

Aan de voorzitter van de Tweede Kamer der
Staten-Generaal
Mevrouw dr. K. Arib
Postbus 20018
2500 EA DEN HAAG

Onderwerp
Wetsvoorstel Wet op de inlichtingen-
en veiligheidsdiensten 20.. (34 588)

Datum
3 februari 2017
Ons kenmerk
2017/0005/AvD/JB/LR

Geachte mevrouw Arib,

Op 17 januari 2017 is de Nota naar aanleiding van het verslag (hierna: Nota) over het voorstel voor een nieuwe wet op de inlichtingen- en veiligheidsdiensten en enkele andere wetten' (Wiv) aan uw commissie toegezonden. Het betoog van de regering in de Nota biedt op diverse punten een zeer gewenste verduidelijking in de precieze strekking van sommige bepalingen in het wetsvoorstel. De daarbij gevoegde Nota van wijziging (NvW) bevat ook een aantal verbeteringen in de tekst van het voorstel. Daarmee zijn evenwel de mensenrechtelijke knelpunten en zorgen eerder door het College - en ook door de Afdeling advisering van de Raad van State, de CTIVD en de Autoriteit Persoonsgegevens - zijn gesignaleerd, geenszins volledig weggenomen. In deze brief wil het College een aantal belangrijke resterende knelpunten en onduidelijkheden onder uw aandacht brengen.

Een opmerking vooraf: Waardering voor de Nota van wijziging, die zorgt voor versterking van de waarborgen

Hoewel het College een aantal belangrijke zorgen blijft houden ten aanzien van het wetsvoorstel, constateert het dat de Nota van wijziging wel reeds versterking biedt van de in het wetsvoorstel voorziene mensenrechtelijke waarborgen. Dit vooral vanwege de invoering van een zorgplicht voor de geautomatiseerde gegevensverwerking door de diensten (in art. 24, tweede lid, onderdeel a) en vanwege de aanvulling van de wegingscriteria bij het aangaan van een samenwerkingsrelatie met buitenlandse diensten (in art. 88, derde lid).

Overigens rijst bij de opname van het criterium in art. 88, derde lid, onder e (het door de betreffende dienst geboden niveau van gegevensbescherming) wel de vraag welke consequenties deze zeer terecht in de wet opgenomen eis heeft voor gegevensuitwisseling met de diensten van de VS, nu president Trump recentelijk alle overheidsdiensten heeft gedecreteerd geen bescherming op grond van de

Amerikaanse Privacy Act te bieden aan buitenlandse onderdanen. Dit decreet lijkt te duiden op een volledig of in ieder geval grotendeels ontbreken van een gegevensbeschermingsregime in de VS ten aanzien van persoonsgegevens die betrekking hebben op niet-onderdanen.

Een andere vraag die rondom dit onderwerp rijst is waarom de inwerkingtreding van deze eis door de overgangsrechtelijke bepalingen in het wetsvoorstel met twee jaar wordt uitgesteld. Zoals ook in het recent aan u toegezonden standpunt van de CTIVD (in vervolg op haar eerdere zienswijze over het wetsvoorstel) is opgemerkt, ontstaat hierdoor een (tijds)gat in de rechtsbescherming waarvoor geen goede rechtvaardiging gegeven is.

Knelpunten en onduidelijkheden

1. De TIB is goed, maar niet voldoende

Anders dan de afdeling advisering van de Raad van State waardeert het College het invoegen van een toets door de Toetsingscommissie Inzet Bevoegdheden (TIB) onmiddellijk na de ministeriële toestemmingsverlening voor de inzet van de meest ingrijpende en omvangrijke bijzonder bevoegdheden van de diensten als een positief punt van het voorliggende wetsvoorstel. De bezwaren van de Afdeling advisering, die in het Verslag onder meer zijn aangehaald door de VVD-fractie, dat toetsing door de TIB zich niet zou verhouden met de ministeriële verantwoordelijkheid voor het optreden van de diensten, vindt het College niet overtuigend. Terecht wijst de regering er in de Nota op dat toetsing door de TIB van de toestemmingverlening voor de inzet van bijzondere bevoegdheden niets afdoet aan de ministeriële verantwoordelijkheid voor de beleidsmatige afweging om de diensten op een bepaald terrein al dan niet een onderzoek te laten verrichten. In die zin verschilt de positie van de ministers ten opzichte van de diensten niet van die van de Minister van Veiligheid en Justitie die ten opzichte van de Kamer verantwoordelijk is voor het verrichten van opsporingsonderzoeken door de politie waarbij gebruik gemaakt wordt van bijzondere opsporingsmethoden die rechterlijke autorisatie vereisen.

