Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Evaluatiecommissie Wiv 2017

Uw kenmerk

Ons kenmerk
2020/0096

Datum
11 augustus 2020

Betreft
Reactie wetsevaluatie

Geachte mevrouw Jones-Bos,

Op 10 juli 2020 heeft de afdeling toezicht van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) een gesprek met uw commissie gevoerd over een aantal onderwerpen met betrekking tot de evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Naar aanleiding van onze presentatie heeft uw commissie vragen gesteld, waarop een levendige discussie volgde en onze visie op punten is aangescherpt. Wij danken u voor de mogelijkheid dit gesprek met uw commissie aan te gaan. Uw commissie voert nog een separaat gesprek met de afdeling klacht. Ook is reeds een aantal verdiepende sessies met de afdeling toezicht gepland.

Met uw commissie is afgesproken dat wij onze visie op schriftelijke wijze nader toelichten. Mochten nieuwe ontwikkelingen of verdiepingssessies daartoe aanleiding geven, dan zal de CTIVD deze reactie nader aanvullen.

Deze toelichting beperkt zich tot de onderwerpen die ook in de presentatie aan bod zijn gekomen, te weten (1) het normatief kader, (2) toezicht, (3) bulkdatasets, (4) geautomatiseerde data-analyse en (5) (inter)nationale samenwerking. De brief sluit af met een overzicht van de kernpunten.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

## 1 Achtergrond

De visie van de CTIVD kan worden geplaatst tegen de volgende achtergrond.

De CTIVD bewaakt de juiste balans tussen het belang van bescherming van de nationale veiligheid én dat van de fundamentele rechten van de burger. Sinds 2002 (met de inwerkingtreding van de Wiv 2002) treedt de CTIVD op als onafhankelijke toezichthouder op de rechtmatigheid van het hele spectrum van activiteiten van de AIVD en de MIVD, zoals gereguleerd in de Wiv 2017 en de Wet veiligheidsonderzoeken (Wvo).

Sinds de totstandkoming van de Wiv 2017 hebben zich diverse belangrijke nieuwe ontwikkelingen op het terrein van gegevensverwerking in het kader van nationale veiligheid en de inrichting van een effectief (bindend) toezichtstelsel voorgedaan. Deze voortschrijdende inzichten nopen tot aanpassing van de Wiv 2017. Het gaat met name om de ontwikkeling in de uitgebreide jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie van de Europese Unie (HvJ EU) over waarborgen en de rol en bevoegdheden van toezicht in relatie tot gegevensverwerking.[1]

Deze jurisprudentie met voortschrijdende inzichten heeft zich onder meer vertaald in een wijzigingsprotocol tot aanpassing van verdrag 108 tot bescherming van personen met betrekking tot (geautomatiseerde) verwerking van persoonsgegevens van de Raad van Europa.[2] De nieuwe versie, ook wel 'Conventie 108+' genoemd, is het eerste Europese instrument dat (naast de algemene context van het Europese Verdrag voor de Rechten van de Mens (EVRM) en het EU-Grondrechtenhandvest) expliciet betrekking heeft op gegevensverwerking in het kader van de nationale veiligheid en ingaat op de rechtsbescherming van burgers, de inrichting en bevoegdheden van toezicht, de internationale uitwisseling van gegevens en samenwerking tussen toezichthouders. Nederland heeft dit verdrag reeds ondertekend en is nu het ratificatieproces gestart.

Conventie 108+ geeft slechts beperkte mogelijkheden om in het belang van de nationale veiligheid uitzonderingen te maken op onder meer (bindende) vergaande bevoegdheden van toezichthouders op de naleving van het verdrag. Bovendien zijn uitzonderingen alleen mogelijk "*to the extent that it constitutes a necessary and proportionate measure in a democratic society*". Uitzonderingen mogen daarbij geen afbreuk doen aan het algemene beginsel van onafhankelijk en effectief toezicht.[3] Deze uitgangspunten vragen om een expliciete motivering van zowel de bestaande wet als eventuele daarop te maken wijzigingen wanneer uitzonderingen noodzakelijk en proportioneel zijn. Hier ligt dus een nieuw vertrekpunt voor wat

---

[1] Zie, met name, EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije*), EHRM 19 juni 2018, nr. 35352/08, ECLI:CE:ECHR:2018:0913JUD005817013 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24690/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. Het Verenigd Koninkrijk*) (beide zaken in behandeling bij de Grote Kamer sinds februari 2019), HvJ EU 21 december 2016, C-203/15 en C698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen en Secretary of State for the Home Department t. Tom Watson e.a.*), HvJ EU 16 juli 2020, ECLI:EU:C:2020:559 (*Schrems II*).

[2] Sinds oktober 2018 is dit wijzigingsprotocol opengesteld voor ondertekening en ratificatie. Het gewijzigde verdrag (Conventie 108+) zal in werking treden nadat alle verdragspartijen (55) het wijzigingsprotocol hebben geratificeerd, dan wel vijf na openstelling (oktober 2023) indien op dat moment 38 verdragspartijen hebben geratificeerd.

[3] Zie Artikel 11 lid 3 van het wijzigingsprotocol: "*This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party*".

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

betreft de juridische inkadering van de inrichting en bevoegdheden van toezicht op de inlichtingen- en veiligheidsdiensten in Nederland. Overigens vormen de internationale jurisprudentie en verdragen een ondergrens waar het gaat om het bieden van waarborgen. Het staat Nederland vrij om een hoger beschermingsniveau te bieden.

De CTIVD heeft inmiddels ruime ervaring met de Wiv 2017. Zij heeft, mede op verzoek van de Tweede Kamer, de implementatie van de nieuwe Wiv kritisch gemonitord en vastgelegd in voortgangsrapportages (de vierde en laatste voortgangsrapportage wordt op 8 september 2020 gepubliceerd). De voortgangsrapportages richten zich op een aantal belangwekkende implementatievraagstukken. Tezamen met de ervaringen van de CTIVD met de toepassingspraktijk van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) (o.a. neergelegd in de diverse toezichtsrapporten), maken deze voortgangsrapportages duidelijk dat de huidige wet aanpassing behoeft. Hierna zal in de afzonderlijke paragrafen op een aantal elementen expliciet worden ingegaan.

Op basis van geschetste juridische ontwikkelingen en de opgedane ervaringen van de CTIVD, zijn de volgende hoofdlijnen in ieder geval duidelijk:

- De wet kent op diverse onderdelen een te hoog detailniveau dat niet aansluit bij de (gewenste) dagelijkse praktijk van zowel de diensten als het toezicht. Inzichten bij de totstandkoming van de Wiv 2017 blijken nu al achterhaald en onderstrepen daarmee de noodzaak van een robuust normatief kader (zie nader paragraaf 2).
- De Wiv 2017 bevat een gefragmenteerd toezichtstelsel, bestaande uit bindende *ex ante* toetsing van de inzet van bepaalde bijzondere bevoegdheden door de Toetsingscommissie Inzet Bevoegdheden (TIB), rechterlijke toestemming voor de inzet van bijzondere bevoegdheden tegen advocaten en journalisten, *ex nunc* en *ex post* toezicht door de CTIVD op de naleving van de gehele Wiv 2017, waaronder de inzet van algemene bevoegdheden, internationale gegevensverstrekking en de rechtmatigheid en kwaliteit van gegevensverwerking door de diensten, en tot slot bindende klachtbehandeling door de CTIVD. Deze fragmentatie sluit niet aan bij de praktijk van gegevensverwerking door de diensten die in de kern bestaat uit het nader verwerken/analyseren van gegevensbestanden (met als bijzonderheid de toenemende importantie van bulkdatasets). Deze gegevensverwerking is een continue dynamisch en complex proces. Bindende *ex ante* toetsing/toestemming bestrijkt slechts een beperkt deel van dat proces, namelijk de inzet van bepaalde bijzondere bevoegdheden, en heeft geen zicht op de verdere verwerking van de gegevens. Bovendien vereist toezicht op gegevensverwerking andere vaardigheden en methoden, zoals systeemtoezicht,[4] steekproeven en diepteonderzoeken, en grondige kennis van de operaties van de diensten. In het bijzonder door het ontbreken van bindende bevoegdheden in het toezicht kan juist daar waar de inbreuk op de rechten van burgers het grootst is – het proces van gegevensverwerking – de rechtmatigheid niet voldoende worden

[4] Bij systeemtoezicht richt de toezichthouder zich vooral op systemen en processen, waarbij de feitelijke output (van de organisatie) niet langer het primaire object van controle is. Anders gezegd, systeemtoezicht is al het toezicht waarbij de opzet, reikwijdte en werking van zowel systemen als processen wordt vastgesteld. De toezichthouder zal zich bij systeemtoezicht dus een oordeel over de kwaliteit van het systeem (o.a. management-, zorg- en/of interne controlesysteem) moeten vormen, omdat deze de waarde van de beschikbare informatie bepaalt. De organisatie moet laten zien dat de interne controlesystemen, die ervoor moeten zorgen dat wettelijke eisen worden nageleefd, op orde zijn: van beleid tot uitvoering, verantwoording en evaluatie, niet alleen op papier, maar ook in de praktijk. De output van de interne controlesystemen levert een belangrijke bijdrage aan de prioritering van het toezicht en het uitvoeren van steekproeven.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

gewaarborgd. Het bindende karakter van de oordelen van de afdeling klachtbehandeling van de CTIVD is eveneens nodig, maar vormt als zodanig geen substituut voor of invulling van effectief en geïntegreerd (integraal) toezicht. Hetzelfde geldt voor rechtseenheidsoverleg. De zich in de afgelopen jaren ontwikkelde jurisprudentie van het EHRM en het Hof van Justitie van de Europese Unie (HvJ EU) vormt een bevestiging hiervan (zie nader paragraaf 3).

