Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

De Voorzitter en Leden van de Commissie voor
Binnenlandse Zaken van de Eerste Kamer
Prof. mr. J.W.M. Engels
Binnenhof 22
2513 AA Den Haag

Uw kenmerk

Ons kenmerk
2017/0079

Datum
22 maart 2017

Betreft
Wetsvoorstel Wiv 20..

Geachte heer Engels,

Op 28 oktober 2016 stuurde het kabinet het voorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten naar de Tweede Kamer. Het voorstel is op 14 februari 2017 door de Tweede Kamer aangenomen. Een gewijzigd voorstel van wet is op diezelfde dag aangeboden aan de Eerste Kamer.

De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) geeft hierbij haar visie op het gewijzigde wetsvoorstel, ten behoeve van haar gesprek met de Commissie voor Binnenlandse Zaken van de Eerste Kamer op 28 maart aanstaande. Zij bouwt hierbij voort op haar op 9 november 2016 aan de Eerste en Tweede Kamer toegezonden Zienswijze en op haar Nader Standpunt dat op 30 januari 2017 aan de Tweede Kamer is aangeboden.[1]

De CTIVD beschikt als onafhankelijk toezichthouder over een expertise en deskundigheid die haar goed in staat stelt de inhoud van het wetsvoorstel en de toepassing daarvan in de praktijk op waarde te schatten. In haar visie op het wetsvoorstel staat centraal het antwoord op de vraag of effectief toezicht op de naleving van de nieuwe wettelijke bepalingen goed mogelijk is. Zij gaat daarbij met name in op die onderwerpen waarbij naar haar opvatting nog drempels bestaan, die

[1] Zowel de Zienswijze van de CTIVD op het wetsvoorstel Wiv 20.. als het nader Standpunt zijn beschikbaar op www.ctivd.nl.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

effectief toezicht in de weg kunnen staan. De nadruk hierbij ligt op het onderwerp verantwoorde databeperking.

Uitbreiding van bevoegdheden

Het beeld dat de CTIVD heeft van de reikwijdte van de bestaande bevoegdheden van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), bevestigt de noodzaak van de voorgestelde uitbreiding van die bevoegdheden. Het is van belang dat de diensten blijvend in staat worden gesteld huidige en toekomstige dreigingen tijdig te onderkennen en daarbij ook internationaal samen te werken. Niet alleen veranderingen in de aard en omvang van deze dreigingen, in termen van ernst en waarschijnlijkheid, maar ook de technologische en maatschappelijke ontwikkelingen van de afgelopen jaren spelen daarbij een rol. Communicatiemiddelen en –methoden zijn zowel kwalitatief als in geboden toepassingen sterk verbeterd en zullen zich in de toekomst blijven ontwikkelen. Het wetsvoorstel geeft de AIVD en de MIVD de ruimte met deze ontwikkelingen mee te bewegen. In die zin steunt de CTIVD de voorgestelde uitbreiding van de bevoegdheden en pleit in dit verband tevens voor een spoedige inwerkingtreding van de wet.

Evenwicht

De operationele ruimte die met de uitbreiding van bevoegdheden voor de diensten ontstaat, dient wel in balans te zijn met wettelijke waarborgen die effectieve bescherming bieden tegen misbruik van die bevoegdheden. Het gaat hierbij met name om waarborgen die nu én in de toekomst grondrechten en vrijheden als privacybescherming en vrijheid van meningsuiting in voldoende mate garanderen.

Wettelijke versterking van waarborgen

Het wetsvoorstel heeft gedurende de parlementaire behandeling door de Tweede Kamer op het punt van die waarborgen enkele belangrijke positieve wijzigingen ondergaan, waarmee ook mogelijkheden voor effectief toezicht worden geboden.