De positieve waardering voor invoeging van de toetsing door de TIB betekent echter niet dat daarmee het toezicht op de diensten in zijn geheel voldoende stevig is vormgegeven. Zoals reeds door vele anderen is opgemerkt biedt de **toetsing door de TIB slechts een beperkte waarborg** die vergezeld moet worden van andere mechanismen, in het bijzonder een versterkte positie en toetsingsmogelijkheid voor de CTIVD. Vanuit het perspectief van de eisen die uit EHRM-jurisprudentie zijn af te leiden omtrent de inrichting van het toezicht op de inlichtingen- en veiligheidsdiensten moet worden opgemerkt dat in die jurisprudentie een vorm van onafhankelijke toetsing voorafgaand aan de inzet van de bijzondere bevoegdheden van de diensten weliswaar nadrukkelijk wordt gewaardeerd, maar dat daarin met misschien nog wel meer nadruk wordt gehecht aan de aanwezigheid van een onafhankelijke toezichthouder die beschikt over voldoende middelen en bevoegdheden om een daadwerkelijk effectief toezicht op de lopende (interceptie)operaties van de diensten uit te voeren. Het EHRM hecht daarbij sterk aan de mogelijkheid voor die toezichthouder om lopende operaties te kunnen beëindigen als die als onwettig

of onrechtmatig worden beoordeeld.¹ **Uit de huidige toetsingspraktijk van de CTIVD valt reeds af te leiden dat die onrechtmatigheid zich in de loop van een interceptieoperatie kan gaan voordoen, ook als die operatie in eerste aanleg - en in abstracto - wel als rechtmatig is beoordeeld.** Het College constateert dat het wetsvoorstel niet voorziet in een bindend rechtmatigheidsoordeel door de CTIVD, behoudens in reactie op een aan de commissie voorgelegde klacht. Gegeven het relatief geringe aantal klachten dat wordt ingediend (de inzet van bijzondere bevoegdheden door de diensten vindt immers in het geheim plaats, dus betrokkenen zijn er doorgaans niet van op de hoogte) levert dat een belangrijke beperking op van een waarborg die het EHRM terdege relevant vindt. Ook de CTIVD heeft in haar recent aan u toegezonden standpunt in vervolg op de eerdere zienswijze over het wetsvoorstel gewezen op het risico van een toezichtshiaat. In het wetsvoorstel zou duidelijk tot uitdrukking moeten komen dat het CTIVD rechtmatigheidstoezicht zich ook kan richten op de rechtmatigheid van de feitelijke toepassing van bevoegdheden waarvoor de TIB toestemming heeft gegeven. Het College voegt daaraan toe dat de EHRM-jurisprudentie aanwijzingen bevat dat dit rechtmatigheidsoordeel bij voorkeur bindend zou moeten zijn. **In ieder geval dient de op p. 41 van de Nota gewekte indruk dat het oordeel van de TIB over de rechtmatigheid van een operatie leidend is voor een uiteindelijk rechtmatigheidsoordeel over de uitvoering van die operatie in al haar onderdelen, te worden weggenomen.**