## 2 Normatief kader

De Wiv 2017 vormt de wettelijke grondslag voor de bevoegdheden van de AIVD en de MIVD ter uitvoering van hun taken. De verwerking van gegevens betreft daarbij de kerntaak, waarbij de gegevensverwerking telkens plaatsvindt in het belang van de nationale veiligheid. Het normatief kader dient zoveel als mogelijk techniekonafhankelijk te zijn om voldoende armslag te bieden hun taken te kunnen uitvoeren. Tegelijkertijd dienen bevoegdheden die een (ernstige) inbreuk op de fundamentele rechten van burgers maken voldoende duidelijk te worden genormeerd en dient de wet voldoende waarborgen te bevatten ter bescherming van de in het geding zijnde fundamentele rechten.

***Problematiek in de huidige wet***

De CTIVD is in haar toezichtspraktijk tegen twee belangrijke kwesties aangelopen waar de Wiv 2017 op dit punt niet in balans is. Ten eerste betreft dit de zogenoemde bulkdatasets. Het toezichtsrapport over door derden aangeboden bulkdatasets op internet[5] en het nog te verschijnen toezichtsrapport over de verzameling en verdere verwerking van passagiersgegevens[6] laten zien dat ook met de inzet van algemene bevoegdheden, in dit geval de informantenbevoegdheid, ernstige inbreuken op de fundamentele rechten van burgers plaatsvinden.

Een belangrijke consequentie van het huidige onderscheid tussen algemene en bijzondere bevoegdheden is dat bijzondere bevoegdheden aan hogere toestemmingsvereisten onderhevig zijn en een onderzoeksplicht op relevantie van de daarmee verzamelde gegevens bestaat (binnen één jaar met de mogelijkheid van verlenging van zes maanden). Dat laatste vereiste is overigens gezien de aard en omvang van bulkdatasets niet mogelijk, wat de diensten ertoe heeft gebracht bepaalde bulkdatasets na afloop van de bewaartermijn als geheel of grotendeels relevant te verklaren om de sets zo langer te kunnen bewaren met het oog op het belang ervan voor de nationale veiligheid. Deze wijze van relevantiebeoordeling is echter onrechtmatig en holt de wettelijke waarborgen uit. De CTIVD heeft dit aan de orde gesteld in de derde en vierde voortgangsrapportage over de implementatie van de Wiv 2017[7] en in het nog te verschijnen toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan.[8] Het huidige onderscheid tussen algemene bevoegdheden en bijzondere

[5] Toezichtsrapport van de CTIVD nr. 55 (2017) over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 155 (bijlage), beschikbaar op www.ctivd.nl.
[6] De publicatie wordt verwacht op 22 september 2020. Een versie van het vastgestelde rapport zal u zo spoedig mogelijk na 25 augustus 2020 onder embargo worden verstrekt.
[7] CTIVD nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage) en de nog te verschijnen vierde voortgangsrapportage (publicatie gepland op 8 september 2020).
[8] De publicatie wordt verwacht op 22 september 2020. Een versie van het vastgestelde rapport zal u zo spoedig mogelijk na 25 augustus 2020 onder embargo worden verstrekt.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

bevoegdheden voor wat betreft het verzamelen en verder verwerken van bulkdatasets verdient daarom heroverweging. Dit onderwerp komt nader aan de orde in paragraaf 4.

Ten tweede is de regulering van geautomatiseerde (meta)data-analyse in de Wiv 2017 niet in balans. Geautomatiseerde data-analyse is een dagelijkse kernactiviteit van de diensten waarbij juist ook eenvoudige vormen een grote inbreuk op de rechten van de burger kunnen maken. De Wiv 2017 schrijft alleen een bijzondere bevoegdheid voor bij metadata-analyse op gegevens uit onderzoeksopdrachtgerichte interceptie (OOG-I) ter identificatie van personen of organisatie. Daarvoor is toestemming van de minister en toetsing op rechtmatigheid daarvan door de TIB nodig. Overige vormen van (meta)data-analyse vallen onder de (algemene) bevoegdheid uit artikel 60, waarvoor geen specifieke waarborgen gelden. Dit terwijl onder deze bepaling een breed scala van (eenvoudige/feitelijke tot complexe/voorspellende) vormen van data-analyses valt, die betrekking hebben op alle gegevens bij de diensten, waaronder gegevens/bulkdatasets die via algemene of bijzondere bevoegdheden zijn verzameld. De CTIVD heeft deze problematiek al (deels) aan de orde gesteld in een rechtseenheidsbrief met de TIB van 21 november 2018[9] en in (een nulmeting en twee steekproeven die ten grondslag liggen aan) de voortgangsrapportages over de implementatie van de Wiv 2017.[10] De nadere uitwerking van het onderwerp van geautomatiseerde data-analyse vindt plaats in paragraaf 5.

***Naar een algemeen normatief kader***

Twee jaar na inwerkintreding van de Wiv 2017 is voor de CTIVD duidelijk dat de Wiv 2017 tenminste zodanig moet worden aangepast dat wordt voorzien in een (uniform) normatief kader voor het verzamelen en verder verwerken van bulkdatasets en voor geautomatiseerde data-analyse. Waar het gaat om gegevens(verwerking), dient de inzet van bevoegdheden te worden onderscheiden van de "opbrengst" en wat met deze opbrengst wordt gedaan. Een nieuwe regeling in de wet voor bulkdatasets en geautomatiseerde data-analyse draagt bij aan uniformiteit en daardoor een beter voorzienbare wetgeving voor de burgers met voldoende waarborgen ter bescherming van de fundamentele rechten.

Een nieuwe regeling in de wet biedt tevens de mogelijkheid het normatief kader met betrekking tot de gegevensverwerking na samenspraak met de diensten nader in te vullen, zoals het stellen van bewaartermijnen na verwerving van verschillende typen bulkdatasets en specifieke waarborgen bij de verwerking van deze gegevens in het kader van geautomatiseerde data-analyse. Op deze wijze kan meer recht worden gedaan aan de dynamische operationele praktijk van de diensten.

De rechtmatigheidsbeoordeling van een dergelijk normatief kader voor bulkdatasets en geautomatiseerde data-analyse ligt bij het toezicht, zoals dat nu ook het geval is ten aanzien van andere normatieve aspecten (zorgplicht, proportionaliteit, subsidiariteit, noodzakelijkheid, gerichtheid) en wordt verder vorm gegeven in een toetsingskader.

***Tussenconclusie***

- De wet dient te voorzien in normatieve kaders voor het verzamelen en verder verwerken van bulkdatasets enerzijds en voor geautomatiseerde data-analyse anderzijds. Hiermee wordt beter

[9] Brief van 23 november 2018 van de TIB en de CTIVD over geautomatiseerde data-analyse, *Kamerstukken II* 2018/19, 29 924, nr. 174.
[10] CTIVD nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage) en de nog te verschijnen vierde voortgangsrapportage (publicatie gepland op 8 september 2020).

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

recht gedaan aan de vereisten van voorzienbaarheid, uniformiteit en de rechtsbescherming van de burger.

- De nadere invulling van het normatieve kader geschiedt door de CTIVD na samenspraak met de diensten in een toetsingskader, waarna de rechtmatigheidsbeoordeling van de praktijk plaatsvindt aan de hand van het aldus ontwikkelde toetsingskader. Dit doet recht aan de dynamische operationele praktijk van de diensten.

## 3 Toezicht

Tijdens de bijeenkomst met de evaluatiecommissie werd gevraagd om nadere duiding van het door de CTIVD beoogde toezichtsmodel. In deze paragraaf worden diverse toezichtvragen op hoofdlijnen geadresseerd. De CTIVD nodigt uw commissie uit in een afzonderlijke verdiepingssessie het onderwerp toezicht nader te bespreken (met name waar het gaat om de concrete inrichting van geïntegreerd toezicht, de verdere borging van de onafhankelijkheid en aanwezige professionaliteit). Wij stellen voor daar ook de voorzitter van de afdeling klacht van de CTIVD en de voorzitter van de TIB voor uit te nodigen.

Bij de inzet van bevoegdheden die een vergaande inmenging vormen in de persoonlijke levenssfeer vereist het Europees Hof voor de Rechten van de Mens (EHRM) voldoende toezicht vooraf, tijdens en na de inzet van de bevoegdheid. Toezicht moet onafhankelijk en effectief zijn. Deze lijn is niet alleen zichtbaar in de jurisprudentie over de interceptie van telecommunicatie[11], maar ook in meer specifieke instrumenten, zoals de Conventie 108+ van de Raad van Europa en de Algemene Verordening Gegevensbescherming (AVG) van de Europese Unie. De AVG gaat niet over nationale veiligheid, maar geeft wel aan wat relevant is wanneer het gaat om onafhankelijk en effectief toezicht in het kader van gegevensverwerking. Bovendien vormt de AVG een belangrijke inspiratiebron voor Conventie 108+ die nadrukkelijk wel van toepassing is op gegevensverwerking in het kader van nationale veiligheid.