1. Zo is voor de diensten een **zorgplicht** geïntroduceerd voor de kwaliteit van de gegevensverwerking, waaronder de toepassing van algoritmen en (gedrags)modellen. Het complexe en grootschalige karakter van geautomatiseerde gegevensverwerkingsprocessen vraagt, gezien de daaraan inherente risico's, om aanvullende waarborgen. Het is van evident belang dat de diensten kunnen garanderen dat geautomatiseerde gegevensverwerkingsprocessen doen wat daarvan wordt verwacht en dat de toezichthouder dit kan toetsen. De genoemde zorgplicht vormt hiervoor een belangrijke waarborg en stelt de CTIVD in staat (systeem)toezicht uit te oefenen op zowel de kwaliteit als de rechtmatigheid van (geautomatiseerde) gegevensverwerkingsprocessen.

2. Ook zijn **aanvullende waarborgen** opgenomen bij de samenwerking met buitenlandse diensten. Zo is wettelijk verankerd dat de verstrekking van gegevens aan buitenlandse diensten plaatsvindt in het kader van een samenwerkingsrelatie, waarvan de aard en intensiteit verbonden is met de uitkomst van een toetsing van eveneens in de wet

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

opgenomen samenwerkingscriteria. Voor verstrekking van gegevens buiten een samenwerkingsrelatie is een uitzonderingsregeling getroffen waarin aanvullende vereisten zijn opgenomen.

Handvatten voor effectief toezicht

Naast deze wettelijke versterking van waarborgen, heeft de regering bovendien voorzien in een nadere uitleg van het wetsvoorstel, zowel in de Nota naar aanleiding van het verslag als tijdens het plenaire debat in de Tweede Kamer en in de schriftelijke reactie van de regering op ingediende amendementen. De CTIVD vindt in deze nadere uitleg, *zoals zij deze verstaat*, handvatten voor effectief toezicht, met name waar het gaat om de verwerving en verdere verwerking van grote hoeveelheden gegevens.

1. De regering heeft herhaaldelijk aangegeven dat het vereiste, dat de inzet van bevoegdheden **'zo gericht mogelijk'** moet zijn, een integraal onderdeel vormt van de al bestaande vereisten van proportionaliteit en subsidiariteit.[2] De door de Tweede Kamer kamerbreed aangenomen motie nr. 66 van het lid Recourt (PvdA)[3] geeft in dit verband nog eens nadrukkelijk aan dat de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit in alle gevallen zo geïnterpreteerd moeten worden en in de praktijk toegepast dienen te worden, dat een zo gericht mogelijke inzet van bevoegdheden plaatsvindt. De CTIVD begrijpt dit aldus dat de diensten (telkens en uit zichzelf) de vraag of de inzet van bevoegdheden niet gerichter kan, gemotiveerd moeten beantwoorden in de verzoeken om toestemming voor die inzet. Ook bij het toezicht op de uitvoering van die inzet is het criterium 'zo gericht mogelijk' daarmee maatgevend. Het toezicht zal zich expliciet op de toepassing van dit criterium kunnen gaan richten.

2. Om invulling te geven aan de eerder genoemde wettelijke **zorgplicht** van de diensten voor de kwaliteit van de gegevensverwerking adviseerde de CTIVD een aantal **instrumenten** in de wet op te nemen,[4] ontleend aan andere wettelijke en verdragsrechtelijke regelingen waaronder de Algemene Verordening Persoonsgegevens.[5] De CTIVD ziet het als een randvoorwaarde dat de diensten niet alleen de verantwoordelijkheid hebben voor de kwalitatief goede inrichting van hun gegevensverwerkingssystemen, maar zelf ook interne controle uitoefenen op de werking daarvan. De naleving van de zorgplicht laat zich moeilijk toetsen indien aan de invulling

---

[2] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 7; Concept verslag plenaire vergadering Tweede Kamer, 8 februari 2017, beschikbaar op www.tweedekamer.nl.
[3] Motie nr. 66 van het lid Recourt (PvdA), *Kamerstukken II* 2016/17, 34 588 nr. 66.
[4] Zienswijze van de CTIVD, bijlage I, p. 25-26, beschikbaar op www.ctivd.nl.
[5] EU Verordening 2016/679 van het Europees Parlement en de Raad van de EU, 27 april 2016, Pb EU L119 d.d. 4 mei 2016. De Verordening is per 25 mei 2018 van toepassing voor de gehele marktsector en overheidssector, m.u.v. de AIVD en MIVD. De uitzondering voor de beide diensten is terug te voeren op artikel 4 van het EU Verdrag dat, kort gezegd, EU recht niet van toepassing verklaart op de nationale veiligheid.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

