NEDERLANDSE ORDE VAN ADVOCATEN

Aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties
de heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA DEN HAAG

Den Haag, 1 september 2015
Dossiernummer: 3.1.2/3
telefoonnummer: 070 – 335 35 77
E-mal: r.huges@advocatenorde.nl
Bijlage: advies adviescommissies strafrecht en adviescommissie rechtsstatelijkheid

Betreft: consulatie wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten

Zeer geachte heer Plasterk,

Op 2 juli 2015 is het wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten (WIV) in consulatie gegeven. Het wetsvoorstel WIV strekt ter vervanging van de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 ("WIV 2002"). Met het wetsvoorstel WIV wordt beoogd een wettelijk kader voor de inlichtingen- en veiligheidsdiensten in brede zin te realiseren dat toekomstbestendig is en in lijn met de vereisten van de Grondwet alsmede het EVRM.

De kern van de reactie van de Nederlandse orde van advocaten (NOvA) is dat de minister met het wetsvoorstel WIV nog ver afstaat van de realisatie van zijn voornemen te komen tot een wettelijk kader dat in lijn is met grondwettelijke waarborgen en andere belangrijke (rechtsstatelijke) uitgangspunten.

De NOvA spreekt dan ook de wens uit dat deze en vergelijkbare consultatiereacties zullen leiden tot de noodzakelijke bijstellingen van het wetsvoorstel. Het verdere wetgevingsproces zullen we dan ook met grote belangstelling blijven volgen.

Gelet op het ontbreken van wettelijke waarborgen in het wetsvoorstel WIV ingeval bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten jegens advocaten worden uitgeoefend, voelt de Nederlandse orde van advocaten zich genoodzaakt op dit onderdeel in het bijzonder in te gaan in zijn reactie.

De algemene raad heeft het wetsvoorstel WIV met het oog daarop voorgelegd aan zijn adviescommissies strafrecht en rechtsstatelijkheid. Graag vraag ik uw aandacht voor bijgaand advies.

Bezoekadres
Neuhuyskade 94
2596 XM Den Haag
Tel. 070 - 335 35 35
Fax 070 - 335 35 31

Postadres
Postbus 30851
2500 GW Den Haag

www.advocatenorde.nl

Procedure tot nu toe

Sinds medio 2014 brengt de NOvA onder uw aandacht dat zij met zorg de ontwikkelingen volgt met betrekking tot de omgang van de Nederlandse inlichtingen- en veiligheidsdiensten met vertrouwelijke communicatie tussen rechtszoekenden en hun advocaten. De verzoeken van de NOvA om wettelijke waarborgen - zoals een voorafgaande rechterlijke toetsing - ter bescherming van de vertrouwelijke communicatie tussen advocaten en hun cliënten werden door u afgewezen. U heeft aangegeven daarin geen noodzaak te zien omdat deze waarborgen al voldoende zouden vastliggen in intern beleid.

Tijdens een overleg op 28 mei jl. met uw ambtsgenoot van Defensie, minister Hennis-Plasschaert, werd de NOvA uitgenodigd de gelegenheid van de consultatie aan te grijpen om onze zorgen over de schending van cliëntvertrouwelijkheid nogmaals onder de aandacht te brengen.

Bij kort geding vonnis van de rechtbank Den Haag van 1 juli 2015[1] is beslist dat dat bestaande interne beleid voor wat betreft de bescherming van de vertrouwelijkheid van de communicatie tussen advocaten en hun cliënten gelet op de rechtspraak van het Europees Hof voor de Rechten van de Mens ("EHRM") onvoldoende waarborgen bevat. De voorzieningenrechter geeft de Staat zes maanden de tijd om maatregelen te treffen die voorzien in beleid op grond waarvan de inzet van bijzondere bevoegdheden met het oog op bescherming van het verschoningsrecht van advocaten in de zin van richtlijn 249/77 EEG kan worden getoetst door een onafhankelijk orgaan dat in ieder geval de bevoegdheid heeft om de uitoefening van bijzondere bevoegdheden te voorkomen of te beëindigen. Op 2 juli verscheen vervolgens het consultatievoorstel zonder verwijzing naar bovengenoemd rechterlijk vonnis.

Blijkens uw schriftelijke reactie van 27 juli 2015 op het kort geding vonnis aan de Voorzitter van de Tweede kamer, wenst de Staat te voorzien in een vorm van onafhankelijke toetsing bij het tappen van advocaten. Tegelijkertijd heeft de Staat ook spoedappel ingesteld tegen de door de kort geding rechter gegeven aanwijzingen over de inhoud van de inrichting van genoemde onafhankelijke toets, alsmede de termijn van zes maanden waarbinnen voorzien moet worden in een onafhankelijke toets.

Op 1 september jl. heeft u een brief gestuurd aan de Tweede Kamer waarin u aangeeft dat de AIVD opnieuw de vertrouwelijkheid van gesprekken tussen advocaat en cliënt heeft geschonden. Dit onderstreept de noodzaak van introductie van een voorafgaande rechterlijke toets. Daarbij speelt dat schendingen en de afwezigheid van toetsing het wantrouwen van de samenleving bepaald aanwakkert; te meer nu van herhaaldelijke schendingen is gebleken.

Kernbezwaar: ontbreken van wettelijke waarborgen

Een inbreuk op het verschoningsrecht raakt artikel 8 EVRM (recht op privacy) en artikel 6 EVRM (recht op eerlijk proces). Inbreuken op deze rechten zijn slechts gerechtvaardigd wanneer zij bij wet zijn voorzien en in het licht van een specifiek doel noodzakelijk zijn. De Staat maakt door het afluisteren van gesprekken tussen advocaten en hun cliënten inbreuk op het verschoningsrecht van advocaten. Het verschoningsrecht van advocaten is een fundamenteel recht. Op grond van dit fundamentele recht is vertrouwelijke communicatie met zijn advocaat gewaarborgd.

