensten een eigen verhaal te vertellen hebben, dan moedigt de Evaluatiecommissie hen aan dit te doen.[300]

---

[296] *Kamerstukken II* 2016/17, 34 588, nr. 53 (motie Kamerlid Verhoeven).

[297] *Handelingen II* 2016/17, 50-10, p. 63.

[298] Het rapport van VKA is, tezamen met het eindrapport van de Evaluatiecommissie, digitaal ter inzage beschikbaar op de website van de rijksoverheid **http://rijksoverheid.nl**.

[299] Zie onder meer: NOS. (4 oktober 2018). *MIVD: we hebben Russische hack van OPCW in Den Haag voorkomen*. Beschikbaar via **https://nos.nl/collectie/13693/artikel/2253313-mivd-we-hebben-russische-hack-van-opcw-in-den-haag-voorkomen**; NOS. (12 oktober 2020). *MIVD-baas waarschuwt: telefoons en tablets van tafel bij vergaderingen*. Beschikbaar via **https://nos.nl/artikel/2351988-mivd-baas-waarschuwt-telefoons-en-tablets-van-tafel-bij-vergaderingen.html**; NOS. (10 oktober 2020). *AIVD ontmaskert twee Russische diplomaten als spionnen*. Beschikbaar via **https://nos.nl/artikel/2360085-aivd-ontmaskert-twee-russische-diplomaten-als-spionnen.html**.

[300] In dit kader verwijst de Evaluatiecommissie ook naar het Anderson rapport waarin voorbeelden worden gegeven van het werk van de Britse diensten. Anderson, D. (2016). *Report of the Bulk Powers Review.* Independent Reviewer of Terrorism Legislation.

10.4 Administratieve organisatie

De invoering van de wet heeft gezorgd voor een verbetering van de administratieve organisatie van de diensten. Zo heeft de instelling van de TIB geleid tot een verbeterd proces voor de toestemmingsaanvragen tot de inzet van bijzondere bevoegdheden. Daarnaast heeft de zorgplicht en het toezicht van de CTIVD geleid tot een verbetering van de interne datahuishouding (zie §9.2.5). Tegelijkertijd brengt de versterking van de waarborgen, inclusief de zorgplicht, ook een grotere werkbelasting met zich mee voor de diensten. Deze lastenverzwaring hoort voor een deel bij de noodzakelijke professionalisering van een organisatie. Waar de Evaluatiecommissie is gestuit op mogelijkheden om processen te versimpelen en te stroomlijnen, heeft zij hiertoe aanbevelingen gedaan. Aangezien deze evaluatie gericht is op de wet is niet naar de gehele (administratieve) organisatie van de diensten gekeken. Daarom moedigt de Evaluatiecommissie de diensten aan om voortdurend kritisch te blijven kijken naar de eigen administratieve processen.

10.5 Verhouding bewaartermijnen en Archiefwet

Eén van de specifieke onderwerpen die volgt uit de opdracht van de Evaluatiecommissie is de vraag hoe de Wiv 2017 zich voor wat betreft het datareductiestelsel (waaronder de bewaartermijnen) verhoudt tot de Archiefwet 1995.[301] De Wiv wijkt wat betreft bewaartermijnen, overdracht aan het rijksarchief en vernietiging sterk af van de regeling in de Archiefwet. De Evaluatiecommissie heeft onvoldoende gelegenheid gehad om dit zorgvuldig te onderzoeken.

[301] *Kamerstukken I* 2019/20, 34 588, nr. M (Kamerbrief Evaluatie Wiv 2017).

11 Overzicht conclusies en aanbevelingen

Hieronder staat een overzicht van de verschillende conclusies en aanbevelingen uit de verdiepende hoofdstukken.

11.1 Conclusies en aanbevelingen hoofdstuk 4 Bulkdata

De Evaluatiecommissie onderschrijft het belang van bulkdata voor de taakuitvoering van de diensten. Tegelijkertijd is het verwerven en verwerken van bulkdata gevoelig vanwege de aard daarvan. Het omvat gegevens van personen en/of organisaties die niet in onderzoek zijn van de diensten en dat ook nooit zullen worden. Juist over de nut en noodzaak van de verzameling van grote hoeveelheden gegevens is veel maatschappelijke discussie. De Wiv 2017 voorziet nu niet in de nodige waarborgen voor zorgvuldige omgang met bulkdata. Niet alleen is de wet qua waarborgen te veel gericht op de bevoegdheid waar gegevens mee worden verworven, de wet spreekt bovendien alleen van bulk in het kader van OOG-interceptie. Daardoor is zowel de bulkverwerving als de daaropvolgende verwerking in de wet niet uniform geregeld en onvoldoende voorzienbaar. In de verschillende aanbevelingen maakt de Evaluatiecommissie gebruik van het conceptueel en praktisch nuttige onderscheid tussen register-bulkdata en gedragbulkdata.

Er is meer uniformiteit en met name voorzienbaarheid nodig in de verschillende manieren waarop de diensten bulkdata kunnen *verwerven*. Hiertoe is een bulkparagraaf in de wet de aangewezen weg. Ook is een extra stap in de huidige toestemmingsprocedure voor bulkverwerving nodig: het aantonen van de bulkbehoefte. Hierbij wordt de noodzakelijkheid van bulk gemotiveerd. Voordat tot verwerving wordt overgegaan, moet de betrokken minister akkoord zijn met de behoefte. Dit betekent een extra waarborg ten opzichte van de huidige situatie. Voor de verwerving van bulkdata beveelt de Evaluatiecommissie een passende invulling van het gerichtheidsvereiste aan. Naast het terugbrengen van aantal personen/organisaties in de bulkdataset, wordt een nieuwe invulling van gerichtheid geïntroduceerd aan de hand van datapunten.

De belangrijkste aanbeveling van de Evaluatiecommissie ten aanzien van de *verwerking* van bulkdata is om een uniform systeem van waarborgen te introduceren voor álle bulkdata, onafhankelijk van de wijze waarop deze bulkdata is verkregen. In dit systeem gelden handelings-, toegangs- en tijdswaarborgen, gebaseerd op het huidige OOG-stelsel. Gegevens uit bulkdata moeten worden geselecteerd voordat deze kunnen worden gebruikt in het inlichtingenproces (handelingswaarborg). Medewerkers uit dit inlichtingenproces hebben in beginsel geen toegang tot bulkdata (toegangswaarborg). Daarnaast moet alle bulkdata op relevantie worden beoordeeld op basis van de operationele waarde, binnen een termijn van drie jaar (tijdswaarborg). Tenslotte geldt voor het delen van bulkdata met buitenlandse diensten de eis van ministeriële toestemming en meldplicht aan de CTIVD (handelingswaarborg). Ten opzichte van de huidige situatie betekent dit een verzwaring van de waarborgen op handeling en toegang. Voor de tijdswaarborg geldt dat het enerzijds een verzwaring is van de waarborgen doordat alle bulkdata op relevantie moet worden beoordeeld. Anderzijds is de beoordelingstermijn verlengd van maximaal anderhalf naar drie jaar.

1. Neem in de wet een bulkparagraaf op.
2. Kom tot één grondslag voor het verkrijgen van gegevens (inclusief bulkdata) van Nederlandse medeoverheden.
3. Voeg een stap aan het toestemmingsproces toe waarbij de bulkbehoefte voorafgaand aan het inzetverzoek ter toestemming wordt voorgelegd aan de minister.