Het EHRM voorziet daarbij al jaren een 'holistische benadering' van toezicht vooraf, tijdens en achteraf, met een nadruk op een voorafgaande, onafhankelijke (rechterlijke) toets en bindende elementen.[12] Hierbij geldt dat het toezichtstelsel als geheel in balans dient te zijn. Een aanscherping hiervan kan worden afgeleid uit recente jurisprudentie van het EHRM, als ook uit die van het Hof van Justitie EU en uit Conventie 108+. Hieruit volgt dat toezicht integraal dient te zijn met bindende bevoegdheden ten aanzien van activiteiten waarbij een inbreuk op de fundamentele rechten in het geding is. Dit wordt onder meer met het volgende citaat van het EHRM geïllustreerd: *"Therefore while the Court considers judicial authorization to be an important safeguard, and perhaps even 'best practice', by itself it can neither be necessary nor sufficient to ensure compliance with Article 8"* (...) *"Rather regard must be had to the actual*

[11] EHRM GC 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, par. 233/249 (*Roman Zakharov t. Rusland)*, en EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije)*, en EHRM 13 september 2018, 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 233/258 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*). ECLI:CE:ECHR:2018:0619JUD003525208, par. 151-161 (*Centrum För Rättvisa t, Zweden*). Beide laatste zaken zijn voorgelegd aan de Grote Kamer van het EHRM.

[12] EHRM GC 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306, par. 233/249 (*Roman Zakharov t. Rusland)*, en EHRM 12 januari 2016, nr. 37138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije)*,

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

*operation of the system of interception, including checks and balances of the exercise of power, and the existence or absence of any evidence of actual abuse"*.[13]

***Problematiek in de huidige wet***

De Commissie Dessens (evaluatiecommissie Wiv 2002) raadde in 2013 een vorm van 'integraal en bindend toezicht' aan. Dat wil zeggen een concentratie van *ex ante*, *ex nunc* en *ex post* toezicht. Het voorstel was dat de CTIVD direct na de toestemmingsverlening door de minister een bindend oordeel geeft over de rechtmatigheid van de inzet van bevoegdheden die diep ingrijpen in de grondrechten van burgers.[14] Integraal toezicht werd onderschreven door de Raad van State in zijn advies over het wetsvoorstel.[15] De kritiek van de Raad van State op het creëren van een nieuwe commissie die een rechtmatigheidstoets vooraf uitvoert, richtte zich er met name op dat daarmee een versnipperd stelsel van toezicht wordt gecreëerd.[16]

In de Wiv 2017 heeft de wetgever uiteindelijk gekozen voor een gefragmenteerd model met de introductie van de TIB die *ex ante* een bindende rechtmatigheidstoets uitvoert bij de inzet van bepaalde bijzondere bevoegdheden. De rechtbank Den Haag dient *ex ante* toestemming te geven voor de inzet van de bevoegdheid tot het openen van brieven en voor de inzet van bijzondere bevoegdheden jegens advocaten en journalisten (art. 30 lid 2 en 3, art. 27 lid 2). Er werd niet gekozen om alles te concentreren bij de Nederlandse rechter, omdat deze zich mogelijk niet bevoegd zou achten zich uit te spreken over de inzet van bevoegdheden in het buitenland en omdat de toetsing van de inzet van bevoegdheden niet alleen juridische maar ook technische en inlichtingenmatige kennis en kunde vereist die in een specialistische commissie als de TIB kan worden opgebouwd.[17] De CTIVD houdt toezicht op de rechtmatige naleving van de gehele Wiv 2017 (en de Wvo) en behandelt klachten hierover en meldingen van misstanden. De oordelen van de afdeling toezicht van de CTIVD zijn, anders dan die van de afdeling klacht, niet bindend.

De huidige fragmentatie in het toezichtstelsel sluit niet aan bij de praktijk van gegevensverwerking door de diensten die in de kern bestaat uit het nader verwerken/analyseren van gegevensbestanden (met als bijzonderheid de toenemende importantie van bulkdatasets). Deze gegevensverwerking is een continue, dynamisch en complex proces. Bindende *ex ante* toetsing/toestemming bestrijkt slechts een beperkt deel van dat proces, namelijk de inzet van bepaalde bijzondere bevoegdheden, en heeft geen zicht op de verdere verwerking van (de daarmee verzamelde) gegevens. Bovendien vereist toezicht op gegevensverwerking andere vaardigheden en methoden, zoals systeemtoezicht,[18] steekproeven en diepteonderzoeken en grondige kennis van de operaties van de diensten. In het bijzonder door het ontbreken van bindende bevoegdheden in het toezicht kan juist daar waar de inbreuk op de rechten van burgers het grootst is – het proces van gegevensverwerking – de rechtmatigheid niet voldoende worden gewaarborgd. Het bindende karakter van de oordelen van de afdeling klachtbehandeling van de CTIVD is eveneens nodig, maar vormt als zodanig geen substituut voor of invulling van effectief en geïntegreerd (integraal) toezicht. Het compartimentaliseren van het toezichtstelsel is niet in overeenstemming met de

[13] EHRM 13 september 2018, 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 316-320 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*).
[14] Rapport Dessens, Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen. *Kamerstukken II* 2013/14, 33 820, nr. 1.
[15] Advies Raad van State op het wetsvoorstel Wiv 20xx, *Kamerstukken II* 2016/17, 34 588, nr. 4, p. 12-19.
[16] Zie ook het advies van de Raad van State, *Kamerstukken II* 2016/17, 34 588, nr. 4.
[17] *Kamerstukken II* 2016/17, 34 588, 3, p. 51.
[18] Voor uitleg van dit begrip zie voetnoot 4.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

noodzakelijk te hanteren werkwijzen van de diensten, noch bezien vanuit het perspectief van het toezicht ter bescherming van de onderliggende belangen van nationale veiligheid en mensenrechten. Rechtseenheidsoverleg is nuttig, maar geen substituut voor effectief en geïntegreerd (integraal) toezicht. De zich in de afgelopen jaren ontwikkelde jurisprudentie van het EHRM en het HvJ EU vormt een bevestiging hiervan.

***Naar geïntegreerd en effectief toezicht***

Uit de eerder genoemde EHRM-jurisprudentie, jurisprudentie van het Hof van Justitie EU[19] en 'Conventie 108+' over geautomatiseerde gegevensverwerking uit 2018 (waarin de jurisprudentie van het EHRM en de AVG worden gecodificeerd) volgt dat effectief toezicht op de verwerking van gegevens binnen het nationale veiligheidsdomein ook betekent dat een toezichthouder effectief behoort te kunnen optreden tegen onrechtmatige gegevensverwerkingen.

In Conventie 108+ wordt uitgelegd dat dit betekent dat het uitgangspunt is dat toezichthouders de bevoegdheid moeten hebben gegevensverwerkingen bij geconstateerde onrechtmatigheden stop te zetten en de vernietiging van gegevens op te leggen.[20] Ook is denkbaar dat andere maatregelen worden opgelegd, waarbij een beroep op besluitvorming door de toezichthouder bij een rechterlijke instantie mogelijk kan zijn.[21] Zoals eerder aangegeven, is een beperkt aantal uitzonderingen hierop slechts mogelijk voor zover dat noodzakelijk en proportioneel wordt geacht in een democratische samenleving.[22]

De CTIVD ziet in dit verband geen redenen waarom bijvoorbeeld het ontbreken van doorzettingsmacht ten aanzien van gegevensverwerking kan worden gerechtvaardigd met een beroep op het noodzakelijkheids- en proportionaliteitsvereiste. In andere vormen van toezicht is dergelijke doorzettingsmacht ten aanzien van de rechtmatigheidstoetsing gebruikelijk (vergelijk de Autoriteit Persoonsgegevens (AP)). Daarnaast is er wel een dergelijke doorzettingsmacht aanwezig bij de *ex ante* toetsing en het klachtenrecht.

Conventie 108+ noopt ook tot nadenken over de inrichting van onafhankelijk en effectief toezicht op gegevensverwerking in het kader van de nationale veiligheid in brede zin: houdt de AP onafhankelijke en effectief toezicht op deze bijzondere gegevensverwerkingen buiten de AIVD en de MIVD (bijvoorbeeld in samenwerkingsvormen en gegevensverwerkingen door de Nationaal Coördinatorbestrijding Terrorisme en Veiligheid (NCTV)) (zie verder paragraaf 6).

De toezichtspraktijk van de CTIVD onderstreept waarom het vanuit rechtsstatelijk perspectief essentieel is voor onafhankelijk en effectief toezicht dat de CTIVD de instrumenten krijgt toebedeeld om te handhaven bij onrechtmatige gegevensverwerkingen. In de derde voortgangsrapportage[23] rapporteerde de CTIVD dat enkele bulkdatasets die zijn verkregen door toepassing van de hackbevoegdheid bij het verlopen van de bewaartermijn (uit artikel 27 Wiv 2017) grotendeels of in het geheel relevant zijn verklaard en worden gebruikt voor gegevensverwerkingen, terwijl deze gegevens op grond van de wet hadden moeten zijn vernietigd en het overgrote merendeel van deze gegevens van personen in deze bulkdatasets niet

[19] Zie voetnoot 11.
[20] Zie artikel 15 Conventie 108+.
[21] Artikel 15 lid 9 Conventie 108+.
[22] Zie artikel 11 lid 3 Conventie 108+, waarbij uitzonderingen alleen aan de orde mogen zijn: *"by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim."*
[23] CTIVD nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage).

