

Vergaderjaar 2016–2017

**34 588**

## **Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)**

**E**

### **NADERE MEMORIE VAN ANTWOORD**

Ontvangen 9 juni 2017

#### **1. Algemeen**

De leden van de fracties van de SP, PvdA en GroenLinks geven aan nog een aantal nadere c.q. aanvullende vragen te hebben. Op deze vragen ga ik graag, mede namens de Minister-President, Minister van Algemene Zaken, de Minister van Defensie en de Minister van Veiligheid en Justitie, in. Ik houd daarbij de volgorde van het nader voorlopig verslag aan. Waar dat dienstig wordt geacht zijn vragen samengenomen en antwoorden gebundeld.

#### **2. De verwerking van gegevens door de diensten**

De leden van de fracties van de SP, GroenLinks en de PvdA hebben een aantal vragen in verband met verantwoorde databeperking. Zij vragen of voor onderzoeksoopdrachtgerichte interceptie een andere norm met betrekking tot de toets op relevantie bestaat dan voor gerichte interceptie. Voor beide vormen van interceptie geldt dezelfde norm, namelijk dat de gegevens op relevantie dienen te worden onderzocht ten behoeve van de bruikbaarheid in het onderzoek. De wijze waarop die toets op relevantie plaatsvindt verschilt. Bij gerichte interceptie is sprake van reeds onderkende targets, terwijl onderzoeksoopdrachtgerichte interceptie zich ook richt op het onderkennen van netwerken en ongekennde dreigingen en daarmee op nog niet geïdentificeerde targets. Dat brengt een andere wijze van werken met zich mee, die in de artikelen 48 tot en met 50 van het wetsvoorstel is neergelegd. Gerichte interceptie dient gegevens over en van het specifieke target op te leveren, waarna de relevantie per verkregen gegeven kan worden bepaald. Onderzoeksoopdrachtgerichte interceptie daarentegen levert een bredere dataset op. De relevantie van gegevens in die dataset wordt bepaald door de combinatie van het bepalen van de specifieke datastroom, de negatieve en positieve filtering alsmede tot slot de selectie van gegevens. Zowel de gegevens die zijn verkregen door de inzet van gerichte interceptie als die welke zijn verkregen door onderzoeksoopdrachtgerichte interceptie worden vernietigd indien blijkt dat deze niet relevant zijn voor het onderzoek waar ze voor

verworven zijn, of enig ander lopend onderzoek. Gegevens die relevant zijn mogen worden bewaard ten behoeve van onderzoek. Gegevens die niet binnen de daartoe gestelde termijn op relevantie zijn onderzocht, dienen na afloop van die termijn terstond te worden vernietigd. De zo gericht mogelijke inzet van onderzoeksopdrachtgerichte interceptie wordt gewaarborgd doordat in het verzoek om toestemming voor de uitoefening van deze bevoegdheid nadrukkelijk de noodzakelijkheid, proportionaliteit, subsidiariteit dient te worden beargumenteerd, alsmede hoe invulling wordt gegeven aan het daarin besloten liggende criterium van een zo gericht mogelijke inzet, zoals verwoord in de door de Tweede Kamer aangenomen motie Recourt. Het is allereerst aan de Minister om te beoordelen of op een adequate wijze invulling is gegeven aan de gestelde criteria; indien de Minister overgaat tot het verlenen van toestemming voor de inzet van de bevoegdheid, wordt deze toestemming voor een rechtmatigheidstoets voorgelegd aan de onafhankelijke TIB.