4. Neem in de wet op dat het gerichtheidscriterium bij de verwerving van bulkdata kan worden ingevuld aan de hand van zowel het terugbrengen van aantallen personen en/of organisaties als het terugbrengen van het aantal te verwerven datapunten.
5. Leg een uniform verwerkingsregime voor alle bulkdata in de wet vast.
6. Laat het wettelijk onderscheid tussen metadata en inhoud los.
7. Verklaar de selectiebevoegdheid van toepassing op alle bulkdata, zonder onderscheid tussen inhoud en metadata.
8. Beleg het toestemmingsniveau voor selectie intern bij de diensten.
9. Laat ruimte bestaan voor onderbouwde uitzonderingen, waar een versimpelde selectieprocedure kan worden gevolgd.
10. Het verstrekken van bulkdata aan buitenlandse diensten wordt op het niveau van de minister belegd en is onderhevig aan meldplicht aan de CTIVD. Het wettelijke onderscheid tussen 'geëvalueerd' en 'ongeëvalueerd' komt daarmee te vervallen.
11. Maak bulkdata niet toegankelijk voor alle medewerkers in het inlichtingenproces. Slechts bepaalde functionarissen krijgen toegang voor search gericht op selectie.
12. Het vereiste van relevantiebeoordeling geldt voor alle bulkdata.
13. Stel een termijn in van drie jaar voor de relevantiebeoordeling van bulkdata.
14. Verklaar het vereiste van zo spoedig mogelijk niet van toepassing op de relevantiebeoordeling van bulkdata.
15. Koppel de relevantiebeoordeling niet aan specifieke personen/organisaties maar aan de operationele waarde. Hierbij kan het onderscheid register- en gedrag-bulkdata nuttig zijn.
16. Toets de als relevant aangemerkte bulkdata eerder en vaker op betekenis.

11.2 Conclusies en aanbevelingen hoofdstuk 5 GDA

Grootschalige gegevensverwerking is een kernactiviteit van de diensten. GDA is in de Wiv 2017 opgenomen om de diensten een grondslag te bieden voor het doen van geavanceerde vormen van gegevensverwerking. Omdat de toepassing hiervan op OOG-metadata als extra gevoelig werd gezien, zijn daarvoor waarborgen in het leven geroepen: om GDA te verrichten met OOG-metadata moet vooraf toestemming gevraagd worden aan de minister, getoetst door de TIB.

Aangezien deze waarborg op OOG-metadata de enige waarborg op het verwerken betrof, is er in de zoektocht naar een gemeenschappelijk wettelijk kader een situatie ontstaan waarin het begrip GDA uiteindelijk vrijwel elke vorm van gegevensverwerking omvat. De discussie hierover tussen de minister en de diensten enerzijds en de TIB en CTIVD anderzijds is vastgelopen. Dit rapport doet een voorstel om uit deze situatie te geraken.

De Evaluatiecommissie beveelt aan om een specifiek omschreven categorie gegevensverwerking, GDA+, te introduceren. GDA+ komt in de plaats van het oorspronkelijke GDA begrip en moet worden voorzien van extra handelingswaarborgen: voor het ontwikkelen van nieuwe technische functionaliteiten ten behoeve van GDA+ moet de betrokken minister vooraf toestemming geven en de CTIVD kan op de ontwikkeling en de toepassing systeemtoezicht houden.

17. Herdefinieer de categorie gegevensverwerking (hier genoemd GDA+) die voorzien moet worden van handelingswaarborgen. Het oorspronkelijke begrip GDA wordt vervangen door GDA+.

18. Voor het ontwikkelen van nieuwe technische functionaliteiten ten behoeve van GDA+ moet de betrokken minister vooraf toestemming geven. Als deze toestemming wordt gegeven, dan wordt de CTIVD daarvan op de hoogte gebracht.

11.3 Conclusies en aanbevelingen hoofdstuk 6 OOG-interceptie

De mogelijkheid om te kunnen intercepteren op de kabel was de belangrijkste modernisering van de Wiv 2017. Het is sinds de introductie van deze wet, nu ruim twee jaar geleden, de diensten nog niet gelukt deze bevoegdheid in zijn volledigheid in te zetten. Dat komt vooral doordat OOG-interceptie op de kabel technisch, juridisch en organisatorisch een complexe en bovendien nieuwe bevoegdheid is. Ook het ontwikkelen van een gemeenschappelijk begrippenkader waardoor voor alle stappen in het OOG-stelsel toestemming kon worden gevraagd én kon worden getoetst, vergt kennelijk de nodige inspanningen.

De belangrijkste aanbevelingen in dit hoofdstuk betreffen het stroomlijnen, optimaliseren en soms repareren van het oorspronkelijke OOG-stelsel. Er worden geen fundamentele wijzigingen voorgesteld en de oorspronkelijke waarborgen blijven intact.

De aanbevelingen stellen de diensten in staat om op basis van metingen een geschikte accesslocatie uit te zoeken. Dit komt de gerichtheid van de inzet van het middel ten goede en doet meer recht aan het strategische karakter van een accesslocatie. Ook de eventuele toestemmingsaanvraag voor interceptie is door de metingen beter te onderbouwen en te toetsen. Daarnaast wordt aanbevolen om artikel 52 van een termijn te voorzien waarbinnen de aanbieders van communicatiediensten een informatieverzoek moeten beantwoorden. Tenslotte wordt er een aanbeveling gedaan om in de wettelijke bepaling voor OOG-interceptie een uitzondering te maken op de eis van ministeriële toestemming en toets door de TIB voor interceptie van militair HF-verkeer.

19. Koppel artikel 53 los van artikel 48 en introduceer een artikel '52 a' waarmee de diensten metingen kunnen doen bij bepaalde aanbieders.
20. Voorzie de verplichting van artikel 52 van een termijn van vier weken.
21. Voeg *search* gericht op interceptie toe aan de huidige wettelijke bepaling voor de interceptiebevoegdheid.
22. Maak in de wettelijke bepaling voor OOG-interceptie een uitzondering voor militair HF-verkeer, net als bij gerichte interceptie.

11.4 Conclusies en aanbevelingen hoofdstuk 7 De hackbevoegdheid

Door het toenemend gebruik van computers is de hackbevoegdheid een essentiële bevoegdheid voor de diensten. Tegelijkertijd is de hackbevoegdheid één van de meest indringende bevoegdheden, omdat computers steeds meer informatie over het privéleven van personen bevatten. Met de hackbevoegdheid kan heimelijk in computers worden binnengedrongen.

Over het algemeen wordt geconstateerd dat de wet redelijk functioneert, maar op een aantal specifieke punten aanpassingen vergt. Het eerste punt betreft het toestemmingsniveau voor het verkennen van een geautomatiseerd werk, dat moet worden verlaagd van ministerieel niveau naar diensten intern. Dit bevordert de kwaliteit en gerichtheid van de toestemmingsaanvragen

voor het binnendringen van een geautomatiseerd werk, die *wel* langs de minister gaan. Het tweede punt is dat artikel 54, waarmee gegevensbestanden kunnen worden opgevraagd bij aanbieders van telecommunicatie- en opslagdiensten, voorzien moet worden van een bijschrijfmogelijkheid. Beide punten worden ondersteund door zowel de diensten als de TIB.

Verder is gebleken dat de toelichting op artikel 45 op sommige punten onvoldoende aansluit bij de snelheid en complexiteit van de hackbevoegdheid. Bij de omschrijving van technische risico's voor de TIB-toets is het gewenst meer richting te geven over de mate van detail waaraan de beschrijving moet voldoen; de vraag wanneer een geautomatiseerd werk in gebruik is bij een actor moet nader toegelicht worden; de voorwaarden waaronder via artikel 45 verworven gegevens van derden gebruikt kunnen worden moeten worden verduidelijkt en; de wetgever moet meer helderheid bieden over het toepassingsbereik van artikel 45 in het kader van strategische operaties.

Tot slot concludeert de Evaluatiecommissie dat de TIB een belangrijke waakfunctie vervult voor de inzet van een zware bevoegdheid als de hackbevoegdheid. Tegelijkertijd kan de snelheid en complexiteit – en daaruit voortvloeiende onvoorzienbaarheid – van cyberoperaties in sommige gevallen wringen met de ex-ante toets door de TIB. In deze gevallen ziet de Evaluatiecommissie in het dynamisch toezicht door de CTIVD een geschiktere vorm van toezicht op de uitvoering van hackoperaties.