daarvan geen duidelijk instrumentarium ten grondslag ligt.[6] In navolging van onder meer bovengenoemde Europeesrechtelijke algemene verordening en de Wet politiegegevens kan hierbij gedacht worden aan: een **gegevensbeschermingsbeleid**, **gegevensbeschermingseffectbeoordelingen** en **audits**. Voorkomen moet worden dat de toezichthouder bij het ontbreken van zo'n instrumentarium bij elk verwerkingsproces eerst zelf moet vaststellen op welke wijze invulling moet worden gegeven aan normen van kwaliteit en rechtmatigheid. Dan komt zij niet aan toezicht toe. De regering heeft uitgelegd het niet noodzakelijk te vinden het voorgestelde instrumentarium in de wet op te nemen en dat dit instrumentarium onder de zorgplicht begrepen kan worden geacht.[7] De CTIVD maakt uit deze toelichting op dat zij de genoemde instrumenten in de praktijk expliciet als uitgangspunt kan nemen bij haar toezicht op de (geautomatiseerde) gegevensverwerkingsprocessen van de diensten.

Drempels voor effectief toezicht

Hoewel het wetsvoorstel op bovenstaande onderwerpen lijkt te zijn versterkt en handvatten biedt voor effectief toezicht, voorziet de CTIVD nog een viertal problemen die aan effectief toezicht in de weg kunnen staan. Het gaat om de volgende onderwerpen::

1. Rechtseenheid
2. Toezichtshiaat
3. Overgangsbepaling voor samenwerkingsrelaties
4. Databeperking door onderzoek op relevantie

1. Rechtseenheid

De regering heeft terecht de wenselijkheid uitgesproken van een uniforme en consistente rechtstoepassing tussen de nieuwe toetsingscommissie inzet bevoegdheden (TIB) en de afzonderlijke afdelingen toezicht en klachtbehandeling van de CTIVD. Elk van deze spelers zal zich immers met dezelfde rechtsvragen op één en hetzelfde rechtsterrein bezighouden. De regering wilde hierbij niet zo ver gaan om, als voorgesteld door de CTIVD, het bevorderen van deze rechtseenheid als een wettelijke opdracht aan genoemde instituties in de wet op te nemen. Een en ander zou langs de weg van vrijwilligheid kunnen plaatsvinden. De CTIVD vindt dit een te risicovolle benadering voor zo'n belangrijk onderwerp. Rechtseenheid biedt de burger immers rechtszekerheid in zijn relatie tot de overheid, in het bijzonder in die zaken waarbij die burger geen kennis heeft van de inmenging die de overheid maakt in zijn (grond)rechten, gegeven het heimelijk karakter van die inmenging. Het is daarom van belang, mede t.b.v. de effectiviteit van het toezicht, dat verduidelijkt wordt dat de TIB en de CTIVD de expliciete taak hebben de rechtseenheid te bevorderen.

---

[6] Standpunt van de CTIVD, p. 4-5, beschikbaar op www.ctivd.nl.
[7] Nota van wijziging, *Kamerstukken II* 2016/17, 34 588 nr. 19, p. 6-7; Schriftelijke reactie op amendement nr. 15 van het lid Verhoeven (D66); Concept verslag plenaire vergadering Tweede Kamer, 8 februari 2017, beschikbaar op www.tweedekamer.nl.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

2. Toezichtshiaat

Het wetsvoorstel voorziet niet in de situatie dat de autorisatie van de inzet van bevoegdheden door de TIB en het toezicht door de CTIVD op de uitvoering van die inzet elkaar zullen raken of overlappen. Door de regering is gesteld dat de CTIVD de rechtmatigheid van een door de TIB genomen besluit moet respecteren. Wel kan de CTIVD achteraf vaststellen dat de informatie in de verzoeken die werden voorgelegd aan de TIB onjuist of te beperkt is geweest, respectievelijk dat de verzoeken beter gemotiveerd hadden moeten worden.[8] De situatie kan zich echter voordoen dat het toezicht achteraf de inzet van een bevoegdheid, en daarmee de verleende autorisatie door de TIB, in een andere dan de aanvankelijk veronderstelde operationele context moet plaatsen (bijvoorbeeld vanwege onvoorziene omstandigheden bij de uitvoering). Dientengevolge kan sprake zijn van een fundamenteel andere beoordeling van de rechtmatigheid. Deze benadering wordt door de regering echter, zo lijkt het, als mogelijkheid afgewezen.