De leden van de fracties van de SP, GroenLinks en de PvdA vragen of het klopt dat de diensten metadata mogen bewaren als deze niet op basis van negatieve filtering zijn uitgesloten, zonder dat hierop positieve filtering en selectie worden toegepast. Dat is inderdaad het geval. De met de uitoefening van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie verkregen metadata die resteren na negatieve filtering, mogen ten hoogste drie jaar worden bewaard. Gedurende deze periode worden deze gegevens onderworpen aan vormen van (geautomatiseerde) data-analyse, waardoor – in relatie tot een onderzoeksopdracht en met inachtneming van de voor verwerking van gegevens geldende criteria – gegevens beschikbaar kunnen komen die vervolgens op relevantie ten behoeve van het desbetreffende onderzoek, of enig ander lopend onderzoek, kunnen worden getoetst. Zowel voor metadata als voor gegevens betreffende de inhoud van de communicatie geldt dat alleen gegevens die relevant zijn bevonden voor enig lopend onderzoek mogen worden bewaard. Gegevens die binnen de wettelijk vastgelegde bewaartermijn niet op relevantie zijn onderzocht of niet relevant zijn geacht, worden terstond vernietigd. De bijzondere bevoegdheid tot onderzoeksopdrachtgerichte interceptie brengt onvermijdelijk met zich mee dat ook gegevens worden verworven die betrekking hebben op personen die niet in onderzoek zijn van de dienst(en) en daarvoor ook niet in aanmerking komen. Zowel aan de voorkant van het proces (formulering van het verzoek om toestemming en de zo gericht mogelijke inzet) als in het proces na verwerving worden niet relevante gegevens uit de dataset gehaald. Door de combinatie van het bepalen van de specifieke datastroom, de negatieve en positieve filtering alsmede tot slot de selectie van gegevens wordt gewaarborgd dat geen sprake is van het op grote schaal inbreuk maken op de privacy van personen die zelf geen onderwerp van onderzoek zijn. Voor metadata en inhoudgegevens gelden dezelfde normen en is er dus geen sprake van een lagere selectiestandaard voor metadata, zoals wordt gesteld in de vragen van de fracties van de PvdA en GroenLinks. Zoals in de kabinetsreactie op het rapport van de Commissie Evaluatie Wiv 2002 (commissie-Dessens) al is aangegeven, is naar het oordeel van het kabinet het onderscheid tussen inhoud (content) en niet-inhoud (metadata) niet het enige bepalende element bij het vaststellen van de ernst van de inbreuk op de privacy. Evenzeer is van belang de schaal waarop gegevens worden verzameld en hoe ingrijpend de gehanteerde ontsluitingsmethodiek is voor de privacy van de burger.<sup>1</sup>

De leden van de fracties van de SP, GroenLinks en de PvdA vragen om uitleg inzake de heimelijke, vrijwillige medewerking van een aangezochte partij bij het vergaren van gegevens uit een gegevensbestand. Bij de

<sup>1</sup> Kamerstukken II 2013/14, 33 820, nr. 2, blz. 4.

bevoegdheid van artikel 39 om informanten te raadplegen is sprake van het bevragen van reeds bij andere personen of instanties berustende gegevens, zij het dat die voor een ander doel zijn vergaard dan voor de werkzaamheden van inlichtingen- en veiligheidsdiensten in het kader van de nationale veiligheid. Het bevragen van gegevensbestanden bij derden is dan ook als minder ingrijpend middel te kenmerken, dan wanneer bijzondere bevoegdheden dienen te worden ingezet om deze gegevens langs andere weg te vergaren. De reeds bij de betreffende derde (informant) beschikbare gegevens worden, indien deze daartoe op vrijwillige basis medewerking verleent, voor een ander doel beschikbaar gesteld. Ik merk op dat de uitoefening van elke bevoegdheid tot gegevensverzameling, dus ook het verzoek ex artikel 39, moet voldoen aan de algemene eisen die zijn gesteld aan de gegevensverwerking zoals gesteld in paragraaf 3.1 van het wetsvoorstel, als aan de eisen die meer specifiek aan de verzameling van gegevens zijn gesteld in paragraaf 3.2.1 van het wetsvoorstel. Dat betekent dat er altijd sprake moet zijn van een bevraging voor een bepaald, vooraf vastgesteld doel, en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de wet. Tevens moet worden voldaan aan de vereisten van proportionaliteit en subsidiariteit en geldt ingevolge artikel 19, derde en vierde lid, dat de verwerking van persoonsgegevens wegens iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven slechts plaatsvindt in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is. Het opvragen van dergelijke gegevens louter vanwege die bijzondere kenmerken is dus niet geoorloofd. Tot slot kan de CTIVD toezicht houden op de feitelijke uitvoering van deze bevoegdheid.

De leden van de SP-fractie wijzen erop dat de regering heeft aangegeven dat de bevraging van gegevens via real time toegang tot gegevensbestanden gericht plaatsvindt op hit/no hit basis. Zij vragen of de regering kan bevestigen dat de diensten uitsluitend deze gerichte bevragingmethode toepassen en niet volledig toegang krijgen tot alle gegevens in de gegevensbestanden.