23. Beleg het toestemmingsniveau voor verkennen intern bij de diensten.
24. Bied in de toelichting op de wet meer ruimte voor differentiatie in de mate van detail van de omschrijving van de technische risico's voor de ex-ante toets door de TIB.
25. Bied in de toelichting bij artikel 45, lid 8, een werkbare uitleg wanneer een geautomatiseerd werk 'in gebruik is' van een actor.
26. Voorzie artikel 54 van een bijschrijfmogelijkheid.
27. Geef in de toelichting op de wet meer duidelijkheid over het gebruik van gegevens van derden die via artikel 45 en/of 54 worden verworven.
28. Ga in de toelichting op de wet in op het gebruik van bijzondere bevoegdheden voor strategische operaties door middel van voorbeelden om de TIB meer handvatten te bieden voor differentiatie bij de invulling van normen.

11.5 Conclusies en aanbevelingen hoofdstuk 8 Internationale samenwerking

Internationale samenwerking is van belang voor de diensten omdat dreigingen veelal internationaal van aard zijn. Tegelijkertijd moet deze samenwerking wel met voldoende waarborgen zijn omkleed. De belangrijkste observatie van de Evaluatiecommissie ten aanzien van internationale samenwerking is dat de normering van deze samenwerking moet worden uitgebreid en versterkt, zodat deze beter is gespecificeerd en wettelijk verankerd.

De Evaluatiecommissie ziet de introductie van de wegingsnotities in de Wiv 2017 als een belangrijke versterking van deze waarborgen. Hierdoor worden eventuele risico's bij internationale samenwerking beter inzichtelijk en kunnen de juiste maatregelen worden getroffen om deze risico's te mitigeren. De Evaluatiecommissie doet een aantal aanbevelingen die zien op de wegingsnotities, waaronder het opnemen van de inrichting en effectiviteit van het toezicht als een apart wegingscriterium in de wet. Ook beveelt de Evaluatiecommissie aan om – als de

wetgever dit wil toestaan – een expliciete grondslag op te nemen voor samenwerking met niet-statelijke groeperingen in het buitenland.

Daarnaast beveelt de Evaluatiecommissie aan om een aantal meer inhoudelijke normen in de wet te specificeren en te verankeren. Het gaat hierbij onder meer om een verbod op het delen van register-bulkdata van Nederlandse medeoverheden, een inspanningsverplichting tot het filteren – waar technisch haalbaar en uitvoerbaar – van kenmerken van bijzondere categorieën personen uit te verstrekken gegevens en van Nederlandse kenmerken uit te verstrekken bulkdata en de verplichting om de ontvangende dienst te verzoeken persoonsgegevens van Nederlandse burgers of ingezetenen, die voorafgaand aan verstrekking niet waren onderkend en verder niet direct relevant zijn voor het onderzoek, te verwijderen bij ontdekking. Ook moet in de wet worden opgenomen dat er geen gegevens worden gedeeld als er een reëel risico bestaat dat gebruik door de ontvangende dienst een flagrante schending oplevert van het internationaal recht, en in het bijzonder de mensenrechten en internationaal humanitair recht. Deze normen sluiten enerzijds aan bij bestaande (inter)nationale jurisprudentie, normen en praktijken en kunnen anderzijds bijdragen aan het ontwikkelen van gedeelde (Europese) normen ten aanzien van internationale samenwerking tussen inlichtingen- en veiligheidsdiensten.

Het is de Evaluatiecommissie tenslotte gebleken dat de CTIVD intensief toezicht houdt op internationale samenwerking. Dit is van groot belang gezien de risico's die hierbij bestaan. Vanwege de toenemende internationalisering en het ontstaan van multilaterale samenwerkingsverbanden beveelt de Evaluatiecommissie aan internationale samenwerking tussen toezichthouders zo veel als mogelijk te faciliteren. Nu de CTIVD algeheel toezicht houdt, ook bijvoorbeeld op het ontstaan en de inhoud van de wegingsnotities, ligt het niet in de rede de TIB een rol te geven bij de internationale verstrekking van gegevens of andersoortige vormen van internationale samenwerking, uitgezonderd waar het de inzet van door de TIB te toetsen bijzondere bevoegdheden (mede) ten behoeve van een buitenlandse dient betreft.

29. Voorzie in een eenduidig wetsartikel als grondslag voor het bevragen van internationale partners en het ontvangen van gegevens van deze partners.
30. Als de wetgever samenwerking met niet-statelijke groeperingen wil toestaan, dan moet in de wet een expliciete wettelijke basis komen met de verplichting tot het opstellen van een wegingsnotitie voor deze samenwerking.
31. Neem 'de inrichting en effectiviteit van het toezicht' op als apart wegingscriterium.
32. Leg de volgende inhoudelijke normen in de wet vast die gelden bij het verstrekken van gegevens aan buitenlandse diensten:
    a) De regel dat er geen gegevens worden gedeeld als er een reëel risico bestaat dat gebruik door de ontvangende dienst een flagrante schending oplevert van het internationaal recht, en in het bijzonder van de mensenrechten en internationaal humanitair recht.
    b) Het verbod op het delen van register-bulkdata van Nederlandse medeoverheden.
    c) De inspanningsverplichting om – waar technisch haalbaar en uitvoerbaar – bij het verstrekken van bulkdata te filteren op specifieke Nederlandse kenmerken.
    d) De algemene inspanningsverplichting – waar technisch haalbaar en uitvoerbaar – tot het filteren van bijzondere categorieën personen, met name journalisten en advocaten, en andere specifieke groepen personen, zoals klokkenluiders en dissidenten.
    e) De verplichting om bij verstrekking van gegevens de ontvangende dienst te verzoeken gegevens over Nederlandse burgers en ingezetenen, die voorafgaand aan verstrekking niet waren onderkend en verder niet direct relevant zijn voor het onderzoek, bij eventuele ontdekking te vernietigen.

f) De verplichting om bij verstrekken van gegevens de ontvangende dienst te verzoeken de gegevens te vernietigen als deze niet (meer) worden gebruikt voor het inlichtingenproces.

33. De CTIVD houdt toezicht op internationale samenwerking, en specifiek ook het verstrekken van (bulk)gegevens. Internationale samenwerking en meer specifiek verstrekking van gegevens/bulkdata worden niet getoetst door de TIB. De TIB heeft alleen een rol bij internationale samenwerking waar het de inzet van door de TIB te toetsen bijzondere bevoegdheden (mede) ten behoeve van een buitenlandse dienst betreft.
34. Leg in de wet vast dat het uniforme verwerkingsregime voor bulkdata óók geldt voor bulkdata ontvangen van buitenlandse diensten.
35. Leg in de wet vast dat voor bulkdata ontvangen van een buitenlandse dienst de minister eerst akkoord moet gaan met de bulkbehoefte alvorens deze bulkdata mag worden gebruikt voor het inlichtingenproces.
36. Leg in de wet vast dat een U-bocht constructie ten aanzien van internationale samenwerking verboden is.
37. Stel voor langdurige multilaterale samenwerking aparte overzichtsnotities op.
38. Moedig de CTIVD aan en faciliteer haar in de voortrekkersrol die zij op zich heeft genomen ter bevordering van internationaal toezicht.
39. Geef de CTIVD de wettelijke bevoegdheid om onderzoek te doen naar aanleiding van een verzoek van een toezichthouder van een buitenlandse partnerdienst.

11.6 Conclusies en aanbevelingen hoofdstuk 9 Stelsel van toezicht

De Evaluatiecommissie vindt dat het stelsel van toezicht zich in twee jaar tijd goed heeft gezet en dat het toezicht op het handelen van de diensten stevig is ingebed. De TIB is van grote meerwaarde gebleken en het toezicht van de CTIVD, wat in toenemende mate dynamisch wordt ingevuld, is een onverminderd belangrijke waarborg. Met de overheveling van de klachtbehandeling naar de CITVD is de toegankelijkheid voor de burger niet verminderd. De afdeling klachtbehandeling voert haar taken naar het oordeel van de Evaluatiecommissie zorgvuldig uit.