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

relevant zijn voor de taakuitvoering van de diensten en dat ook nooit zullen worden. Deze werkwijze is onrechtmatig, maar de gegevens in de datasets worden desondanks verder verwerkt. De oordelen van de CTIVD hebben volgens de huidige wet geen bindend karakter. Er bestaat hier een duidelijk toezichtsgat: Effectief en onafhankelijk toezicht houdt in dat een onafhankelijke toezichthouder niet alleen oordeelt over de rechtmatigheid van de gedragingen van de uitvoerende instantie, maar dit oordeel vervolgens ook kan effectueren en dat dit niet ter beoordeling aan de ondertoezichtgestelde instantie zelf wordt gelaten. Het voorbeeld toont de noodzaak aan om bindende oordelen te kunnen geven omtrent onrechtmatige gegevensverwerkingen. Dit raakt geenszins de ministeriële verantwoordelijkheid, immers deze omvat, naast de doelmatigheidstoetsing en politieke verantwoordelijkheid, de rol als medewetgever en de daarmee aanwezige mogelijkheid om binnen de grondwettelijke en rechtsstatelijke kaders te streven naar andere wetgeving. Bindende bevoegdheden in het kader van rechtmatigheidstoetsing zijn hiermee niet in strijd, worden elders in het toezicht reeds toegepast en volgen uit de jurisprudentie.

Overigens brengen eisen van rechtszekerheid en zorgvuldigheid met zich mee dat een toezichthouder transparant is bij de toepassing van een normatief kader en dit neerlegt in een eigen rechtmatigheidstoetsingskader (zoals ook gebruikelijk is bij andere toezichthouders).

***Tussenconclusie***

- Het compartimentaliseren van het toezichtstelsel is niet in overeenstemming met de noodzakelijk te hanteren werkwijzen van de diensten, noch bezien vanuit het perspectief van het toezicht ter bescherming van de onderliggende belangen van nationale veiligheid en mensenrechten. De kern van het werk van de diensten bestaat uit het verwerken/analyseren van gegevensbestanden (met als bijzonderheid de toenemende importantie van bulkdatasets). Deze gegevensverwerking is een continue dynamisch en complex proces. Bindende *ex ante* toetsing bestrijkt slechts een beperkt deel van het proces, namelijk de inzet van bepaalde bijzondere bevoegdheden, en heeft geen zicht op de verdere verwerking van gegevens. Bovendien vereist toezicht op gegevensverwerking andere vaardigheden en methoden, zoals systeemtoezicht in combinatie met steekproeven en diepteonderzoeken. Juist daar waar de inbreuk op de rechten van burgers het grootst is – het proces van gegevensverwerking – dient de rechtmatigheid ervan voldoende gewaarborgd te worden. Bindende bevoegdheden in het rechtmatigheidstoezicht raken niet de ministeriële verantwoordelijkheid.
- Het internationale vereiste van effectief toezicht (jurisprudentie EHRM, HvJ EU en Conventie 108+) op de verwerking van gegevens door de AIVD en de MIVD houdt in dat een toezichthouder doorzettingsmacht heeft om te kunnen optreden tegen onrechtmatige gegevensverwerkingen. Ook de toezichtspraktijk van de CTIVD onderstreept de noodzaak hiervan.
- In de wet kan dit eenvoudig worden verankerd door artikel 124 (lid 4 en 5) over de bindende oordelen van de afdeling klacht van de CTIVD van overeenkomstige toepassing te verklaren op de afdeling toezicht van de CTIVD, dan wel door de betreffende bevoegdheden te incorporeren in enig ander model van toezicht.

## 4 Bulkdatasets

Bulkdatasets zijn een grote gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties of personen die geen onderwerp van onderzoek zijn en dat ook nooit zullen worden. De CTIVD heeft in haar toezichtsactiviteiten vastgesteld dat bulkdatasets worden verworven met de inzet van verschillende bevoegdheden, met name OOG-interceptie, de hackbevoegdheid, de inzet van agenten

en de informantenbevoegdheid.[24] Ook ontvangen en delen de AIVD en de MIVD bulkdatasets (onder de bepalingen uit de Wiv 2017) met buitenlandse inlichtingen- en/of veiligheidsdiensten.

De noodzaak voor het verzamelen en verder verwerken van bulkdatasets in het belang van de nationale veiligheid staat voor de CTIVD buiten kijf. De gegevens in bulkdatasets worden via applicaties veelvuldig bevraagd voor het onderkennen van targets. Het biedt de diensten ook de mogelijkheid nieuwe targets te onderkennen door middel van geautomatiseerde data-analyse. Mede in het kader van het onderkennen van de ongekende dreiging is het van belang dat de diensten over bulkdatasets kunnen beschikken. Zonder de mogelijkheid tot het verwerken van bulkdatasets verliezen de AIVD en de MIVD belangrijke bronnen van gegevens en bestaat het gevaar dat niet meer vroegtijdig bedreigingen voor de nationale veiligheid worden onderkend.

Bij het verzamelen en verder verwerken van gegevens uit bulkdatasets vindt een ernstige inbreuk plaats op de fundamentele rechten van betrokkenen, onder meer het recht op privacy, maar mogelijk ook de vrijheid van meningsuiting voor zover het de verwerking van communicatiegegevens betreft.[25] Het EHRM heeft met betrekking tot bulkinterceptie en de grootschalige opslag van gegevens normen ontwikkeld voor het verzamelen en verder verwerken van bulkdatasets.[26] De uitgangspunten daarvan zijn mede geconsolideerd in Conventie 108+.[27]

De regeling moet waarborgen bevatten bij het verzamelen van bulkdatasets, zoals voorafgaande toestemming door een onafhankelijke instantie en regels voor de (verdere) verwerking van de gegevens. In de zaak *Big Brother Watch e.a. tegen het Verenigd Koninkrijk* geeft het EHRM bijvoorbeeld aan (i) welke procedures er zijn voor het opslaan, toegankelijk maken, onderzoeken en gebruik van de onderschepte gegevens, (ii) welke procedures er zijn voor het versturen van de onderschepte gegevens aan andere partijen en (iii) op welke wijze toezicht is geregeld, notificatie en 'remedies'.[28] Dit zijn elementen die in ieder geval toepasselijk en aanwezig moeten zijn in een regeling voor bulkdatasets in de Wiv 2017.

---

[24] Toezichtsrapport nr. 55 (2017) over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, *Kamerstukken II* 2016/17, 29 924, nr. 155 (bijlage), CTIVD-rapport nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage), en de te verschijnen toezichtsrapporten over de verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD (2020) en toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan door de AIVD en de MIVD (2020).

[25] Zie met name EHRM (GK) 4 december 2015, nr. 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov t. Rusland*), EHRM 19 juni 2018, 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*), HvJ EU 8 april 2014, C293/12, C-594/12, ECLI:EU:C:2014:238, (*Digital Rights t. Ierland*) en HvJ EU 21 december 2016, C-203/15 en C698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen en Secretary of State for the Home Department t. Tom Watson e.a.*).

[26] EHRM 4 december 2008, nrs. 30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204, par. 99 (S. en *Marper t. Het Verenigd Koninkrijk*), EHRM 19 juni 2018, 35252/08, ECLI:CE:ECHR:2018:0913JUD005817013 (*Centrum för Rättvisa t. Zweden*) en EHRM 13 september 2018, 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*).

[27] De systematiek van Conventie 108+ beoogt ook toekomstige jurisprudentie te incorporeren.

[28] EHRM 13 september 2018, 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*),

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

***Problematiek in de huidige wet***

De huidige regeling in de Wiv 2017 is inconsistent, omdat niet bij de inzet van alle toepasselijke bevoegdheden waarmee bulkdatasets kunnen worden verworven een gelijk regime geldt, voor wat betreft de voorafgaande toetsing door een onafhankelijke instantie. Deze voorafgaande toets ontbreekt onder meer bij toepassing van de informantenbevoegdheid, de agentenbevoegdheid en bij het ontvangen van bulkdatasets uit internationale samenwerking.

Daarnaast laat de praktijk zien dat de Wiv 2017 en het beleid voor 'werken met grote datasets'[29] niet consequent of in het geheel niet worden toegepast. De doorzettingsmacht bij de *ex ante* toetsing en bij klachten lost dergelijke onrechtmatigheden gedurende de verwerking van gegevens niet op. In de parlementaire discussie over de Wijzigingswet 2017 zijn zowel in de Tweede Kamer als in de Eerste Kamer veelvuldig vragen gesteld over de mogelijkheid bulkgegevens te vergaren op grond van de informantenbevoegdheid en in het kader van internationale samenwerking (zie paragraaf 6) met daarbij de vraag of de huidige regeling volstaat.[30]

Een belangrijk probleem in de Wiv 2017 doet zich voor bij bulkdatasets die via bijzondere bevoegdheden (buiten OOG-I) zijn verzameld. Op basis van artikel 27 Wiv 2017 dienen de verzamelde gegevens 'zo spoedig mogelijk' te worden onderzocht op relevantie. Gegevens die niet binnen één jaar zijn onderzocht (met de mogelijkheid van verlenging van zes maanden) , moeten terstond worden vernietigd. De CTIVD weet vanuit haar toezichtspraktijk dat het gezien de aard en omvang van bulkdatasets niet mogelijk is aan dit vereiste te voldoen. Hier verdient opmerking dat in de Wiv 2017 voor gegevens uit OOG-I, in essentie bulkgegevens, niet het vereiste van 'zo spoedig mogelijk' beoordelen op relevantie geldt en een bewaartermijn van drie jaar bestaat. Gelet op het belang van bulkdatasets voor de nationale veiligheid, heeft dit de diensten ertoe gebracht bepaalde bulkdatasets na afloop van de bewaartermijn geheel of grotendeels relevant te verklaren om de sets zo langer te kunnen bewaren. Deze wijze van relevantiebeoordeling is echter onrechtmatig en holt de wettelijke waarborgen uit.