In antwoord hierop kan ik bevestigen dat de bevraging van gegevens via *real time* toegang tot gegevensbestanden (rechtstreeks geautomatiseerde toegang) gericht plaatsvindt op hit/no hit basis. Door de diensten ingevoerde gegevens worden vergeleken met de gegevens bij de desbetreffende verantwoordelijke voor de gegevensverwerking. Is er sprake van een hit dan kunnen de daaraan gerelateerde gegevens aan de diensten worden verstrekt; het bestaan van een rechtstreeks geautomatiseerde toegang brengt immers geen plicht tot verstrekking met zich mee en de verantwoordelijke kan derhalve altijd een verstrekking tegenhouden.<sup>2</sup> Wanneer de diensten rechtstreeks geautomatiseerde toegang tot gegevensbestanden wordt verleend, zorgen functiescheiding en autorisatie ervoor dat slechts een beperkte groep medewerkers toegang tot de gegevens krijgt.

Gegevensbestanden die aan de diensten zijn verstrekt – hierbij is dus geen sprake van rechtstreeks geautomatiseerde toegang – kunnen ook op andere wijzen worden bevroegd. In dat kader kan worden gedacht aan analysemethoden die zijn gericht op het snel zicht krijgen op een netwerk. Hierbij moet worden voldaan aan de algemene eisen die zijn gesteld aan de gegevensverwerking zoals gesteld in de wet. De uitvoering van bevoegdheden valt onder het toezicht van de CTIVD.

De leden van de SP-fractie vragen of de recente berichtgeving inzake de Wannacry-software iets aan het Nederlandse standpunt inzake het gebruik van onbekende kwetsbaarheden door inlichtingen- en veiligheidsdiensten

<sup>2</sup> Kamerstukken II 2016/17, 34 588, nr. 3, blz. 58.

heeft veranderd. Dit is niet het geval. De vraag of de Nederlandse inlichtingen- en veiligheidsdiensten een andere afweging zouden hebben gemaakt dan die welke de berichtgeving over de Verenigde Staten veronderstelt, kan ik niet beantwoorden, daar ik niet op de hoogte ben van de specifieke feiten van het geval. Voor de Nederlandse situatie geldt het standpunt inzake het beperken van de omgang met onbekende kwetsbaarheden, zoals neergelegd in de brief van 8 november 2016 (Kamerstukken II 2016/17, 26 643, nr. 428).

De leden van de fracties van de SP en GroenLinks hebben gevraagd naar de omgang met onbekende kwetsbaarheden en of er een (interne) richtlijn bestaat voor het mogen achterhouden van kwetsbaarheden en de termijn die daaraan gebonden is. Over de feitelijke omgang met kwetsbaarheden door de inlichtingen- en veiligheidsdiensten kan in het openbaar geen verdere mededeling worden gedaan. Met betrekking tot de vraag over de richtlijn heb ik naar aanleiding van een aanbeveling van de CTIVD ter zake in haar toezichtsrapport nr. 53 aangegeven dat deze zal worden opgesteld.<sup>3</sup> Momenteel wordt hieraan gewerkt.

De leden van de SP-fractie vragen of de voorafgaande toetsing voor het mogen gebruiken en achterhouden van kwetsbaarheden bij de TIB kan worden belegd.

Voor de beantwoording van deze vraag is het onderscheid tussen gebruiken en achterhouden van kwetsbaarheden relevant. Waar het gaat om het *gebruiken* van kwetsbaarheden merk ik het volgende op. De bevoegdheid tot het binnendringen van een geautomatiseerd werk is een bijzondere bevoegdheid waarvoor toestemming van de voor de dienst verantwoordelijke Minister is vereist en aansluitend – voorafgaand aan de daadwerkelijke uitoefening ervan – een bindende rechtmatigheidstoets door de TIB plaatsvindt. Voor zover bij de uitoefening van deze bevoegdheid gebruik wordt gemaakt van een kwetsbaarheid zal daarvan in het verzoek om toestemming blijken, evenals van de technische risico's die daaraan verbonden zijn. Dat betekent dat dit ook in de rechtmatigheidstoets van de TIB kan worden betrokken.

Waar het gaat om het *achterhouden* van kwetsbaarheden – bedoeld zal zijn: het niet melden daarvan – merk ik op dat dit niet een aspect is dat is verbonden aan de uitoefening van een bijzondere bevoegdheid in een concreet geval en derhalve ook niet in een verzoek om toestemming aan de orde zal komen en reeds om die reden niet aan een voorafgaande toets door de TIB is onderworpen. Omtrent de omgang met door de diensten geconstateerde kwetsbaarheden in het kader van de uitvoering van een wettelijke bevoegdheid ben ik in de memorie van antwoord reeds ingegaan; voorts verwijs ik naar hetgeen ik hiervoor reeds – onder verwijzing naar het kabinetsstandpunt ter zake – heb gesteld.<sup>4</sup>