Het niet-bindend toezicht achteraf kan meer de breedte en de diepte ingaan dan de toetsing vooraf. De CTIVD zal de inzet van een bijzondere bevoegdheid in de context van de gehele operatie kunnen beoordelen, daarmee de onderliggende gegevens en besluitvormingsprocessen beter kunnen doorgronden en daarover met medewerkers van de diensten kunnen spreken. Die breedte en diepgang is vaak essentieel voor een juiste beoordeling. Het toezicht achteraf op de rechtmatigheid van de inzet van die bevoegdheden moet derhalve niet zonder meer uitgesloten zijn als autorisatie door de TIB eenmaal heeft plaatsgevonden, met name niet wanneer het gaat om een fundamenteel andere beoordeling. Als de CTIVD zich hierover niet meer betekenisvol kan uitspreken, is sprake van een toezichtshiaat en schiet de effectiviteit van het toezicht daarmee tekort. Het voorgaande heeft dus geenszins de strekking het werk van de TIB telkens over te doen. Het zal zich dienen te beperken tot die beoordelingen die er toe doen.

3. Overgangsbepaling voor samenwerkingsrelaties

Zowel in de huidige wet als in het wetsvoorstel is neergelegd dat de AIVD en de MIVD kunnen samenwerken met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen. Of en in welke mate een buitenlandse dienst voor samenwerking in aanmerking komt is afhankelijk van de uitkomst van een weging van samenwerkingscriteria. Dit is in het wetsvoorstel vastgelegd, alsmede de samenwerkingscriteria waaraan moet worden getoetst. In een overgangsbepaling (artikel 166) wordt de invoering van deze systematiek, die onder de huidige wet (Wiv 2002) ook al geldt, gedurende twee jaar na inwerkingtreding uitgesteld. De CTIVD heeft geen rechtvaardiging kunnen vinden voor deze overgangsbepaling.

Enerzijds wordt met het wetsvoorstel beoogd aanvullende waarborgen aan te brengen door onder meer een nu al geldende regeling voor samenwerkingsrelaties, die grotendeels zijn grondslag vindt in de wetsgeschiedenis bij de Wiv 2002, expliciet wettelijk vast te leggen. Anderzijds wordt met de overgangsbepaling de grotendeels al vijftien jaar geldende regeling voor samenwerkingsrelaties met twee jaar uitgesteld. Dit rijmt niet met elkaar. Het heeft tot gevolg dat

---

[8] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 39. Concept verslag plenaire vergadering Tweede Kamer, 8 februari 2017, beschikbaar op www.tweedekamer.nl.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

gedurende twee jaar de AIVD en de MIVD formeel niet verplicht zijn aan de hand van samenwerkingscriteria te bepalen of met een buitenlandse dienst kan worden samengewerkt en op grondslag van welke geconstateerde risico's welke vormen van samenwerking daarbij geoorloofd zijn. Dit leidt ertoe dat van de Wiv 20.. gedurende die twee jaar formeel geen beperkende werking uitgaat op de samenwerkingsrelaties met buitenlandse diensten, een periode waarin het aannemelijk is dat de samenwerking met buitenlandse diensten en de gegevensuitwisseling die in dat kader plaatsvindt juist intensiveert. Hiermee ontstaat niet alleen een aanzienlijk hiaat in de rechtsbescherming van de burger, maar is effectief toezicht op de uitwisseling van gegevens voor twee jaar voor een groot deel uitgesloten. Dit kan, gelet op de geformuleerde uitgangspunten bij het wetsvoorstel, toch niet de bedoeling zijn geweest.