Wel ziet de Evaluatiecommissie dat er spanningen zijn ontstaan in het stelsel ten aanzien van het object van en de normstelling bij de ex-ante toets. Deze spanningen zijn het gevolg van een stelsel waarin de relatie tussen ex-ante en ex-post toezicht niet goed is doordacht. Zo heeft de wetgever de TIB niet alleen een rol toegewezen bij verwerving van gegevens – wat past bij de aard van de ex-ante toets – maar ook bij bepaalde bevoegdheden in de verwerkingsfase. Daarnaast bieden de wet en de wetsgeschiedenis onvoldoende aanknopingspunten voor differentiatie van de invulling van de open toetsingsnormen. De Evaluatiecommissie beveelt aan om de TIB-toets te beperken tot de fase van verwerving, waarbij de toets niet strekt tot aspecten van verwerking. Bij deze autoriserende rol past het niet om voorwaarden aan een rechtmatigheidsoordeel te verbinden.

Met deze aanpassingen wordt de relatie tussen het ex-ante en ex-post toezicht verduidelijkt en daarmee de diffuse rolverdeling binnen het stelsel van toezicht verhelderd. Wel benadrukt de Evaluatiecommissie dat aansluiting van de rol van de TIB en van de CTIVD een belangrijke voorwaarde voor effectief toezicht is. Door middel van het voeren van beleidseenheidsoverleg, waarin casuïstiek wordt besproken, kunnen de ex-ante toets en het ex-post toezicht elkaar versterken. Dit is een stap naar beter geïntegreerd toezicht.

De Evaluatiecommissie beveelt aan om balans aan te brengen in het stelsel van toezicht door een rechterlijke procedure mogelijk te maken in geval van geschillen over de uitleg van wettelijke begrippen, de invulling van de toetsingsnormen en de intensiteit van de toetsing. De Afdeling bestuursrechtspraak van de Raad van State wordt aanbevolen als enige en hoogste rechter in deze geschillen. Deze procedure kan ook ruimte bieden aan algemeen-belangbehartigers, wat het maatschappelijke debat ten zal goede zal komen. Ook wordt met deze procedure de weg vrijgemaakt om prejudiciële vragen te stellen aan het EHRM of het HvJEU.

Tenslotte doet de Evaluatiecommissie voor de benoeming en de bezetting van zowel de TIB als de CTIVD verschillende aanbevelingen. Zo is het wenselijk de benoemingsprocedure van de leden van de TIB en CTIVD op enkele punten aan te passen en zou de TIB, onder meer vanwege de kwetsbaarheid, de mogelijkheid moeten krijgen om intensiever met plaatsvervangende leden te werken.

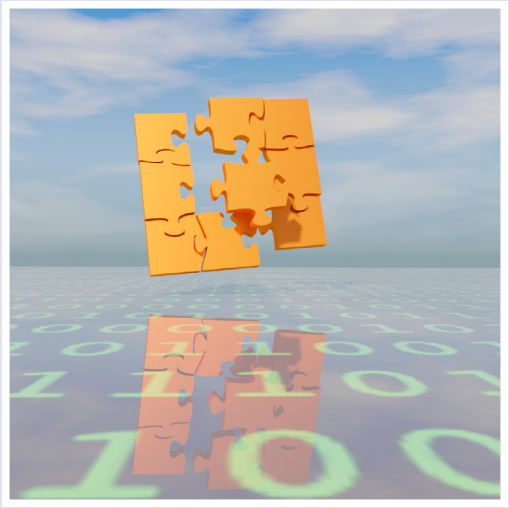
40. De TIB blijft in haar huidige vorm bestaan met behoud van de bevoegdheid om bindend ex-ante te toetsen.
41. De CTIVD afdeling toezicht blijft in haar huidige vorm bestaan met behoud van de huidige bevoegdheden.
42. De afdeling klachtbehandeling van de CTIVD blijft in haar huidige vorm bestaan met behoud van het bindend oordeel.
43. Maak het gebruik van de figuur van de geclausuleerde toestemming niet mogelijk.
44. Verduidelijk de wet en toelichting zodat duidelijk is dat de TIB alleen bij de inzet van verwervende bevoegdheden een rol heeft, niet bij bevoegdheden voor verwerking. Specificeer hierbij ook dat bij deze TIB-toets op de inzet van verwervende bevoegdheden de verwerking van de te verwerven gegevens geen rol speelt.
45. Neem in de toelichting op de wet voorbeelden op van verschillende omstandigheden aan de hand waarvan de TIB de invulling van de normen bij de toets kan differentiëren. Hierbij kan de aard van de verschillende wettelijke taken van de diensten een rol spelen.
46. Intensiveer de samenwerking tussen de TIB en de CTIVD, waarbij casuïstiek wordt besproken in een beleidseenheidsoverleg. De huidige wet vormt hiervoor geen belemmering.
47. Vul het stelsel van toezicht aan met een rol voor de rechter. Deze rechter bepaalt de grenzen van het speelveld van toezicht door de uitleg van wettelijke begrippen, de invulling van toetsingsnormen en de intensiteit van de toetsing.
48. Belast de Afdeling bestuursrechtspraak van de Raad van State in eerste en enige instantie met geschilbeslechting en het doen van richtinggevende uitspraken over de uitleg van wettelijke normen en begrippen.
49. Behoud de benoemingsprocedure voor leden van de TIB en de CTIVD zoals deze nu is en neem daarbij een raadgevende rol van de voorzitter van het betreffende college op.
50. Maak ofwel een lichtere procedure mogelijk voor benoeming van een tijdelijke waarnemer voor de TIB op korte termijn ofwel benoem - na inwerkingtreding van het wetsvoorstel tot wijziging van de Wiv 2017 - voldoende plaatsvervangende leden van de TIB.
51. Laat het wettelijk vereiste vallen dat drie kandidaten voor de TIB en de CTIVD in het openbaar moeten worden voorgedragen en vervang “ten minste drie personen” door “zo mogelijk drie personen”.
52. Maak de naam van de te benoemen kandidaten pas openbaar na (positieve) afronding van het veiligheidsonderzoek.
53. Regel de rechtspositie van de TIB en de CTIVD op hoofdlijnen in de Wiv, met mogelijkheid van delegatie naar een AMvB.

54. Maak het de TIB mogelijk intensiever te werken met plaatsvervangers met verschillende achtergronden, zowel ter vervanging van een vast lid in geval van (langdurige) afwezigheid als ter aanvulling op de aanwezige expertise (in geval van technisch, juridisch en/of operationeel complexe operaties).
55. Maak het de TIB mogelijk gebruik te maken van een kenniskring.

11.7 Conclusies en aanbevelingen hoofdstuk 10 Overige bevindingen

56. Bij een toekomstige wetswijziging moet tijdig aandacht zijn voor de implementatie daarvan en bij iedere afzonderlijke wetswijziging moet worden overwogen of overgangsrecht nodig is.
57. Doe een ICT-uitvoeringstoets bij wijzigingen van de wet.

Bijlagen



Bijlage 1 Samenstelling commissie en secretariaat

Samenstelling Evaluatiecommissie 2017

- Mevrouw drs. R.V.M. Jones-Bos, voorzitter
- De heer mr. Th.P.L. Bot
- De heer prof. mr. E.J. Dommering
- Mevrouw prof. dr. L.J. van den Herik
- De heer prof. dr. B.P.F. Jacobs
- De heer W. Nagtegaal, vice-admiraal b.d.
- De heer prof. mr. S.E. Zijlstra

V.l.n.r.: dhr. Nagtegaal, dhr. Jacobs, dhr. Zijlstra, mw. Jones-Bos, dhr. Bot, mw. van den Herik en dhr. Dommering.