De leden van de fracties van de SP en GroenLinks hebben gevraagd naar de reikwijdte van de onderzoeksopdrachtgerichte interceptie. Ik hecht eraan onderscheid te maken tussen de wijze van formulering van de onderzoeksopdracht, die geen relatie heeft tot een concrete inbreuk op de privacy, en het verzoek om toestemming, waarbij verzocht wordt om de inzet van onderzoeksopdrachtgerichte interceptie. Dit verzoek onderscheidenlijk de verleende toestemming dient door de Minister onderscheidenlijk de TIB te worden getoetst aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De CTIVD kan op de uitvoering van de bijzondere bevoegdheid toezicht houden. De voorbeelden die de fractie noemt zijn voorstelbare onderdelen van de weging. Zo kan bijvoorbeeld geografie in het ene geval een relevante beperkende factor zijn en in het

<sup>3</sup> Kamerstukken II 2016/17, 29 924, nr. 149.

<sup>4</sup> Kamerstukken I 2016/17, 34 588, nr. C, blz. 12.

andere geval niet. Ik acht de formulering van nadere criteria daarom niet wenselijk; een en ander is immers contextafhankelijk.

De leden van de PvdA-fractie vragen de regering uiteen te zetten hoe de TIB de veiligheidsrisico's enerzijds en anderzijds de noodzaak, evenredigheid en subsidiariteit van grootschalige, abstract aangeduide en technisch complexe operaties zodanig goed kan inschatten dat zij daadwerkelijk de rol kan vervullen die haar in het wetsvoorstel wordt toebedeeld.

De wettelijke rol van de TIB bestaat uit het (bindend) toetsen op rechtmatigheid van een door de Minister verleende toestemming voor de uitoefening van een bijzondere bevoegdheid voorafgaand aan de daadwerkelijke uitoefening daarvan. Het behoort – anders dan de leden van deze fractie veronderstellen – niet tot de taak van de TIB om de veiligheidsrisico's in relatie tot de noodzaak, proportionaliteit en subsidiariteit van grootschalige, abstract aangeduide en technisch complexe operaties – die immers meer omvat dan alleen de inzet van bijzondere bevoegdheden – in te schatten. Een dergelijke inschatting behoort tot de operationele verantwoordelijkheid van de diensten en de daarvoor verantwoordelijke ministers. In de praktijk zal deze inschatting aan de orde komen bij de vraag of een bepaalde bijzondere bevoegdheid voor uitoefening in aanmerking komt gelet op de operationele, veiligheidsrisico's die daaraan verbonden zijn; dat is een andere afweging dan die waarvoor de TIB zich gesteld ziet, die immers de rechtmatigheid toetst indien – naar aanleiding van de hiervoor geschetste afweging – tot de uitoefening van een bijzondere bevoegdheid is besloten.

Met de recente beantwoording van de motie Schouten<sup>5</sup> is het budget ten aanzien van de CTIVD en TIB vergroot. Zoals nu voorzien is dit budget voldoende om de afdeling Klachtbehandeling van de CTIVD en de TIB op te richten, de huidige CTIVD te versterken en hen zo in staat te stellen hun wettelijke taken te vervullen. Mocht na inwerkingtreding van de nieuwe wet op de inlichtingen- en veiligheidsdiensten anders blijken, dan zal de Minister-President hierover het gesprek met de voorzitters van beide commissies aangaan.

De leden van de PvdA-fractie vragen, naar aanleiding van de uitleg van de motie van het voormalige Tweede Kamerlid Recourt, waaruit kan blijken dat het gebruik van de genoemde wettelijke criteria leidt tot een zo gericht mogelijke inzet van bevoegdheden.

Dit zal dienen te blijken uit het verzoek om toestemming tot de inzet van een bevoegdheid en uit de verslaglegging omtrent de uitoefening daarvan.

De leden van de PvdA-fractie vragen hoe de CTIVD de naleving van de zorgplicht kan toetsen als aan de invulling daarvan geen duidelijk instrumentarium ten grondslag ligt. Naar mijn oordeel is geen sprake van de veronderstelde onduidelijkheid. Ingevolge de zorgplicht dragen de hoofden van de diensten er zorg voor dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens deze wet is bepaald. Tot de maatregelen, bedoeld in artikel 24, eerste lid, behoren in ieder geval de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt alsmede ter bevordering van de kwaliteit van de gegevensverwerking, waaronder begrepen de daarbij gehanteerde algoritmen en modellen, de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking alsmede de aanwijzing van

<sup>5</sup> Kamerstukken II, 2016/17, 34 588, nr. 67.

personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens. Deze maatregelen hebben en zullen hun beslag krijgen in beleid, instructies alsmede technische en organisatorische voorzieningen en zijn aldus kenbaar voor de CTIVD. De CTIVD hoeft dus niet zelf het kader vast te stellen, maar kan toetsen aan het hierboven geschetste geheel van normen.