4. Databeperking door onderzoek op relevantie

Onderzoeksopdrachtgerichte interceptie (interceptie in bulk) brengt met zich mee dat grote hoeveelheden gegevens worden verwerkt van personen en organisaties die géén doelwit van de diensten zijn. Dit kan gepaard gaan met een aanzienlijk risico op ongeoorloofde inbreuken op de privacy. Dit risico kan worden beperkt door zorg te dragen voor een "verantwoorde databeperking". De kern hiervan is dat (persoons)gegevens altijd zo gericht mogelijk dienen te worden verworven (zie hiervoor) en dat deze verworven gegevens zo spoedig mogelijk moeten worden gereduceerd tot die gegevens die de AIVD en de MIVD daadwerkelijk nodig hebben om hun taken goed uit te voeren. Om hierin te voorzien, heeft de CTIVD in haar eerdere zienswijze op het wetsvoorstel geadviseerd vijf aanvullende waarborgen in de wet op te nemen.[9]

Volgens de regering echter, is het niet noodzakelijk aanvullende waarborgen op te nemen omdat verantwoorde databeperking al impliciet besloten ligt in het wetsvoorstel. Enerzijds in het proportionaliteitsvereiste (waaronder ook het criterium 'zo gericht mogelijk' moet worden begrepen) en anderzijds in de verplichte uitvoering van het 'onderzoek op relevantie'.[10] De plicht de gegevens op relevantie te onderzoeken is neergelegd in artikel 48 lid 5. Daar staat dat verworven gegevens drie jaar mogen worden bewaard t.b.v. de bevoegdheden van search, metadata-analyse en selectie. En vervolgens dat: "Gegevens waarvan in dat kader is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel enig ander lopend onderzoek vallend onder de taken [...] worden vernietigd. Gegevens die niet op hun relevantie zijn onderzocht, worden na afloop van deze periode vernietigd."

De CTIVD vindt het niet duidelijk op welke wijze dit wetsartikel waarborgt dat verantwoorde databeperking plaatsvindt. Onderzoek op relevantie impliceert dat van een (persoons)gegeven inhoudelijk wordt beoordeeld of het vernietigd dan wel bewaard moet worden t.b.v. het operationeel proces.[11] In het kader van onderzoeksopdrachtgerichte interceptie (bulk) is een inhoudelijke beoordeling van elk verworven gegeven echter niet aan de orde. De hoeveelheid

---

[9] Zienswijze van de CTIVD, bijlage I, p. 6-19, beschikbaar op www.ctivd.nl.
[10] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 74; Concept verslag plenaire vergadering Tweede Kamer, 8 februari 2017, beschikbaar op www.tweedekamer.nl.
[11] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 32.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

gegevens die naar verwachting zal worden verworven, zou een dergelijke beoordeling op inhoud praktisch onuitvoerbaar maken. Maar wat geldt dan wel?

In ieder geval is sprake van het vaststellen van relevantie bij het filteren van gegevens tijdens de interceptie zelf. Het filteren leidt ertoe dat alleen die verworven gegevens worden opgeslagen, waarvan duidelijk is dat deze aan bepaalde kenmerken voldoen. Dit kunnen uiterlijke en technische kenmerken zijn, bijvoorbeeld locatiegegevens, landcodes, een specifieke communicatietoepassing of een specifieke versleuteling die is gebruikt, telefoonnummers of IP adressen.[12] Het filteren zorgt ervoor dat de communicatie die door het filter wordt herkend, wordt opgeslagen en het overige terstond wordt vernietigd. Ook is in het verwerkingsproces sprake van een plicht gegevens terstond te vernietigen als op basis van bijvoorbeeld de bevoegdheid van search wordt vastgesteld dat verworven gegevens *niet* relevant zijn voor een lopend onderzoek. Search is er primair op gericht door het verkennen van de communicatie het verwervingsproces of het selectieproces bij te stellen. Het kan zijn dat men hierbij stuit op gegevens die geen enkele relatie hebben tot een onderzoeksopdracht. Deze gegevens moeten dan terstond vernietigd worden. Deze bijkomstigheid van search wordt de doorlopende vernietigingsplicht genoemd.[13] Het gaat bij zowel het filteren als bij search veelal om technisch complexe processen.