Samenstelling secretariaat

- Mevrouw mr. R.S.I. Lawant, secretaris
- De heer K.M. van den Dool, MSc
- De heer mr.drs. R. Hendrix
- De heer mr. A. Hoeneveld
- Mevrouw M. den Hollander, MA
- De heer drs. F. van Kampen
- Mevrouw L.M. Saarloos, secretariële ondersteuning

Bijlage 2 Instellingsregeling

Regeling van 17 april 2020 tot instelling van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017 (Regeling instelling Evaluatiecommissie Wiv 2017)

De Minister-President, Minister van Algemene Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie, de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties;

Handelende in overeenstemming met het gevoelen van de ministerraad;

Gelet op artikel 6, eerste lid, van de Kaderwet adviescolleges en artikel 2 van de Wet vergoedingen adviescolleges en commissies;

Besluiten:

Artikel 1
Er is een Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017 (Evaluatiecommissie Wiv 2017), hierna te noemen de commissie.

Artikel 2
1. De commissie heeft tot taak de Wet op de inlichtingen- en veiligheidsdiensten 2017 te evalueren en naar aanleiding daarvan aan ons een rapport uit te brengen.
2. De commissie dient in haar evaluatieonderzoek in ieder geval aandacht te besteden aan de volgende vragen:
   a. heeft de wet datgene gebracht wat de wetgever daarmee voor ogen had (realisatie van de doelstellingen van de wet);
   b. is de wet in de praktijk een werkbaar instrument gebleken voor de taakuitvoering van de diensten;
   c. welke knel- en aandachtspunten zijn in de toepassingspraktijk van de wet te onderkennen.
3. Bijzondere aandacht dient voorts te worden geschonken aan de volgende aspecten:
   a. het integrale stelsel van toezicht, waarbij in ieder geval aandacht wordt geschonken aan:
      i. inrichting, functie en positie van de Toetsingscommissie Inzet Bevoegdheden (TIB), een en ander tegen de achtergrond van het vraagstuk van de ministeriële verantwoordelijkheid;
      ii. positionering van de klachtbehandeling bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de effectiviteit daarvan mede vanuit het burgerperspectief;
      iii. de rechtseenheidsvoorziening TIB - CTIVD;
      iv. de benoemingsprocedure voor de leden van TIB en CTIVD.

   b. de bevoegdheden van de diensten tot gegevensverwerking en de daarvoor geldende waarborgen, waarbij in ieder geval aandacht wordt geschonken aan:
      i. de toepassing en inpasbaarheid van nieuwe technieken binnen de wettelijk geregelde bevoegdheden (techniekonafhankelijkheid);
      ii. de toepassing van het gerichtheidscriterium bij bijzondere bevoegdheden;
      iii. het datareductiestelsel en de bewaartermijnen;
      iv. de duidelijkheid van in de wet gehanteerde terminologie.

   c. de bevoegdheden en waarborgen met betrekking tot internationale samenwerking van de diensten (zowel op vlak van gegevensverstrekking als ondersteuning).

Artikel 3

1. De commissie bestaat uit ten minste zes en ten hoogste zeven leden, waaronder de voorzitter.
2. Als voorzitter van de commissie wordt benoemd: mevrouw drs. R.V.M. Jones-Bos.
3. De overige leden worden bij ministerieel besluit benoemd.

Artikel 4

1. De voorzitter en de leden van de commissie, voor zover niet vallend onder de uitzondering van artikel 2, derde lid, van de Wet vergoedingen adviescolleges en commissies, ontvangen een vaste vergoeding per maand.
2. De voorzitter ontvangt voor de duur van het onderzoek een vaste vergoeding, gebaseerd op een arbeidsduurfactor van 40% en salarisschaal 18 trede 10, zoals overeengekomen in de laatstelijk afgesloten collectieve arbeidsovereenkomst voor ambtenaren die krachtens een arbeidsovereenkomst bij de Staat werkzaam zijn.
3. De overige leden ontvangen voor de duur van het onderzoek een vaste vergoeding, gebaseerd op een arbeidsduurfactor van 20% en salarisschaal 18, trede 10, zoals overeengekomen in de laatstelijk afgesloten collectieve arbeidsovereenkomst voor ambtenaren die krachtens een arbeidsovereenkomst met de Staat werkzaam zijn.

Artikel 5

Indien de commissie ter ondersteuning van haar onderzoek externe deskundigen inschakelt, blijft die ondersteuning beperkt tot werkzaamheden, waarbij de kennisneming van staatsgeheim gerubriceerde informatie is uitgesloten.

Artikel 6

1. De commissie brengt voor een door de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie, na overleg met de voorzitter van de commissie, gezamenlijk te bepalen datum, aan ons een rapport uit. Van de datum wordt mededeling gedaan in de Staatscourant.
2. Het rapport bevat in ieder geval:
   a. de uitwerking van de onderzoeksvragen;
   b. de verantwoording van de gehanteerde onderzoeksmethoden en de gebruikte informatie;
   c. de beschrijving en analyse van de bevindingen van het onderzoek;
   d. de conclusies die uit het onderzoek worden getrokken;
   e. eventuele (gemotiveerde) voorstellen voor wetswijzigingen.
3. Na het uitbrengen van het rapport is de commissie opgeheven.

Artikel 7

De commissie draagt zo spoedig mogelijk na de beëindiging van haar werkzaamheden of, zo de omstandigheden daartoe aanleiding geven, zoveel eerder, de bescheiden betreffende die werkzaamheden over aan het archief van de Algemene Inlichtingen- en Veiligheidsdienst. Bescheiden die zijn verkregen van een andere instantie dan de Algemene inlichtingen- en Veiligheidsdienst worden, onder aantekening van welke bescheiden het betreft, geretourneerd aan die instantie.

Artikel 8

Deze regeling treedt in werking met ingang van 1 mei 2020 en vervalt een maand na de datum, bedoeld in artikel 6, eerste lid.

Artikel 9
Deze regeling wordt aangehaald als: Regeling instelling Evaluatiecommissie Wiv 2017.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Minister-President,
Minister van Algemene Zaken,
M. Rutte

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

TOELICHTING

Op 1 mei 2018 is de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) volledig in werking getreden. Deze wet vervangt de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002), die sinds 29 mei 2002 het wettelijk kader vormde voor de activiteiten van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze wet is in 2013 door de Evaluatiecommissie Wiv 2002 (Commissie Dessens) geëvalueerd en in december 2013 heeft de commissie haar evaluatierapport uitgebracht. Dit rapport en het daarover uitgebrachte kabinetsstandpunt hebben geleid tot een wetstraject met als eindresultaat de Wiv 2017. Evenals de Wiv 2002 biedt de Wiv 2017 een vrijwel uitputtende regeling voor de activiteiten van de AIVD en de MIVD.

In het regeerakkoord van het Kabinet-Rutte III – Vertrouwen in de toekomst – is afgesproken dat de nieuwe wet uiterlijk twee jaar na inwerkingtreding zal worden geëvalueerd. Ter zake wordt het volgende opgemerkt: 'Er is een nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Informatie-uitwisseling beperkt zich tot partnerdiensten, tenzij de minister toestemming geeft voor uitwisseling met niet-partnerdiensten. Van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of het buitenland ('sleepnet') kan, mag en zal geen sprake zijn. Daarom zal het kabinet bij de uitvoering strikt de hand houden aan de extra waarborgen in deze wet. De evaluatie, waarbij aan dit punt bijzonder belang zal worden toegekend, wordt vervroegd uitgevoerd door een onafhankelijke commissie en zal in ieder geval niet later beginnen dan twee jaar na inwerkingtreding. Indien de evaluatie hiertoe aanleiding geeft, zal het kabinet voorstellen additionele waarborgen in de wet op te nemen en het toezicht hierop te versterken.'