2. De mate van indringendheid van de TIB-toetsing

Het belang van het voorkomen van het hierboven gesignaleerde toezichtshiaat is vooral van belang omdat **van de indringendheid van de toetsing door de TIB voorafgaand aan de inzet van bijzondere bevoegdheden geen overdreven hoge verwachtingen moeten worden gekoesterd.** De regering geeft in de Nota aan dat de TIB een volle toetsing verricht op noodzakelijkheid, proportionaliteit en subsidiariteit van de inzet. Vooral bij de inzet van onderzoeksopdrachtgerichte interceptie, die naar zijn aard raakt aan de privacy van grote groepen burgers, bevindt de afweging die in de autorisatiefase gemaakt moet worden zich echter onvermijdelijk op een tamelijk abstract niveau waarin allerlei bredere beleidsafwegingen een rol spelen. De beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit kunnen in zo'n geval niet een zelfde strak toetsingskader bieden als wanneer de inbreuk op de privacy van een enkel individu of een beperkt groepje mensen beoordeeld moet worden. Vele deskundigen op het terrein van (toezicht op) de inlichtingendiensten wijzen hierop.²

De waarde van de TIB-toetsing zal vooral liggen in de druk die daarvan uitgaat op

¹ Zie voor een analyse van en meer gedetailleerde bronverwijzingen naar deze EHRM-jurisprudentie: J.P. Loof e.a., "Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten" (Onderzoek in opdracht van het CTIVD, Universiteit Leiden, augustus 2015), gepubliceerd op www.ctivd.nl.

² Zie o.m. European Commission for Democracy through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, adopted its 102nd Plenary Session, CDL-AD(2015)006, Strasbourg 7 April 2015, p. 3.

de diensten en de verantwoordelijke ministers om de beslissing over de inzet van bijzondere bevoegdheden zorgvuldig voor te bereiden en draagkrachtig te motiveren, op een zodanige manier dat de gemaakte afweging in ieder geval goed zichtbaar is. De TIB-toetsing is en blijft echter een ‘papieren’ toets door een instantie die geen directe toegang heeft tot alle gegevens van de diensten. Zoals onder 1. reeds is aangegeven kan de TIB-toetsing dan ook nooit het definitieve en alomvattende rechtmatigheidsoordeel over de volledige uitvoering van een onderzoeksopdrachtgerichte interceptieoperatie opleveren. Diverse passages in de Nota wekken de illusie dat dit wel zo is.

3. Dekt de TIB-toetsing alle relevante inzet van bevoegdheden?

In het wetsvoorstel is niet voorzien in toetsing door de TIB van de in art. 55 geregelde bevoegdheid tot het opvragen van zogenaamde verkeersgegevens bij telecombedrijven. Voor het uitoefenen van deze bevoegdheid hoeft ook niet in alle gevallen toestemming te worden gevraagd aan de minister. Tot dusverre is over dit element van het wetsvoorstel nog weinig discussie geweest, vooral omdat het hier geen nieuwe bevoegdheid betreft en art. 55 in wezen niets verandert aan het regime dat reeds geldt op grond van de huidige Wiv. Desalniettemin dwingen recente Europese jurisprudentiële ontwikkelingen tot een nadere bezinning op dit onderdeel van het wetsvoorstel. Zowel in de jurisprudentie van het EU HvJ als in die van het EHRM is de laatste jaren herhaaldelijk overwogen dat een bevoegdheid tot het opvragen van verkeersgegevens, ook wanneer die niet alleen betrekking heeft op personen jegens wie een concrete verdenking bestaat, in het licht van de bescherming van (onder meer) de nationale veiligheid noodzakelijk kan zijn. Volgens beide Europese hoven moet de uitoefening van die bevoegdheid dan, behoudens in spoedeisende gevallen, wel zijn onderworpen aan ‘een voorafgaand toezicht door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit’.³ Aan deze eis wordt in het nu voorliggende wetsvoorstel niet voldaan.

4. Hoe gericht is ‘onderzoeksopdrachtgericht’?

Kernpunt van de discussie over dit wetsvoorstel betreft de grootschaligheid van de nieuw gecreëerde bevoegdheid tot onderschepping van telecommunicatiegegevens op kabelgebonden netwerken (bulkinterceptie). De Raad van State heeft in zijn advies aangegeven de noodzaak van deze bevoegdhedenuitbreiding voldoende beargumenteerd te achten. Ook het College stelt vast dat de onderbouwing van de voorgestelde bevoegdhedenuitbreiding in ieder geval een stuk steviger is dan bij het eerder gepubliceerde conceptwetsvoorstel het geval was. Ook bevat de Nota op verschillende plaatsen nog weer een verder verduidelijking van de praktische omvang van dit type interceptie. Die verduidelijking is zeer waardevol.