Hierbij is van belang dat bulkdatasets voor het merendeel uit gegevens bestaan die betrekking hebben op personen of organisaties die geen onderwerp van aandacht van de diensten zijn en dat ook nooit zullen worden. Deze gegevens zullen dus nooit (juridische) relevantie in de zin van artikel 27 Wiv 2017 hebben voor de taakuitvoering van de diensten. Dit begrip dient te worden onderscheiden van de gangbare maatschappelijke betekenis die het woord heeft. De CTIVD benadrukt dat bulkdatasets noodzakelijk (relevant) zijn voor het werk van de diensten, met name ook het onderkennen van (nieuwe) targets. Door de sets na afloop van de bewaartermijn uit artikel 27 Wiv 2017 (grotendeels) juridisch relevant te verklaren, is het gevolg dat alle data in het betekenisregime (artikel 20 Wiv 2017) komen, met als consequentie dat deze gegevens voor alle taken van de diensten mogen worden gebruikt, zonder op voorhand vastgestelde bewaartermijn of vernietigingsplicht. De gekozen toepassing van de relevantiebeoordeling leidt dus tot een uitholling van de noodzakelijke waarborgen. De oplossing dient dan ook te worden gezocht in een ruimere bewaartermijn voor bulkdatasets met voldoende waarborgen ter bescherming van de fundamentele rechten van de burger. De CTIVD heeft dit aan de orde gesteld in de derde en vierde voortgangsrapportage over de implementatie van de Wiv 2017[31] en in het nog te verschijnen

[29] Zie: https://www.aivd.nl/onderwerpen/werken-met-grote-datasets.
[30] *Kamerstukken II* 2019/20, 35 242, nr. 6 en *Kamerstukken I* 2019/20, 35 242, nr. A.
[31] CTIVD nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage) en de nog te verschijnen vierde voortgangsrapportage (publicatie gepland op 8 september 2020).

toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan.[32]

Bij bulkdatasets die zijn verzameld via algemene bevoegdheden of verkregen via internationale samenwerking doet zich het probleem voor dat deze direct in het betekenisregime (artikel 20 Wiv 2017) komen. Gegevens die in het betekenisregime komen, mogen worden gebruikt voor alle taken van de diensten. Een bepaalde bewaartermijn is niet aan de orde. Hierbij is van belang op te merken dat het bij deze bulkdatasets naar de aard ervan (mate van inbreuk op de fundamentele rechten van burgers) om dezelfde bulkdatasets kan gaan die met de inzet van bijzondere bevoegdheden worden verzameld (zie ook de voorgaande alinea).

***Naar een uniforme regeling voor bulkdatasets***
In het kader van de voorzienbaarheid en bescherming van de fundamentele rechten van burgers is het van belang dat in de Wiv 2017 een eenduidige regeling voor bulkdatasets (als bijzondere bevoegdheid) wordt gecreëerd.

Hierbij dient het uitgangspunt te zijn: 'bulk is bulk'. De wijze van verwerving van bulk is niet leidend voor de mate van inbreuk op de rechten van burgers. De aard van de gegevens (bulk) is dat wel. Een dergelijk stelsel van bevoegdheden en waarborgen voor bulk is nu bij wet slechts geregeld voor OOG-interceptie.[33] In een nieuwe regeling voor bulkdatasets is het volgens de CTIVD daarnaast van belang dat diensten de ruimte hebben de verdere verwerking van gegevens in een dynamische proces uit te voeren met daarbij voldoende *checks and balances*.

Uit de praktijk blijkt dat er in ieder geval knelpunten bestaan in de termijn van de uit te voeren relevantietoets bij de inzet van bijzondere bevoegdheden (zoals de agentenbevoegdheid en de hackbevoegdheid). De CTIVD stelt vast dat bij bulkdatasets van te voren veelal niet goed is vast te stellen hoe lang de gegevens bewaard moeten worden, omdat de operationele levensduur van een bulkdataset pas echt duidelijk wordt gedurende de verdere verwerking van de gegevens in de bulkdataset. Mede op basis van de ervaringsleer uit het voorgaande jaar, kan gemotiveerd worden waarom de verlenging noodzakelijk, proportioneel en subsidiair is. Een toetsingskader kan er dan bijvoorbeeld in voorzien dat de AIVD en de MIVD periodiek - aan de hand van bepaalde toetsingselementen - nagaan of de bulkdataset bewaard moeten blijven en dit gemotiveerd ter toetsing aan het toezicht voorleggen. Gecomplementeerd met bindende bevoegdheden wordt zo een betere balans aangebracht voor wat betreft de belangen van de diensten en de daarbij noodzakelijke waarborgen.

***Tussenconclusie***
- Er dient een uniforme wettelijke regeling te komen voor bulkdatasets. Hiervoor dient 'bulk is bulk' het uitgangspunt te zijn. Dit betekent dat niet de wijze van verwerving van de datasets leidend is, maar de aard (bulkkarakter) van de data.
- De verzameling van bulkdatasets behoort in een nieuwe regeling als bijzondere bevoegdheid vorm te krijgen. Wanneer het verwerven niet is voorzien, wordt *ex-post* een toestemming verkregen alvorens de gegevens verder worden verwerkt door de diensten. Indien een

[32] De publicatie wordt verwacht op 22 september 2020. Een versie van het vastgestelde rapport zal u zo spoedig mogelijk na 25 augustus 2020 onder embargo worden verstrekt.
[33] Zie de bijzondere bevoegdheden voor de fasen van (1) interceptie (artikel 48), (2) optimalisatie van interceptie en selectie (artikel 49), en (3) de analyse en selectie van de geïntercepteerde gegevens (artikel 50 Wiv 2017).

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

toestemming niet wordt verleend, dient de betreffende bulkdataset terstond te worden vernietigd. Daar waar de diensten meer ruimte krijgen voor de verwerking van gegevens (inclusief geautomatiseerde data-analyse), dient een toetsingskader met passende waarborgen (zoals bindend *ex nunc* en *ex post* toezicht) tegenover te staan.
- Bij het – door de CTIVD - na samenspraak met de diensten – uit te werken toetsingskader moet worden gedacht aan de nadere de invulling van bewaartermijnen van de bulkdatasets en functie-taakscheiding als onderdeel van een strikt (intern) autorisatieregime bij de verwerking van gegevens uit bulkdatasets.

## 5 Geautomatiseerde data-analyse

Geautomatiseerde data-analyse (GDA ex. art. 50 en 60 Wiv 2017) omvat de kern van de activiteiten van de diensten. GDA bevat veel verschillende vormen: Het betreft in ieder geval het op geautomatiseerde wijze onderling vergelijken van gegevens, het doorzoeken van gegevens aan de hand van profielen en het vergelijken van gegevens met het oog op het opsporen van bepaalde patronen.[34] "Metadata-analyse" is ook aan te merken als GDA.[35]

Bij GDA kan een ernstige inbreuk op de fundamentele rechten van personen plaatsvinden (met name met betrekking tot het recht op bescherming van gegevens en het recht op privacy). De Commissie-Dessens stelde in 2013 al vast dat het analyseren van metadata een ernstige privacy-inbreuk met zich mee kan brengen en meer waarborgen in de Wiv 2017 daarvoor noodzakelijk zijn.

***Problematiek in de Wiv 2017***
Het rapport van de Commissie Dessens resulteerde uiteindelijk in de bijzondere bevoegdheid tot geautomatiseerde metadata-analyse op gegevens uit OOG-interceptie ter identificatie van personen en organisaties (GDA ex. art. 50 Wiv 2017). Daarmee biedt de Wiv 2017 slechts *gedeeltelijk* bescherming aan de fundamentele rechten van burgers. Dit is niet het geval wanneer de analyse plaatsvindt op gegevens verzameld via uitsluitend andere bevoegdheden, zoals de hackbevoegdheid en/of de informantenbevoegdheid (GDA ex. art. 60 Wiv 2017) *of* de analyse (GDA ex. art. 50 Wiv 2017) niet is gericht op de identificatie van een persoon of organisatie, maar bijvoorbeeld op het in kaart brengen van de locatiegegevens of internethistorie van een reeds onderkend target. In dit laatste geval is de *ex ante* toestemming op grond van art. 50 Wiv 2017 niet van toepassing.

Tegelijkertijd blijkt uit de praktijk dat een bescherming in de vorm van een bijzondere bevoegdheid met voorafgaande toetsing niet goed past bij een dynamisch proces als geautomatiseerde data-analyse. De CTIVD concludeert om deze reden dat de Wiv 2017 dient te worden aangepast om een passend beschermingsniveau te bieden voor geautomatiseerde data-analyse en tegelijkertijd de diensten de nodige flexibiliteit te bieden voor de verwerking van gegevens.