Ter uitvoering van deze afspraak voorziet onderhavig besluit in de instelling van een onafhankelijke evaluatiecommissie op grond van artikel 6, eerste lid, van de Kaderwet adviescolleges (hierna: kaderwet). Een onafhankelijke commissie is wenselijk, aangezien het van belang is dat de verschillende aan de orde zijnde kwesties op een onbevooroordeelde manier worden onderzocht. Daarbij speelt tevens een rol dat – zoals de praktijk tot op heden laat zien – er verschillende partijen bij de toepassing van de wet zijn betrokken, met hun eigen belangen en waarbij soms sprake is van divergerende opvattingen over de interpretatie van de wet. De commissie bestaat uit ten minste zes en ten hoogste zeven leden, waaronder de voorzitter. De commissie wordt zodanig samengesteld dat de commissie als geheel deskundigheid en affiniteit bezit met betrekking tot wetsevaluatie, operationele kennis van de werkzaamheden van inlichtingen- en veiligheidsdiensten (civiel en militair, waaronder operaties), gegevensverwerking (vgl. Big Data, GDA, techniek e.d.) en mensenrechten (m.n. privacy- en dataprotectierecht).

Als voorzitter van de commissie wordt mevrouw R.V.M. Jones-Bos benoemd. De overige leden zullen bij afzonderlijk ministerieel besluit worden benoemd, zodra het naar hen ingestelde veiligheidsonderzoek is afgerond en zij een verklaring van geen bezwaar hebben ontvangen. De functie van voorzitter en lid van de commissie alsmede lid van het secretariaat zijn namelijk in verband met het feit dat men in het kader van het onderzoek kennis zal nemen van staatsgeheim gerubriceerde gegevens als vertrouwensfunctie aangewezen.

De voorzitter en de overige leden van de evaluatiecommissie krijgen een vaste vergoeding per maand voor hun werkzaamheden met inachtneming van hetgeen bij en krachtens de Wet vergoedingen adviescolleges en commissie is bepaald. Een vaste vergoeding is hier aangewezen, aangezien de werkzaamheden van de voorzitter en leden van de commissie niet beperkt zijn tot enkele vergaderingen. Artikel 4 van de regeling voorziet daarin.

De commissie wordt in haar werkzaamheden bijgestaan door een ambtelijk secretariaat onder leiding van een secretaris. Voor de werkzaamheden voor de commissie zijn de secretaris en de overige medewerkers van het secretariaat voor de duur van het onderzoek uitsluitend verantwoording verschuldigd aan de commissie (artikel 15 Kaderwet adviescolleges).

De taak van de commissie is omschreven in artikel 2 van de regeling. De commissie heeft tot taak de wet te evalueren en naar aanleiding daarvan een rapport uit te brengen. Het betreft hier een wetsevaluatie en derhalve geen evaluatie van het functioneren van de diensten. Voor dit laatste voorziet artikel 167, tweede lid, van de wet in een opdracht aan de voor de diensten verantwoordelijke ministers om vijf jaar na inwerkingtreding van de wet daarover een verslag aan de Staten-Generaal uit te brengen. In de brief aan de Tweede Kamer van 12 november 2019 (Kamerstukken II 2019/2020, 34 588, nr. 84) zijn de in ieder geval te onderzoeken kwesties meer in detail beschreven. Deze kwesties moeten worden geacht te zijn begrepen in de meer algemeen geformuleerde onderzoeksvragen van artikel 2.

Voor een goede uitoefening van de aan de commissie opgedragen taak is het van belang dat zij de beschikking kan krijgen over alle relevante, waaronder staatsgeheime, gegevens. Tevens moet zij toegang (kunnen) krijgen tot personen die voor haar onderzoek relevante informatie kunnen verstrekken. In het ten behoeve van het onderzoek opgesteld informatieprotocol verplichten de betrokken ministers zich tot alle medewerking op dit vlak. In het protocol worden voorts onder meer eisen geformuleerd waar het gaat om de omgang met staatsgeheime gegevens door de commissie. Voorts wordt een beveiligde werkomgeving aan de commissie ter beschikking gesteld, waartoe uitsluitend de commissie en de leden van het ambtelijk secretariaat toegang hebben. De commissie heeft op grond van artikel 19, tweede lid, van de kaderwet de mogelijkheid zich te doen laten bijstaan door externe deskundigen, zij het dat de inschakeling beperkt blijft tot werkzaamheden, waarbij de kennisneming van staatsgeheime informatie is uitgesloten (artikel 5).

Het eindrapport van de commissie, dat integraal openbaar zal zijn en geen geheim onderdeel zal bevatten, dient voor een door de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie, na overleg met de voorzitter, gezamenlijk te bepalen datum aan de ministers te worden aangeboden. Voor deze constructie is thans gekozen, omdat – hoewel de commissie gewoon per 1 mei wordt ingesteld – nog onduidelijk is of ze haar werkzaamheden in de periode daarna als gevolg van de maatregelen die zijn getroffen in het kader van de bestrijding van het coronavirus ten volle kan ontplooien of dat die aan beperkingen onderhevig zijn. Afhankelijk van die ontwikkelingen kan op enig moment een datum voor het opleveren van het rapport worden vastgesteld. In artikel 6 van de regeling is nader bepaald waaraan het rapport aandacht dient te besteden. Aan de commissie komt de bevoegdheid toe om eventueel (gemotiveerde) voorstellen tot wijziging van de Wiv 2017 in haar rapport op te nemen. Na het uitbrengen van haar rapport is de commissie van rechtswege opgeheven.

In artikel 7 van de regeling is ten slotte een voorziening opgenomen waar het gaat om de bescheiden betreffende de werkzaamheden van de commissie.

De Minister-President,
Minister van Algemene Zaken,
M. Rutte

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops

Besluit van 24 april 2020 tot benoeming van de leden van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017

De Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie, mede namens de Minister-President, Minister van Algemene Zaken en de Minister van Justitie en Veiligheid;

Handelende in overeenstemming met het gevoelen van de ministerraad;

Gelet op artikel 3, derde lid, van de Regeling instelling Evaluatiecommissie Wiv 2017;

Besluiten:

Artikel 1
Tot leden van de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017 worden benoemd:

- mr. Th.P.L. Bot;
- prof. mr. E.J. Dommering;
- prof. dr. L.J. van den Herik;
- prof. dr. B.P.F. Jacobs;
- viceadmiraal b.d. W. Nagtegaal;
- prof. mr. S.E. Zijlstra.

Artikel 2
Dit besluit treedt in werking met ingang van 1 mei 2020 en vervalt met ingang van het in artikel 6, eerste lid, van de Regeling instelling Evaluatiecommissie Wiv 2017 bedoelde tijdstip.

Dit besluit zal met de toelichting in de Staatscourant worden geplaatst en in afschrift worden gezonden aan betrokkenen.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten

TOELICHTING

Bij regeling van 17 april 2020 is de Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: commissie) per 1 mei 2020 ingesteld. Tevens is daarbij mevrouw R.V.M. (Renee) Jones-Bos als voorzitter van de commissie benoemd. In artikel 3, derde lid, van de regeling is bepaald dat de overige leden van de commissie bij ministerieel besluit worden benoemd. Onderhavig besluit voorziet daarin. De vergoeding voor de werkzaamheden van de leden voor de commissie is geregeld in artikel 4 van de regeling.