³ Zie meest recent HvJ EU 21 december 2016, zaken C-203/15 en C-698/15 (Tele2 Sverige AB & Secretary of State for the Home Department), § 120. Eerder ook HvJ EU 8 april 2014, zaak C-293/12 (Digital Rights Ireland), § 62 en EHRM 12 januari 2016, nr. 37138/14 (Szabo en Vissy t. Hongarije), § 77 en 80. Het College realiseert zich dat het EU-recht niet van toepassing is op de inlichtingendiensten, maar de privacybeschermingsprincipes waarop de jurisprudentie van het HvJ EU gestoeld is, hebben wel degelijk ook betekenis voor de operaties van inlichtingendiensten.

Wel wijst het College erop dat juist met betrekking tot de vraag naar de proportionaliteit van de privacyinbreuk in situaties waarin gegevens worden verzameld of bewaard van een onbepaalde groep personen zonder dat daarbij enig onderscheid gemaakt wordt tussen personen die wel of niet enig gevaar opleveren de Europese mensenrechtenjurisprudentie nog volop in beweging is. Er zijn uitspraken van het EHRM en het HvJ EU die erop lijken te wijzen dat beide instanties ongedifferentieerde en ongerichte verzameling van telecommunicatiegegevens van een ieder, naar haar aard disproportioneel achten.⁴ Hoewel deze jurisprudentie nog niet volledig uitgekristalliseerd is, acht het College het van belang in ieder geval van de regering te vernemen hoe zij aankijkt tegen de relevantie van deze jurisprudentie voor het voorliggende wetsvoorstel en de daarin opgenomen uitbreiding van de interceptiebevoegdheden.

In § 1.7 en 3.3.3.3.5 van de Nota geeft de regering aan dat het wetsvoorstel geen ruimte biedt voor een ‘tap op de kabel’. Er gaat geen datasleepnet door de hele communicatiestroom, maar alleen een klein sleepnetje door een stukje van die stroom. En het sleepnet functioneert zo dat allerlei gegevens waarvan op voorhand al kan worden vastgesteld dat ze irrelevant zijn voor de onderzoekopdracht niet in het sleepnet blijven hangen en dus niet bij de diensten terecht komen.

Het is belangrijk dat deze verheldering in de Nota is gegeven, want de bewoordingen van het wetsvoorstel zelf bieden op dit punt geen volstrekte helderheid. Zoals hierboven al opgemerkt laten de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit zich vooral goed toepassen bij het maken van een afweging waarin het nationale veiligheidsbelang tegenover het privacybelang van een bepaald individu staat. In § 3.3.1.3.1 van de Nota geeft de regering zelf ook aan dat de toets op grond van art. 26 zich richt op die individu-specifieke afweging. **Bij onderzoekopdrachtgerichte interceptie is evenwel het privacybelang van een onbepaalde hoeveelheid individuen in het geding en voor die situatie is er behoefte een nadere aanduiding in de wettekst zelf die dwingt tot een zo gericht/selectief mogelijke interceptie.**

De opmerking van de regering in § 1.2.2 van de Nota dat er soms sprake kan zijn van een keuze voor een minder gerichte interceptie omdat de keuze voor de meest gerichte bevoegdheid tot een grotere inbreuk op de privacy leidt, illustreert de ingewikkeldheid van de afweging die gemaakt moet worden. Zij laat echter tevens zien dat er klaarblijkelijk van uitgegaan wordt dat interceptie van communicatiegegevens van een grote groep burgers als minder grote inbreuk op de privacy wordt beschouwd dan een meer gerichte afluisteroperatie (waarbij ook de inhoud van de communicatie wordt onderschept) tegen één of enkele individuen. Het is de vraag of dat een juiste veronderstelling is. **Wat levert nu in totaal de grotere privacyinbreuk op: een ‘milde’ inmenging die een grote groep mensen raakt of een indringender inmenging die slechts één of enkele**

⁴ Zie de in voetnoot 3 genoemde arresten, alsmede EHRM 4 december 2015, nr. 47143/06 (Roman Zakharov t. Rusland).

individuen treft?