### **3. Toezicht, klachtbehandeling en behandeling van de meldingen van vermoedens van misstanden**

De leden van de SP-fractie vragen of – kort gezegd – artikel 114 van het wetsvoorstel de mogelijkheid biedt voor een actio popularis. Het antwoord hierop luidt bevestigend.

### **4. Grondrechtelijke en mensenrechtelijke aspecten**

De leden van de GroenLinks-fractie wijzen erop dat vanuit het maatschappelijk middenveld veel kritiek is gekomen op het wetsvoorstel. Zij wijzen – onder verwijzing naar een concept-dagvaarding – erop, dat onder meer de Nederlandse Vereniging van Journalisten (NVJ), de Nederlandse vereniging van Strafrechtadvocaten (NVSA), de Stichting Platform Bescherming Burgerrechten en de Stichting Privacy First herhaaldelijk hebben aangegeven dat als het voorliggende wetsvoorstel wordt aangenomen dit een forse aantasting van het recht op privacy en andere fundamentele burgerrechten zal betekenen. Deze leden vragen hoe de regering – los van de concept-dagvaarding – de fundamentele bezwaren en de juridische bedenkingen die deze coalitie aandraagt, beoordeelt. Allereerst merk ik op dat ik in dit kader afzie van een reactie op de onderscheiden punten in de concept-dagvaarding. Mocht dit concept worden omgezet in een concrete dagvaarding, dan zal de Staat daar te zijner tijd op reageren. Wel wil ik in algemene zin reageren. Het moge duidelijk zijn dat ik de door de coalitie van NGO's aangevoerde fundamentele bezwaren en juridische bedenkingen niet deel. Alle door deze coalitie aangevoerde onderwerpen waarop hun bezwaren en bedenkingen betrekking hebben, zijn in het wetgevingsproces – internetconsultatie, advisering Afdeling advisering van de Raad van State en nader rapport aan de Koning, de parlementaire behandeling – aan de orde gesteld en op vragen en opmerkingen ter zake is door de regering uitvoerig gereageerd. Gelet hierop zou ik hier willen volstaan met een verwijzing naar hetgeen in de schriftelijke en mondelinge parlementaire behandeling van het wetsvoorstel tot nu toe is gewisseld. Het onderhavig wetsvoorstel – ook waar het gaat om de door de opstellers van de concept-dagvaarding aangehaalde onderdelen van de Wiv – voldoet naar mijn oordeel aan de daaraan te stellen eisen, zoals deze voortvloeien uit de Grondwet en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Een eventuele rechterlijke toets daarvan zie ik met vertrouwen tegemoet.

In antwoord op de vragen van de leden van de GroenLinks-fractie over het systeem van nummerherkenning kan ik uw Kamer melden dat het onderzoek daartoe is opgezet. Met de Nederlandse Orde van Advocaten is contact gelegd en binnenkort vindt overleg plaats. Wat betreft de vraag over de verhouding van de gevolgen van de indirecte tap tot de wettelijke geheimhoudingsplicht acht ik deze met de voorliggende wettelijke regeling in balans. Ik wijs hierbij op artikel 27, tweede lid, waarin is opgenomen dat gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt en verkregen zijn door de uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5 in andere gevallen als bedoeld in artikel 30, derde lid, terstond

worden vernietigd, tenzij de verdere verwerking van de gegevens noodzakelijk is voor het onderzoek in het kader waarvan de gegevens zijn verworven en de rechtbank Den Haag daartoe toestemming heeft verleend.

## **5. Overig**

De leden van de PvdA-fractie vragen wat de stand van zaken is betreffende de met dit wetsvoorstel samenhangende lagere regelgeving. Ik antwoord daarop graag als volgt. Alle voor de invoering van de nieuwe wet benodigde uitvoeringsregelgeving is in concept gereed. Na aanvaarding van het wetsvoorstel door de Eerste Kamer zullen de concept-regelingen (zowel algemene maatregelen van bestuur als ministeriële regelingen) verder in procedure worden gebracht.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,  
R.H.A. Plasterk