Voor het bepalen van de noodzakelijke waarborgen bij GDA onderscheidt de CTIVD primair twee sporen: 1) risico's die zich manifesteren tijdens en als gevolg van de ontwikkeling van applicaties (bij complexere

[34] Zie de niet-limitatieve opsomming in artikel 60 lid 2 Wiv 2017.
[35] Zie ook de rechtseenheidsbrief van 23 november 2018 van de TIB en de CTIVD over geautomatiseerde data-analyse, *Kamerstukken II* 2018/19, 29 924, nr. 174.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

vormen van GDA bestaan veelal hogere risico's) en 2) de mate van inbreuk als gevolg van de inzet van GDA, waarbij ook simpele vormen een grote inbreuk met zich mee kunnen brengen.

We lichten hierna eerst de risico's toe ten aanzien van de ontwikkeling van applicaties, data-analyses die een ernstige privacy-inbreuk maken en GDA met een voorspellend karakter. Daarna gaan we in op onze visie voor een nieuwe regeling.

Er is al een verdiepingssessie met uw commissie gepland over dit onderwerp.

***Risico's bij de ontwikkeling van applicaties***
Al in de ontwerpfase van applicaties dient rekening te worden gehouden met de impact op fundamentele rechten en nakoming van de gegevensverwerkingsbepalingen. Voor alle vormen van gegevensverwerkingen geldt namelijk dat deze worden genormeerd door de algemene bepalingen omtrent gegevensverwerking in de artikelen 18-24 Wiv 2017. Als nadere concretisering van (met name) de zorgplicht in artikel 24 Wiv 2017 is in het nader verslag van de Wiv 2017 opgemerkt dat 'bij het ontwerpen, aankopen en in gebruik nemen van technische systemen de diensten rekening houden met de beginselen van gegevensbescherming, zoals *gegevensbescherming by design* en *by default*'. Daarbij wordt 'gegevensbescherming *by design*' opgevat als een verplichting dat 'de diensten bij de ontwikkeling van systemen het belang van privacy en gegevensbescherming inbouwen'. 'Gegevensbescherming *by default*' ziet volgens de regering erop dat systemen 'zo ontworpen en ingericht worden dat zo min mogelijk persoonsgegevens worden verwerkt'.[36]

De voortgangsrapportages van de CTIVD over de implementatie van de Wiv 2017 laten met betrekking tot GDA bijna twee jaar na de inwerkingtreding van de Wiv 2017 het beeld van een 'gemiddeld risico' op onrechtmatigheden zien.[37] Dat is met name te verklaren omdat veel focus kwam te liggen op de bijzondere bevoegdheid tot geautomatiseerde metadata-analyse in artikel 50 lid 1 sub b Wiv 2017 en minder op de uitwerking van onder meer de zorgplicht bij andere vormen van geautomatiseerde data-analyse in de zin van artikel 60 Wiv 2017, waarbij zich ook risico's met betrekking tot de bescherming van persoonsgegevens voordoen.

***Data-analyses die een ernstige privacy-inbreuk maken***
Door middel van applicaties kunnen medewerkers van de diensten bijvoorbeeld gegevens raadplegen over targets door een zoekslag uit te voeren over verschillende databronnen om meer over hen te weten te komen. Veel van deze vormen worden ook wel beschreven als een eenvoudige of simpele data-analyse.

Door het combineren van verschillende typen gegevens kan echter een 'min of meer volledig beeld van bepaalde aspecten van het privéleven van een persoon' worden verkregen. Daarbij kan gedacht worden aan het analyseren van locatiegegevens van de mobiele telefoon van een target of het analyseren van het internetgebruik na het intercepteren van de communicatie.[38] Software maakt het mogelijk om

---

[36] *Kamerstukken II* 2016/17, 34 588, 18, p. 22.
[37] De vierde voortgangsrapportage wordt 8 september 2020 gepubliceerd. Wij zullen uw commissie deze rapportage eerder onder embargo doen toekomen. .
[38] Zie EHRM 13 september 2018, nrs. 58170/13, 62322/14 en 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, par. 356 (*Big Brother Watch e.a. t. het Verenigd Koninkrijk*) (sinds februari 2019 aanhangig bij de Grote Kamer): "*The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since*

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

verschillende datasets bij elkaar te brengen (als verschillende "lagen van gegevens") en daarmee netwerken of knooppunten van personen in kaart te brengen. De CTIVD voorstaat een technologieneutrale benadering voor geautomatiseerde data-analyse. De privacy-impact wordt niet bepaald door de vraag of een "simpel" of "eenvoudige instrument" wordt ingezet.

In de praktijk bestaan er grote uitvoeringsproblemen met betrekking tot de bijzondere bevoegdheid tot GDA in artikel 50 lid 1 sub b Wiv 2017, waarover de evaluatiecommissie ook door de diensten is geïnformeerd. In de aanvraag tot de uitvoering van de bijzondere bevoegdheid lijkt met name spanning te zitten op te brede formulering en veelvoud van mogelijke verwerkingsvormen ter uitvoering van GDA gedurende ten hoogste een jaar. Bij een *ex ante* toepassing is het lastig te overzien in welke mate een gerechtvaardigde inbreuk op de fundamentele rechten van mensen wordt gemaakt. Ook blijkt het in de praktijk lastig een duidelijk onderscheid te maken tussen 'metadata' en 'inhoud', met name bij internetgerelateerde data.[39] Bovendien bestaat in de wet nu een verschil in niveau van bescherming tussen inhoud en metadata dat niet houdbaar is.

Voor de kennisname van inhoud, bijvoorbeeld selectie van OOG-I gegevens (artikel 50 lid 1 sub a Wiv 2017), bevat de Wiv 2017 zware waarborgen, zoals toestemming van de minister en toetsing door de TIB en een toestemmingsperiode van 3 maanden. Voor metadata geldt dit niet in gelijke mate. Alleen voor analyse van metadata uit OOG-I die gericht is op het identificeren van personen en/of organisaties geldt dat toestemming van de minister en toetsing door de TIB nodig is. De toestemmingsperiode bedraagt echter een jaar. Voor alle overige vormen van (meta)data-analyse gelden deze waarborgen niet. Uit de jurisprudentie van het EHRM (*Big Brother Watch e.a.*, in het kader van bulkinterceptie)[40] en HvJ EU (*Tele2/Watson*, in het kader van (bulk)dataretentie)[41] volgt dat metadata-analyse, waarmee de contacten, bewegingen, internetgeschiedenis en communicatiepatronen van personen in kaart kunnen worden gebracht, een zwaarwegende inmenging in het recht op privacy inhoudt waarvoor voldoende waarborgen noodzakelijk zijn. Een betere regeling is noodzakelijk. Dat versterkt ook de voorzienbaarheid van regelgeving. De jurisprudentie onderkent dit probleem en kiest voor een beoordeling waarbij de impact op de te beschermen belangen voorop staat. In een rechtseenheidsbrief hebben CTIVD en TIB dit probleem al geadresseerd.[42]

***Data-analyses met voorspellend karakter***

Het is ook mogelijk data-analyses uit te voeren die leiden tot een bepaalde voorspelling. Met behulp van technieken als 'profiling' of 'machine learning' is het bijvoorbeeld mogelijk nieuwe targets te onderkennen als personen met een soortgelijk profiel voorkomen in een (of meerdere) dataset(s). De diensten hebben

---

*the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with".* Zie ook HvJ EU 21 december 2016, C 203/15 en C698-15, ECLI:EU:C:2016:970, par. 99 (Tele2 Sverige AB en Watson).

[39] Zie bijlage III bij rapport nr. 64 (2019) over de inzet van de bijzondere bevoegdheid tot selectie door de AIVD en de MIVD. In de zaak *Big Brother Watch t. het Verenigd Koninkrijk* wordt bijvoorbeeld in paragraaf 355 ingegaan op de vraag of IP-adres, URL worden gekwalificeerd als 'inhoud' of 'metadata'.

[40] EHRM 13 september 2018, *Big Brother Watch e.a. t. het Verenigd Koninkrijk*, nrs. 58170/13, 62322/14, 24960/15, ECLI: CE: ECHR: 2018: 0913JUD005817013, par. 356-357 (sinds feb. 2019 aanhangig bij de Grote Kamer).

[41] HvJ EU 21 december 2016, *Tele2 Sverige AB* en *Watson*, C-203/15 en C-698/15, ECLI: EU: C: 2016: 572 en ECLI: EU: C: 2016: 970, par. 99.

[42] Brief van 23 november 2018 van de TIB en de CTIVD over geautomatiseerde data-analyse, *Kamerstukken II* 2018/19, 29924, nr. 174.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

onder andere data-analisten in dienst die op zoek gaan naar nieuwe informatie over targets of onbekende targets via data-analyse, waarbij de wet het ook mogelijk maakt gebruik te maken van data-analyses met een voorspellend karakter.

De wet beperkt deze vorm van data-analyse in het bijzonder door het verbod op het nemen van maatregelen zonder menselijke tussenkomst (artikel 60 lid 3 Wiv 2017). In de toelichting op deze bepaling wordt niet goed duidelijk gemaakt wat wordt bedoeld met 'maatregelen'. Het verbod vindt zijn achtergrond in het risico van stigmatisering en mogelijke discriminatie van individuen of groepen als gevolg van geautomatiseerde besluitvorming. De bepaling is duidelijk geïnspireerd op het verbod tot 'geautomatiseerde besluitvorming' uit de AVG.