Het benoemingsbesluit treedt gelijktijdig met de regeling in werking, te weten per 1 mei 2020, en zal eveneens gelijktijdig met de regeling komen te vervallen, namelijk op het ingevolge artikel 6, eerste lid, van de regeling vast te stellen tijdstip.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten

Bijlage 3 Afkortingenlijst

ABRvS	Afdeling bestuursrechtspraak van de Raad van State
AI	*Artificial Intelligence*
AIV	Adviesraad voor Internationale Vraagstukken
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMvB	Algemene maatregel van bestuur
API	*Advance Passenger Information*
appl. nr.	*Application number* (van een klacht bij het EHRM)
AR	Algemene Rekenkamer
AVG	Algemene Verordening Gegevensbescherming
Awb	Algemene wet bestuursrecht
BRP	Basisregistratie Personen
BVerfG	*Bundesverfassungsgericht*, het Duitse Constitutionele Hof
BZ	Buitenlandse Zaken
BZK	Binnenlandse Zaken en Koninkrijksrelaties
CAVV	Commissie van Advies inzake Volkenrechtelijke Vraagstukken
CCIII	Wet computercriminaliteit III
CIVD	Commissie voor de Inlichtingen- en Veiligheidsdiensten (Tweede Kamer)
CT Infobox	Contra Terrorisme Infobox
CTIVD	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
CZW	Constitutionele Zaken en Wetgeving (ministerie van BZK)
EG	Europese Gemeenschap
EHRM	Europese Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Het Europese Verdrag voor de Rechten van de Mens en de fundamentele vrijheden
GCHQ	*Government Communications Headquarters*
GBVS	Geïntegreerde Buitenland- en Veiligheidsstrategie
GCHQ	Government Communications Headquarters
GDA	Geautomatiseerde Data Analyse
GRU (GROe)	*Glavnoje Razvedyvatelnoje Oepravlenije*, een Russische militaire inlichtingendienst.
HF	*High Frequency*
HUMINT	*Human intelligence*
HvJEU	Hof van Justitie van de Europese Unie
HR	Hoge Raad der Nederlanden
ICT	Informatie- en communicatietechnologie
IED	*Improvised Explosive Devices*
IMEI	*International Mobile Equipment Identity*
IMSI	*International Mobile Subscriber Identity*
INF-verdrag	*Intermediate-Range Nuclear Forces-verdrag*
IP	Internet Protocol
IPT	*Investigatory Powers Tribunal*
Kmar	Koninklijke Marechaussee
KvK	Kamer van Koophandel
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
MvT	memorie van toelichting
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NGO	niet gouvernementele organisatie
NSA	*National Security Agency*

NVS	Nationale Veiligheidsstrategie
OOG	Onderzoeks Opdracht Gericht(e)
OAS	Organisatie van Amerikaanse Staten
OPCW	*Organisation for the Prohibition of Chemical Weapons*
Para.	Paragraaf
PIA	*Privacy Impact Assesment*
RDW	Rijksdienst voor het Wegverkeer (Sinds 1996: RDW)
RFI	*Request for Information*
RIPA	*Regulation of Investigatory Powers Act 2000* (Verenigd Koninkrijk)
r.o.	rechtsoverweging
RvS	Raad van State
SCC	Standard Contractual Clauses
SHF	Super High Frequency
Sigint	Signals Intelligence
Stb.	Staatsblad
Stcrt.	Staatscourant
SyRi	Systeem Risico Indicatie
TIB	Toetsingscommissie Inzet Bevoegdheden
URL	*Uniform Resource Locator*
VN	Verenigde Naties
VwEU	Verdrag inzake de werking van de Europese Unie
VPN	*Virtual Private Network*
Wbp	Wet bescherming persoonsgegevens
Wiv 2017	Wet op de inlichtingen- en veiligheidsdiensten 2017
WRR	Wetenschappelijke Raad voor het Regeringsbeleid

Bijlage 4 Begrippenlijst

Algemene bevoegdheden	Bevoegdheden die voor alle taken van de diensten mogen worden ingezet. Bijvoorbeeld: het verzamelen van gegevens door een informant te raadplegen (artikel 39). *Zie ook 'bijzondere bevoegdheden'.*
Betekenis	Gegevens die als relevant zijn beoordeeld komen in het 'betekenisregime'. Dit houdt in dat de gegevens worden verwijderd als deze, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren (artikel 20). Hierbij is geen specifieke termijn gesteld waarbinnen de betekenis moet worden getoetst. *Zie ook 'relevantie'.*
Bijschrijven	Het toevoegen van technische kenmerken, zoals een IP-adres of een telefoonnummer, aan een eerdere goedgekeurde lastaanvraag, als het geautomatiseerde werk dat hoort bij het nieuwe technische kenmerk dient ter vervanging of aanvulling op het eerdere geautomatiseerde werk waar de last op ziet.
Bijzondere bevoegdheden	Bijzondere bevoegdheden hebben over het algemeen een meer ingrijpend karakter en leiden tot een zwaardere inbreuk op het recht op privacy ten opzichte van algemene bevoegdheden. Deze bevoegdheden mogen niet voor alle taken van de diensten worden ingezet, bijvoorbeeld niet voor het verrichten van veiligheidsonderzoeken en het opstellen van dreigings- en risicoanalyses. Een bijzondere bevoegdheid is bijvoorbeeld het observeren en volgen van een persoon (artikel 40) of de hackbevoegdheid (artikel 45). *Zie ook 'algemene bevoegdheden'.*
Bulkdata	Een omvangrijke verzameling van gegevens waarvan het merendeel betrekking heeft op personen en/of organisaties die niet in onderzoek zijn van de diensten en dit ook nooit zullen worden. Het begrip bulkdata is daarmee niet gerelateerd aan de wijze van verwerving, maar aan de aard en de omvang van de gegevens zelf. Er wordt ook wel gesproken van 'bulkdatasets', waarmee specifieke, nader omlijnde sets aan bulkdata wordt bedoeld.
Cumulatieve naslag	Het automatisch doorzoeken op basis van een startkenmerk. Hiermee kan worden opgezocht welke andere kenmerken in communicatie zijn betrokken of welke andere kenmerken horen bij het startkenmerk.
Derde	Een specifieke invulling van het begrip 'non-target'. Een derde stelt de diensten in staat om toegang te krijgen tot het geautomatiseerde werk van het uiteindelijke target. Via een derde kan worden doorgestapt naar het target, of door het binnendringen van een derde kunnen gegevens worden verworven die noodzakelijk zijn om vervolgens bij het target binnen te dringen. *Zie ook 'non-target'.*
Dynamisch toezicht	Toezicht over de verschillende fases van een operatie waarin de focus van het toezicht kan verschuiven. Dit kan nadat een operatie is afgelopen (ex-post), maar ook gedurende een operatie (ex-nunc).
Enkelvoudige naslag	Een enkelvoudige zoekvraag op basis van een kenmerk, zoals het zoeken van een naam bij een kenteken, een IMEI bij een IMSI of een geolocatie bij een IP-adres.