5. Databeperking

Een zo goed mogelijke gerichtheid van interceptie moet worden aangevuld met heldere waarborgen voor verantwoorde beperking van de data die via een interceptieoperatie zijn binnengehaald: het zo snel mogelijk verwijderen of vernietigen van gegevens die niet nodig zijn voor de bescherming van de nationale veiligheid. De NvW bevat ten aanzien hiervan enkele kleine aanscherpingen van de wettekst. Deze gaan echter nog niet zo ver als de concrete suggesties voor aanscherping van de normering als gedaan door de CTIVD in haar zienswijze. Het College betreurt dat, want het ziet juist in deze **nadere concretisering van wettelijke waarborgen voor databeperking zoals voorgesteld door de CTIVD een belangrijke verheldering van het toetsingskader**. In het bijzonder het maken van onderscheid in de bewaartermijnen voor inhoud en metadata is daarbij van groot belang.

6. Hacken via derde

Het College heet kennisgenomen van de reactie van de regering op het amendement-Verhoeven dat beoogt te regelen dat de zogenoemde bevoegdheid tot 'hacken via derden' alleen mag worden toegepast als dat onvermijdelijk is. De stelling van de regering is dat dit amendement miskent dat de diensten in het merendeel van de gevallen geen directe toegang tot de computersystemen of gegevensdragers van een target hebben. Het College ziet in deze stelling van regeringszijden geen dragend argument dat in de weg staat aan **opname van het criterium 'onvermijdelijk'**. Juist **vanwege de verstrekkendheid en ingrijpendheid van deze bevoegdheid is het College van mening dat invoeging van dit criterium op zijn plaats is**.

7. Delen van gegevens met buitenlandse diensten

Op verschillende plaatsen in de Nota wordt door de regering ingegaan op het verstrekken van gegevens met buitenlandse diensten. Deze passages dragen over het algemeen bij aan verdere verduidelijking van de reikwijdte van deze gegevensverstrekking. Voor zover sprake is van verstrekking van gegevens die verkregen zijn via onderzoeksoopdrachtgerichte interceptie (op basis van art. 48 van het wetsvoorstel) blijft echter nog onhelder in welke fase van gegevensverwerking reeds sprake is kan zijn van de verstrekking van de verzamelde gegevens aan een buitenlandse dienst. Juist omdat bij deze vorm van interceptie sprake zal zijn van grote hoeveelheden data en verantwoorde databeperking zo'n belangrijk onderdeel vormt van het systeem van wettelijke waarborgen om al te omvangrijke privacyaantasting te voorkomen, is de vraag in welke fase van de dataselectie de gegevensverstrekking aan een buitenlandse dienst plaatsvindt. **Levert het verstrekken van bulkgegevens aan een buitenlandse dienst als een deel van die gegevens volgens de Nederlandse wetsystematiek in een latere verwerkingsfase weggefilterd en vernietigd zou moeten worden niet een risico op omzeilen van wettelijke waarborgen op?**

Conclusie

De uitdaging van dit wetsvoorstel ligt in het vinden van een goede balans tussen veiligheid en privacy. Er dient een evenwicht te worden gevonden tussen enerzijds de bevoegdheden van de diensten ten behoeve van de nationale veiligheid en anderszijds de waarborgen die bescherming bieden tegen ongerechtvaardigde inbreuken op mensenrechten. De in de Nota van wijziging opgenomen aanpassingen van het wetsvoorstel zijn nog niet voldoende om deze balans te bereiken. Een verdere aanscherping van het toezicht en de waarborgen is noodzakelijk. Het College hoopt u met de bovenstaande inventarisatie van knelpunten en onduidelijkheden aanknopingspunten te hebben geboden voor een voortzetting van de discussie met de regering over het wetsvoorstel Wiv 20xx.

Mocht u naar aanleiding van deze brief nog vragen hebben of een toelichting willen, dan kunt u contact (laten) opnemen met Juliette Bonneur, via J.Bonneur@mensenrechten.nl of 030-8883888.

Hoogachtend,

mr. Adriana C.J. van Dooijeweert
Voorzitter