Bij probabilistische kansberekening door middel van AI of *machine learning*, bijvoorbeeld door middel van *profiling*, bestaan er risico's zoals *bias* in de datasystemen, discriminatie of stigmatisering. Een verbod op geautomatiseerde besluitvorming vormt hierbij een waarborg. Bij de verwerking van een grote hoeveelheid gegevens die tot in detail het leven van een persoon blootleggen moet aan andere waarborgen worden gedacht, zoals procedures voor de opslag, het vastleggen (inclusief logging) en verantwoording bij data-analyse.

***Naar een betere regeling voor geautomatiseerde data-analyse***
In de Wiv 2017 wordt GDA genormeerd door de algemene bepalingen omtrent gegevensverwerking in artikel 18-24 Wiv 2017 en artikel 50 en 60 Wiv 2017. Het ligt voor de hand een nieuwe bepaling betreffende de bevoegdheid tot GDA (50 en 60 Wiv 2017) op te nemen in de algemene bepalingen omtrent gegevensverwerking. Daarnaast beveelt de CTIVD aan in het bijzonder voor GDA op bulkdatasets in aanvullende waarborgen te voorzien.

Effectief en onafhankelijk toezicht vooraf, tijdens en achteraf de gegevensverwerking is daarbij essentieel. Een onafhankelijke voorafgaande toets voor de inzet van data-analyse is niet altijd goed mogelijk, omdat niet altijd goed van te voren het proces van data-analyse kan worden ingeschat. Voorafgaand en gedurende het gebruik is het wel mogelijk om juist de ontwikkeling van applicaties (op basis van o.a. *machine learning* en *AI*) goed te documenteren en hier verantwoording over af te leggen. De basis hiervoor is een adequaat systeem van interne controle (o.b.v. artikel 24 Wiv 2017), waarbij over elementen als *Responsibility*, *Explainability*, *Accuracy*, *Auditability* en *Fairness* gedurende de ontwikkeling en later tijdens de feitelijke inzet van dergelijke applicaties in het operationeel proces duurzaam verantwoording wordt afgelegd.[43]

De waarborgen dienen volgens de CTIVD daarnaast veel meer in de manier van omgaan met de gegevens te liggen ("behoorlijke en zorgvuldige gegevensverwerking") dan in een vooraf-toets op noodzaak, proportionaliteit en gerichtheid kan worden vormgegeven. Als waarborg denkt de CTIVD aan een toetsingskader (onder meer) gebaseerd op (interne) autorisaties voor de toegang tot applicaties voor data-analyses en voor de toegang tot datasets, als ook logging en interne controle op de verwerkingen. Deze laatste twee elementen zijn ook noodzakelijk voor effectief toezicht. Deze gegevens dienen centraal en eenvoudig voor de toezichthouder beschikbaar te zijn. Bijvoorbeeld aan de hand van *dashboards* en *metrics*. De CTIVD leidt dit soort verplichtingen nu af uit de meer algemene bepalingen omtrent

[43] Deze elementen voor verantwoorde data-analyses zijn afgeleid uit Nicholas Diakopoulos & Sorelle Friedler, 'How to Hold Alorithms Accountable', *MIT Technology Review*, 17 november 2016 en 'A guide to using artificial intelligence in the public sector' van het Alan Turing Institute in het Verenigd Koninkrijk.

gegevensverwerking, maar een algemeen normatief kader voor GDA kan tevens de aspecten duiden die tenminste onderdeel behoren te zijn van een toetsingskader (zoals genoemde interne autorisatiesystemen e.d.).

***Tussenconclusie***

- GDA moet langs twee lijnen beter gereguleerd worden, te weten ten aanzien van risico en inbreuk: (1) data-analyses die een ernstige inbreuk maken op de persoonlijke levenssfeer van personen en (2) data-analyses met een voorspellend karakter die bijdragen aan besluitvorming.
- Effectief en onafhankelijk toezicht tijdens de gegevensverwerking is daarbij essentieel. Een onafhankelijke voorafgaande toets voor de inzet van data-analyse is niet altijd goed mogelijk, omdat niet altijd goed van te voren het proces van data-analyse kan worden ingeschat. Voorafgaand is het wel mogelijk om juist de ontwikkeling van applicaties (op basis van o.a. *machine learning* en *AI*) goed te documenteren en hier verantwoording over af te leggen. De waarborgen dienen volgens de CTIVD daarnaast veel meer in de manier van omgaan met de gegevens (de "behoorlijke en zorgvuldige gegevensverwerking") dan in een vooraf-toets op noodzaak, proportionaliteit en gerichtheid kan worden vormgegeven.
- Bij het – door de CTIVD – na samenspraak met de diensten – uit te werken en vast te stellen toetsingskader moet (onder meer) worden gedacht aan de nadere invulling van interne autorisaties voor de toegang tot applicaties voor data-analyses en voor de toegang tot datasets, logging en interne controle op de rechtmatigheid en kwaliteit van de verwerkingen.

## 6 (Inter)nationale samenwerking

Samenwerking is essentieel en steeds belangrijker voor de bescherming van de nationale veiligheid. De AIVD en de MIVD werken steeds meer en intensiever samen met binnenlandse en buitenlandse partners, in het bijzonder op het gebied van terrorismebestrijding en cyberoperaties en in het kader van militaire missies. Samenwerking is daarbij tweerichtingsverkeer: Het ziet zowel op de verstrekking als het ontvangen van gegevens. In de Wiv 2017 ligt in het normatieve kader de nadruk (nog) op de verstrekking van de gegevens.

De CTIVD geeft in deze paragraaf haar belangrijkste aandachtspunten weer. Graag gaan wij dieper op dit thema in met uw commissie tijdens de geplande verdiepingssessie op 11 september 2020.

***Nationale samenwerking***

De grondslag voor nationale samenwerking kan worden gebaseerd op verschillende bevoegdheden in de Wiv 2017. Zo wordt informatie uitgewisseld op grond van de informantenbevoegdheid, de agentenbevoegdheid of gebaseerd op 'samenwerking met andere instanties' (artikel 91 e.v. Wiv 2017), waarin limitatief de samenwerking met een aantal specifieke (nationale) overheidsorganisaties wordt benoemd.

De CTIVD vindt dat vormen van structurele nationale samenwerking, in het bijzonder waar het betreft overheidsorganisaties, bij voorkeur op één plek in de wet worden samengebracht en wel in een aangepast artikel 91 Wiv 2017.

Door de beperkte huidige reikwijdte van artikel 91 moet nu worden 'uitgeweken' naar de informanten- of agentenbevoegdheid, als het gaat om een structurele verstrekking van gegevensbestanden. Dit is problematisch omdat nu verschillende waarborgenregimes van toepassing zijn, al naar gelang gekozen

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

wordt voor een algemene of bijzondere bevoegdheid. Een uniforme regeling biedt bovendien meer duidelijkheid en doet meer recht aan het inbreukmakende karakter van bepaalde gegevensuitwisseling tussen overheidsinstanties op grond van de algemene bevoegdheid. Een voorbeeld hiervan is het verkrijgen van passagiersgegevens van de Koninklijke marechaussee (Kmar) dat centraal staat in het nog te verschijnen toezichtsrapport over het verzamelen en verder verwerken van passagiersgegevens.

De CTIVD constateert ook dat de AIVD en de MIVD in toenemende mate samenwerken met andere overheidsinstellingen in samenwerkingsverbanden ter bescherming van de nationale veiligheid, bijvoorbeeld op het gebied van (financiering van) terrorisme(bestrijding) en cybersecurity. De gegevensverwerkingen vinden plaats op basis van de bepalingen in de Wiv 2017, maar de CTIVD kan slechts toezicht houden op de gegevensverwerkingen die plaatsvinden door de AIVD en de MIVD. Het komt voor dat in een samenwerkingsverband alle gegevensverwerkingen binnen het kader van de Wiv 2017 worden geplaatst en daarmee onder het toezicht van de CTIVD gebracht (bijvoorbeeld bij de CT-Infobox en de 'Cyber Intel/Info Cel').[44] De vraag dringt zich op in hoeverre gegevensverwerkingen in het belang van de nationale veiligheid door anderen dan de beide diensten, zoals de NCTV, aan bijzonder toezicht – in lijn met dat voor de AIVD en MIVD – onderworpen moeten zijn. In de jurisprudentie en Conventie 108+ wordt immers een generiek nationaal veiligheidsconcept gehanteerd met betrekking tot verwerking van gegevens in het kader van de nationale veiligheid, waarvoor onafhankelijk en effectief toezicht moet zijn ingericht.

***Internationale samenwerking***

Met betrekking tot internationale samenwerking vraagt de CTIVD aandacht voor: 1) het toezichtshiaat bij internationale samenwerking; 2) de eigen interpretatie van het begrip ongeëvalueerde gegevens door de diensten en de onwenselijke gevolgen daarvan en 3) twee overige aandachtspunten bij de samenwerking met buitenlandse partners.