Van belang is hier dat het in deze fasen van verwerving en search niet zozeer gaat om een inhoudelijke, maar meer om een technische beoordeling van de gegevens. Op basis van bijvoorbeeld het type communicatie, de taal waarin de communicatie is gesteld of de locatie waarvan de communicatie afkomstig is, worden gegevens opgeslagen dan wel terstond vernietigd. Uit de toelichting bij het wetsvoorstel blijkt bovendien dat het begrip relevantie in dit kader een andere, ruimere betekenis krijgt. Zo wordt aangegeven dat gegevens niet relevant zijn in de context van het interceptieproces wanneer de gegevens *buiten de kaders van een onderzoeksopdracht vallen* of *op generlei wijze gerelateerd zijn aan onderzoeksopdrachten*.[14] De relatie tot de onderzoeksopdracht is dus een beduidend bredere invulling van het relevantiebegrip en wil zeggen dat gegevens *potentieel* relevant moeten zijn.

Ook bij selectie is sprake van een meer uiterlijke of technische beoordeling van de gegevens. Verworven gegevens die overeenkomen met technische kenmerken (zoals telefoonnummers en e-mailadressen) of met trefwoorden, worden geselecteerd. Dit is een geautomatiseerd proces. De geselecteerde gegevens worden ter beschikking gesteld aan het operationeel team dat belast is met de uitvoering van de onderzoeksopdracht ten behoeve waarvan de selectie heeft plaatsgevonden.

---

[12] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 146. Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 30 en 71.
[13] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 146.
[14] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 146. Verder zijn in de toelichting verwijzingen te vinden naar het vernietigen van in bulk verworven gegevens die *evident niet relevant zijn voor enig onderzoek* (MvT p. 121) en die *niet voor verder onderzoek relevant kunnen zijn* (MvT p. 130).

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

De vraag doet zich voor of ná de fasen van verwerving, search en selectie sprake is van een plicht de verworven (persoons)gegevens inhoudelijk te beoordelen op *daadwerkelijke* relevantie voor een lopend onderzoek. Op dit punt is de toelichting tegenstrijdig. Enerzijds wordt aangegeven dat selectie van gegevens plaatsvindt met het oogmerk van de inhoud kennis te nemen en deze vervolgens op relevantie te toetsen voor het onderzoek ten behoeve waarvoor de selectie heeft plaatsgevonden.[15] Anderzijds wordt opgemerkt dat de doorlopende vernietigingsplicht van gegevens die niet gerelateerd kunnen worden aan de onderzoeksopdrachten de laatste slag van databeperking vormt,[16] hetgeen lijkt in te houden dat geen nadere inhoudelijke relevantiebeoordeling plaatsvindt. Ook wordt toegelicht dat geselecteerde gegevens reeds als 'geëvalueerd', dat wil zeggen relevant, kunnen worden beschouwd.[17] Dit zou betekenen dat alle geselecteerde gegevens bewaard en gebruikt kunnen worden, zonder dat hieraan een inhoudelijke beoordeling op *daadwerkelijke* relevantie ten grondslag ligt. Het gaat hier nog steeds om grote hoeveelheden (persoons)gegevens.

De onduidelijkheden over het onderzoek op relevantie zijn problematisch om twee redenen:

a. Het leidt tot een verschil in waarborgen voor gegevensvernietiging, en daarmee in de mate van rechtsbescherming van de burger, bij de verwerking van gegevens die zijn verzameld door de inzet van bijzondere bevoegdheden.

   Wanneer met een gerichte bevoegdheid, bijvoorbeeld een telefoontap, een e-mailtap of een hack, communicatie wordt verworven, moeten de diensten binnen een jaar inhoudelijk beoordelen of de verworven (persoons)gegevens daadwerkelijk relevant zijn voor het onderzoek waarvoor ze zijn verzameld of enig ander lopend onderzoek van de dienst (artikel 27 lid 1).[18] Het gaat hier om een belangrijke waarborg voor de bescherming van grondrechten: Slechts gegevens die inhoudelijk *daadwerkelijk* relevant zijn, mogen worden bewaard. Dit is anders wanneer de gegevens worden verworven door inzet van interceptie in bulk en worden geselecteerd. Het kan hierbij gaan om exact dezelfde communicatie via exact hetzelfde telefoonnummer of e-mailadres als bij de gerichte inzet. Voor diezelfde gegevens die slechts langs een andere weg verworven zijn, geldt in het wetsvoorstel nu een ander beschermingsregime. Niet meer geldt de garantie dat een inhoudelijke beoordeling plaatsvindt. Alle (gerelateerde) *potentieel* relevante gegevens kunnen worden bewaard.