Filtering	Filters worden gebruikt in het kader van OOG-interceptie om de geïntercepteerde gegevens te reduceren tot gegevens die voor verder onderzoek relevant kunnen zijn.
Geautomatiseerde data analyse (GDA)	GDA is een term die in de Wiv wordt gebruikt voor verschillende vormen van gegevensverwerking waarbij data-analyse geautomatiseerd plaatsvindt. Over de precieze invulling van dit begrip is discussie. Zie voor meer toelichting hoofdstuk 5.
Gedragbulkdata	Bulkdata die niet enkel uit identificerende kenmerken, maar óók uit gedragsgegevens bestaat. Met gedragsgegevens wordt gedoeld op meer tijdsgebonden informatie over gebeurtenissen die inzicht geven in bijvoorbeeld gedragingen van personen. Voorbeelden hiervan zijn passagiersgegevens of telefoniegegevens. *Zie ook 'register-bulkdata'.*
Gerichtheid	De diensten doen wat redelijkerwijze in hun vermogen ligt om reeds bij verwerving van gegevens de niet voor het onderzoek noodzakelijke gegevens tot een minimum te beperken en motiveren dit in hun aanvraag tot de inzet van een bevoegdheid, door zo goed als mogelijk de te vergaren gegevens af te bakenen: geografisch, naar tijdstip, naar soort data/type verkeer, naar object/target, naar gedraging of anderszins.
Gerichtheidsvereiste	Het vereiste dat de diensten doen wat redelijkerwijze in hun vermogen ligt om reeds bij verwerving van gegevens de niet voor het onderzoek noodzakelijke gegevens tot een minimum te beperken en dit te motiveren in hun aanvraag tot de inzet van een bevoegdheid. Dit gebeurt door de gegevens zoveel mogelijk af te bakenen; geografisch, naar tijdstip, naar soort data/type verkeer, naar object/target of naar gedraging.
Meervoudige naslag	Een samengestelde zoekvraag op basis van één of meerdere kenmerken en eventuele andere elementen, bijvoorbeeld locatie of tijd.
Metadata	Die gegevens van telecommunicatie, welke niet de inhoud van de telecommunicatie betreffen.
Ministeriële toestemming	Ministeriële toestemming betekent in de praktijk dat een toestemmingsaanvraag voor de inzet van een bevoegdheid al door diverse personen is gecontroleerd voordat de betrokken minister ernaar kijkt.
Non-target	Een begrip die gebruikt wordt bij de inzet van een bevoegdheid voor een partij die geen target van de diensten is. *Zie ook 'derde'.*
Ongeëvalueerde gegevens	Gegevens die onvoldoende zijn onderzocht door de AIVD of de MIVD waardoor niet genoeg informatie aanwezig is over de aard en feitelijke inhoud van de gegevens om de noodzakelijkheid, de behoorlijkheid en de zorgvuldigheid van de gegevensverstrekking adequaat te kunnen beoordelen. Over de precieze invulling van dit begrip is discussie. Zie hiervoor §4.4.4.

Register-bulkdata	Bulkdata die bestaat uit identificerende kenmerken. Het gaat hierbij om feitelijke, relatief stabiele kenmerken die beschrijven wie of wat je bent. Hierbij kan gedacht worden aan postcodes, geboortedata en paspoortnummers. Deze kenmerken worden ook wel 'attributen' genoemd. *Zie ook 'gedrag-bulkdata'.*
Relevantie	Gegevens verkregen uit bijzondere bevoegdheden moeten zo spoedig mogelijk worden beoordeeld op hun relevantie (artikel 27). Het gaat hierbij om relevantie voor het onderzoek waarvoor de gegevens initieel zijn verworven, óf voor enig ander lopend onderzoek van de diensten. Gegevens die als niet-relevant worden beoordeeld moeten worden vernietigd. Gegevens die wél relevant zijn beoordeeld komen in het zogenaamde 'betekenisregime'. Over de precieze invulling van dit begrip is discussie. Zie hiervoor §4.4.4. *Zie ook 'betekenis'.*
Search	De bevoegdheid die is toegekend aan een beperkte groep functionarissen om geïntercepteerde bulkdata te onderzoeken. Dit kan bedoeld zijn om de interceptie te optimaliseren. In dat geval spreekt men van 'search gericht op interceptie'. Als search is bedoeld om de selectie te optimaliseren, door onder meer potentiële selectiecriteria te verifiëren en nieuwe potentiële targets te identificeren, spreekt men van 'search gericht op selectie'.
Selectie	Selectie is de bijzondere bevoegdheid tot het selecteren van gegevens verkregen door OOG-interceptie. Selectie vindt plaats met het oogmerk om van de inhoud van de geselecteerde gegevens kennis te kunnen nemen, zoals een telefoongesprek. Dit gebeurt aan de hand van selectiecriteria. *Zie ook 'relevantie'.*
Verwerking	Alle handelingen die volgen op de verwerving/verzameling van gegevens. Zie voor meer toelichting het kader in §3.3.1. *Zie ook 'verwerving'.*
Verwerving	Het verkrijgen van gegevens. Ook wel 'verzameling' van gegevens. *Zie ook 'verwerking'.*
Volle toets	Een rechtmatigheidstoets (voor de inzet van bijzondere bevoegdheden) op proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid. Binnen deze rechtmatigheidstoets geldt voor de TIB geen beperking en hieraan kan deze op eigen wijze invulling geven. De TIB krijgt hetzelfde feitencomplex als de minister voorgelegd en kan de in dat kader beoogde bevoegheidsuitoefening in zijn volle omvang aan een rechtmatigheidstoets onderwerpen.
Zerodays	Een onbekende kwetsbaarheid in een geautomatiseerd werk die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen. Van deze kwetsbaarheid kan worden verondersteld dat deze niet bekend is bij de producent of leverancier.

Bijlage 5 Jurisprudentieoverzicht

Europees Hof voor de Rechten van de Mens (EHRM)

- EHRM 6 september 1978, (*Klass en anderen tegen Duitsland),* appl. 5029/71 (1979-80).
- EHRM 29 juni 2006, ECLI:CE:ECHR:2006:0629DEC005493400, (*Weber en Saravia tegen Duitsland),* appl. 54934/00.
- EHRM 1 juli 2008, ECLI:CE:ECHR:2008:0701JUD005824300, (*Liberty tegen Verenigd Koninkrijk)*, appl. 58243/00.
- EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204, *(S and Marper tegen Verenigd Koninkrijk)*, appl. 30562/04 en 30566/04.
- EHRM 18 mei 2010, ECLI:CE:ECHR:2010:0518JUD002683905, (*Kennedy tegen Verenigd Koninkrijk)*, appl. 26839/05.
- EHRM 4 december 2015, ECLI:CE:ECHR:2015:1204JUDO04714306, (*Roman Zakharov tegen Rusland*) appl. 47143/06.
- EHRM 6 juni 2016, ECHR:2016:0112JUD003713814, (*Szabó en Vissy tegen Hongarije),* appl. 37138/14.
- EHRM 19 juni 2018, ECLI:CE:ECHR:2018:0619JUD003525208, (*Centrum för Rättvisa tegen Zweden*) appl. 32352/08.
- EHRM 13 september 2018, ECLI:CE:ECHR:2018:0913JUDO05817013 (*Big Brother Watch tegen Verenigd Koninkrijk),* appl. 58170/13, 62322/14 en 24690/15.
- EHRM 30 januari 2020, ECLI:CE:ECHR:2020:0130JUD005000112, (*Breyer tegen Duitsland*) appl. 50001/12.

Hof van Justitie van de Europese Unie (HvJEU)

- HvJEU 8 april 2014, ECLI:EU:C:2014:238, (*Digital Rights Ireland*), C-293/12 en C-549/12.
- HvJEU 6 oktober 2015, ECLI:EU:C:2015:650, (*Schrems*), C-362/14.
- HvJEU 19 oktober 2016 ECLI:EU:C:2016:779 (*Breyer*), C-582/14.
- HvJEU 21 december 2016, ECLI:EU:C:2016:970, (*Tele2 Sverige*), C-203/15 en C-698/15.
- HvJEU 2 oktober 2018, ECLI:EU:C:2018:788, (*Ministerio Fiscal),* C-207/16.
- HvJEU 29 juli 2019, ECLI:EU:C:2019:629, (*Facebook ID,* C-40/17.
- HvJEU 16 juli 2020, Schrems II, ECLI:EU:C:2020:559, (*Schrems II), C-311/18.*
- HvJEU 6 oktober 2020, ECLI:EU:C:2020:790, (*Privacy International*), C-623/17.
- HvJEU 6 oktober 2020, ECLI:EU:C:2020:929, *(Quadrature du Net and others/Ordre des barreaux francophones et germanophones and others*), C-511/18, 512/18 en C-520/18.

Hoge Raad

- HR 6 januari 1998, ECLI:NL:HR:1998:AA9342, (*Pikmeer II*).

Rechtbank Den Haag

- Rechtbank Den Haag 5 februari 2020, ECLI:NL:RBDHA:2020:865, (*SyRI).*

BundesVerfassungsgericht

- BVerfG 15 december 1983, NJW 1984, *Volkszählungsurteil*
- BVerfG 20 mei 2020, ECLI:DE:BVerfG:2020:rs20200519.1bvr283517, 1 BvR 2835/17.