*Toezichtshiaat*

In CTIVD-rapport nr. 56 (2018) over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten maakt de CTIVD duidelijk dat het toezicht van toezichthouders op inlichtingen- en veiligheidsdiensten, ook internationaal gezien vergeleken met andere toezichthouders, in de praktijk is beperkt tot uitsluitend het nationaal niveau. Bij sommige (Europese) toezichthouders op inlichtingen- en veiligheidsdiensten ontbreekt zelfs het mandaat om überhaupt toezicht te houden op internationale samenwerking. Dat wil zeggen dat gemeenschappelijke verwerkingen in een internationaal samenwerkingswerkingsverband buiten Nederland, door de CTIVD niet effectief gecontroleerd kunnen worden. In zoverre is er sprake van een 'toezichtshiaat'. De CTIVD heeft dit tezamen met vier Europese toezichthouders ook geadresseerd in een gezamenlijk statement.[45] De CTIVD werkt samen met internationale toezichthouders, maar heeft geen toestemming van de verantwoordelijk minister gekregen om staatsgeheime informatie over bepaalde onderwerpen te delen. De CTIVD merkt op dat in Conventie

[44] Convenant tussen AIVD, MIVD, Politie, OM, KMar, Belastingdienst, IND, Inspectie SZW, FIU en NCTV inzake de samenwerking in de CT Infobox (Convenant samenwerking CT Infobox 2020), *Stcrt*. 2020, 27315; Convenant tussen AIVD, MIVD, Politie, NSCS, OM en NCTV inzake de samenwerking in de Cyber Intel/Info Cel (Convenant samenwerking CIC), *Stcrt*. 2020, 30702.

[45] Joint Statement: Strengthening Intelligence Oversight Cooperation, 4 november 2018, te raadplegen via https://english.ctivd.nl/documents/publications/2018/11/14/index); Beleidsreactie van de ministers van BZK en Defensie, *Kamerstukken II* 2018/19, 34 588, nr. 82.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

108+ enkele bepalingen staan (zie artikel 16-18) over internationale samenwerking van toezichthouders, ook in het kader van nationale veiligheid. Hieraan dient in wetgeving invulling te worden gegeven.

*Interpretatie begrip 'evalueren van gegevens'*
De CTIVD heeft in rapport nr. 65 verduidelijking en handvatten voor een rechtmatige toepassing van de begrippen 'geëvalueerde' en 'ongeëvalueerde' gegevens geboden.[46] Deze begrippen komen in de Wiv 2017 voor in het kader van samenwerking met buitenlandse diensten, meer specifiek het verstrekken van gegevens aan deze diensten. De CTIVD is – mede op grond van de wetsgeschiedenis - van oordeel dat alleen sprake kan zijn van 'geëvalueerde' gegevens indien de dienst over voldoende feitelijke kennis van de inhoud van de gegevens beschikt dat de dienst weet wat hij geeft. De ministers volgen dit oordeel van de CTIVD niet en vinden dat gegevens 'geëvalueerd' zijn als een relevantiebeoordeling heeft plaatsgevonden (ongeacht de aard van de relevantiebeoordeling en dus of hiermee kennis bestaat van de inhoud van de gegevens).[47] Een dergelijke toepassing van de relevantiebeoordeling leidt tot een uitholling van de bescherming van de fundamentele rechten van de burger.

De ruime toepassing van de AIVD en de MIVD met betrekking tot het relevantiebegrip in artikel 27 Wiv 2017 heeft zichtbare consequenties voor de rechtmatigheid bij het verstrekken van gegevens aan buitenlandse diensten. De diensten hebben bij bepaalde bulkdatasets na het verlopen van de bewaartermijn van anderhalf jaar uit artikel 27 Wiv 2017 een bepaalde relevantietoets uitgevoerd, die de CTIVD als onrechtmatig beoordeeld.[48] Vervolgens worden deze bulkdatasets als gevolg van deze relevantiebeoordeling gedeeld onder de noemer van 'geëvalueerde' gegevens, terwijl deze datasets niet inhoudelijk op gegevensniveau zijn beoordeeld. Bulkdatasets kunnen daarmee zonder toestemming van de minister en zonder meldplicht aan de CTIVD worden verstrekt (zie ook paragraaf 4).

*Overige aandachtspunten*
In de Wiv 2017 bestaat een inconsistentie bij de regeling in artikel 90 (met name lid 3). Indien de AIVD of de MIVD aan een buitenlandse dienst verzoekt een bijzondere bevoegdheid uit te voeren, moet volgens de wet aan de bepalingen van de inzet van een bijzondere bevoegdheid worden voldaan, maar niet aan het toestemmingsregime ten aanzien van de inzet van die bijzondere bevoegdheden. Het verdient overweging voor de inzet van de bepaalde bijzondere bevoegdheden te allen tijde *ex ante* toestemming te vereisen.

De CTIVD zal uw commissie in een verdiepende sessie attenderen op een andere tekortkoming in de artikelen over de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen.

***Tussenconclusie***

- De verstrekking van gegevens door andere overheidsinstanties aan de AIVD en de MIVD in de nationale context behoeft één (consistente) grondslag en passende waarborgen.

---

[46] Toezichtsrapport nr. 65 (2019) van de CTIVD over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, *Kamerstukken II* 2019/20, 29 924, nr. 193 (bijlage).
[47] Beleidsreactie ministers van BZK en Defensie op rapport nr. 65 van 15 oktober 2019, *Kamerstukken II* 2019/2020, 29 924, nr. 193.
[48] CTIVD nr. 66 (2019), Voortgangsrapportage III, *Kamerstukken II* 2019/00, 34 588, nr. 85 (bijlage); Zie ook het nog te verschijnen toezichtsrapport over het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking ervan door de AIVD en de MIVD (2020) en de vierde voortgangsrapportage.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

- De CTIVD kan in nationale samenwerkingswerkingsverbanden in het kader van de nationale veiligheid uitsluitend de rol van en gegevensverwerking door de AIVD en de MIVD op rechtmatigheid toetsen. De vraag dringt zich op, mede door Conventie 108+, of de beperking tot de AIVD en de MIVD nog passend is.
- Toezicht op gezamenlijke gegevensverwerking bij internationale samenwerkingsverbanden is op nationaal niveau niet goed mogelijk. De wet voorziet niet in de mogelijkheid voor de CTIVD om staatsgeheime informatie te delen met andere toezichthouders.
- De diensten houden er een andere interpretatie op na dan de CTIVD met betrekking tot het begrip: 'evalueren van gegevens'. De onrechtmatige toepassing van de relevantiebeoordeling uit artikel 27 Wiv 2017 ten aanzien van bulkdatasets, heeft tot gevolg dat deze sets onder de noemer van 'geëvalueerde' gegevens met buitenlandse diensten kunnen worden gedeeld, zonder toestemming van de minister en meldplicht aan de CTIVD.
- Bij internationale samenwerking als bedoeld in artikel 90 lid 3 ontbreekt de toepassing van de toestemmingsvereisten bij de inzet van bijzondere bevoegdheden.

## 7 Tot slot

De CTIVD heeft in deze brief haar visie op een aantal kernonderwerpen in het kader van de wetsevaluatie uiteengezet. Het gaat om: (1) het normatief kader, (2) toezicht, (3) bulkdatasets, (4) GDA en (5) (inter)nationale samenwerking.

Voor een aantal van deze onderwerpen, en met de afdeling klachtbehandeling, zijn al verdiepende sessies gepland. In deze brief heeft de CTIVD aangegeven het van belang te vinden ook met uw commissie een verdiepingssessie te hebben over de concrete inrichting van het toezicht. De CTIVD is uiteraard beschikbaar om ook op andere onderwerpen een nadere toelichting te geven.

De CTIVD wil haar brief aan uw commissie afsluiten met de kern van haar boodschap:

- Recente ontwikkelingen in de jurisprudentie en internationale verdragen nopen tot een herinrichting van het toezichtstelsel met bindende instrumenten voor de toezichthouders. In de visie van de CTIVD houdt dit een geïntegreerd stelsel van toezicht in met de mogelijkheid voor de CTIVD om een bindend oordeel te geven over de rechtmatigheid van gegevensverwerkingen.

- Er is een toekomstvast normatief kader in de wet nodig. Dit sluit aan bij de werkwijze van de diensten en de bescherming van fundamentele rechten. Na samenspraak met de diensten wordt nadere invulling gegeven aan het normatieve kader. De uitvoering ervan is onderworpen aan het rechtmatigheidstoezicht. In dit verband:

    - Is integrale en consistente wetgeving t.a.v. het verzamelen en verder verwerken van bulkdatasets noodzakelijk. Uitgangspunt hierbij is 'bulk is bulk', ongeacht de wijze van verwerving ervan.

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl

- Dienen de bijzondere bevoegdheid tot geautomatiseerde metadata-analyse (GDA) in artikel 50 en de bevoegdheid tot GDA in artikel 60 te worden geïntegreerd. GDA is een dagelijkse kernactiviteit van de diensten. Dit behoeft regulering in de algemene bepalingen over gegevensverwerking door de diensten.

Hoogachtend,

Dr. N.A.N.M. van Eijk
Voorzitter CTIVD

Mr. drs. K.C. Koese
Secretaris CTIVD

**Bezoekadres**:
Oranjestraat 15 | 2514 JB Den Haag
**T** 070 315 58 20 | **F** 070 318 71 68

**Postadres**:
Oranjestraat 15 | 2514 JB Den Haag
**E** info@ctivd.nl | www.ctivd.nl