b. Het staat effectief toezicht in de weg.
   De regering heeft bij herhaling verwezen naar het belang van toezicht in het bepalen van de grenzen van de proportionaliteit van de toepassing van onderzoeksopdrachtgerichte

---

[15] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 142.
[16] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 146; Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 72.
[17] Memorie van toelichting, *Kamerstukken II* 2016/17, 34 588 nr. 3, p. 214.
[18] Nota naar aanleiding van het verslag, *Kamerstukken II* 2016/17, 34 588 nr. 18, p. 32.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | **F** 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl

interceptie (interceptie in bulk). Benadrukt wordt dat de komende jaren rechtsvorming zal moeten plaatsvinden en dat de toezichthouder de kaders werkendeweg nader zal moeten invullen.[19] De proportionaliteit (en daarmee de rechtmatigheid) van de toepassing van onderzoeksopdrachtgerichte interceptie en de daarop volgende verwerking, is voor een belangrijk deel afhankelijk van de mate waarin gegevens worden vernietigd die niet relevant zijn voor de taakuitvoering van de diensten. Om effectief toezicht uit te kunnen oefenen, is het echter van groot belang dat vanaf het moment dat de wet in werking treedt helder is wat die relevantie inhoudt, wat de diensten moeten doen om die relevantie te beoordelen en wanneer dit moet leiden tot vernietiging van gegevens. Zonder die duidelijkheid, zonder heldere normen, heeft het toezicht onvoldoende handvatten te kunnen toetsen of bepaalde verworven gegevens (terstond) vernietigd hadden moeten worden.

Om voorgaande redenen is het essentieel dat de betekenis van het begrip onderzoek op relevantie verduidelijkt wordt. In de fasen van verwerving, search en selectie, is het onderzoek op relevantie erop gericht aan de hand van uiterlijke en technische kenmerken te bepalen welke verworven gegevens *gerelateerd zijn aan de onderzoeksopdrachten* en dus van *potentiële waarde* zijn voor enig lopend onderzoek van de diensten. Niet te relateren gegevens dienen terstond te worden vernietigd. Nadat aldus selectie heeft plaatsgevonden, dient het onderzoek op relevantie erop te zijn gericht op basis van de inhoud van de geselecteerde gegevens te beoordelen of de gegevens *daadwerkelijk van waarde* zijn voor enig lopend onderzoek. Gegevens die in dit verband niet van waarde zijn, dienen terstond te worden vernietigd. Slechts indien door de regering díe verduidelijking wordt gegeven aan de plicht gegevens op relevantie te onderzoeken, wordt gewaarborgd dat verantwoorde databeperking plaatsvindt en dat a) voor verzamelde gegevens, ongeacht de wijze waarop de verzameling heeft plaatsgevonden, dezelfde waarborgen voor gegevensvernietiging gelden en b) effectief toezicht hierop mogelijk is.

Tot slot

De CTIVD is zich ervan bewust dat de onderwerpen die zij bespreekt wellicht niet eenvoudig te doorgronden zijn. Zoals zij ook in de Zienswijze heeft aangeven is de materie soms simpelweg complex. De CTIVD ziet ernaar uit de inhoud van deze brief nader toe te lichten in het gesprek van 28 maart aanstaande.

Hoogachtend,

b.a.

Mr. H.N. Brouwer
voorzitter CTIVD

Mr. H.T. Bos-Ollermann
secretaris CTIVD

[19] Concept verslag plenaire vergadering Tweede Kamer, 8 februari 2017, beschikbaar op www.tweedekamer.nl.

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 - 315 58 20 | F 070 - 381 71 68
E info@ctivd.nl | www.ctivd.nl