[1] ECLI: NL: RBDHA:2015:7436

De inlichtingen- en veiligheidsdiensten kunnen op twee manieren beschikking krijgen over vertrouwelijke informatie van advocaten:

(i) direct - door de inzet van bijzondere bevoegdheden jegens advocaten; en
(ii) indirect - door zogenaamde 'bijvangst' als bijvoorbeeld de cliënt van een advocaat 'target' is van de inzet van bijzondere bevoegdheden.

De basis waarop inlichtingen- en veiligheidsdiensten hun huidige bevoegdheden thans ontlenen (artikel 25 WIV 2002) om communicatie tussen advocaten en hun cliënten af te luisteren, voldoet niet aan de door het EHRM gestelde waarborgen die een inbreuk op het verschoningsrecht rechtvaardigt. Blijkens het wetsvoorstel WIV ondergaat artikel 25 WIV 2002[2] geen enkele wijziging, noch worden waarborgen elders in het wetsvoorstel WIV beschreven. Hoewel de waarborgen in het consultatievoorstel ontoereikend zijn, worden de in paragraaf 3.2.2 van het wetsvoorstel WIV bepaalde bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten fors uitgebreid. Ook kabelgebonden telefoon- en dataverkeer (o.a. internetverkeer, chatsessie, mobiel dataverkeer) kan straks op basis van het wetsvoorstel WIV grootschalig worden afgetapt. Voor het tappen van communicatie waarbij advocaten betrokken zijn, wordt in het wetsvoorstel WIV geen wettelijke waarborg getroffen die eventuele inbreuken op het verschoningsrecht zou kunnen rechtvaardigen. Het gemis van wettelijke waarborgen doet zich dan ook alleen nog maar sterker voelen nu de afluisterbevoegdheden enorm worden verruimd.

Noodzaak introductie voorafgaande rechterlijke toets (direct tappen)

Alleen in geval de diensten bijzondere bevoegdheden willen inzetten jegens journalisten, is blijkens artikel 24, vierde lid, wetsvoorstel WIV voorafgaande rechterlijke toestemming noodzakelijk. De aanleiding hiervoor is de uitspraak van 22 november 2012 van het EHRM in de zogenoemde Telegraafzaak[3], waarin het EHRM oordeelde dat de inzet van bijzondere bevoegdheden (afluisteren) door de AIVD tegen de journalisten van de Telegraaf een schending oplevert van artikel 8 en artikel 10 (vrijheid van meningsuiting) en de WIV 2002 onvoldoende waarborgen ter bescherming van de bronnen van journalisten bevat.

Een gelijke schending van artikel 8, tweede lid, EVRM is evenwel eveneens geconstateerd in voornoemd kort geding vonnis. Op basis van dit vonnis is door u reeds aangegeven dat voorzien wordt in een onafhankelijke toets. Het ligt dan ook in de rede - nu in het wetsvoorstel WIV een *voorafgaande* last van een onafhankelijke rechter wordt geïntroduceerd voor de inzet van bijzondere bevoegdheden tegen journalisten - dit ook en te meer voor de inzet van deze bevoegdheden jegens advocaten te laten gelden. De mogelijkheid van inbreuken op het verschoningsrecht van advocaten raakt aan de vertrouwelijkheid van de communicatie tussen advocaten en hun cliënten en daarmee aan het recht op een effectieve verdediging en de toegankelijkheid van advocaten. De onomkeerbaarheid van mogelijke inbreuken brengt met zich mee dat toetsing voor een eventuele rechtvaardiging daaraan *vooraf* dient plaats te vinden. Ook uit het rechtsstatelijke beginsel van machtenscheiding volgt dat *voorafgaande* controle op de toepassing van uitzonderingen nodig is, onafhankelijk van het orgaan dat tot die toepassing besluit. Anders bestaan onvoldoende waarborgen tegen misbruik van bevoegdheden en daarmee hoe dan ook een zeker 'chilling effect' op het vertrouwen dat op het beroepsgeheim van advocaten geen onterechte inbreuken worden gemaakt.

[2] Artikel 32 wetsvoorstel WIV
[3] EHRM 22 november 2012, nr. 39315/06, Telegraaf Media Nederland Landelijke Media B.V en anderen tegen Nederland

De NOvA verzoekt u dan ook het er toe te leiden dat de bescherming die blijkens het wetsvoorstel WIV toe gaat komen aan journalisten op gelijke wijze voor advocaten te laten gelden en in artikel 24 , vierde lid, wetsvoorstel WIV 'advocaten' toe te voegen. Op die wijze wordt het wetsvoorstel WIV op dat punt in lijn gebracht met de eisen van het EVRM.

Noodzaak uitbreiden systeem Nummerherkenning (indirect tappen)

Rechtvaardiging voor inperking van het verschoningsrecht indien de advocaat niet 'target' is van de inzet van de bijzondere bevoegdheden door de inlichtingen- en veiligheidsdiensten maar zijn cliënt, (indirect tappen) is moeilijk voorstelbaar. Gelet op de eisen van artikel 8, tweede lid, EVRM, is voor doorbreking van het verschoningsrecht slechts in zeer uitzonderlijke omstandigheden plaats. Blijkens Nederlandse en Europese jurisprudentie is voor een doorbreking van het verschoningsrecht bijvoorbeeld slechts plaats als de verschoningsgerechtigde zelf is aangemerkt als verdachte. Dat is bij indirect tappen niet aan de orde.

Voor zover de inlichtingendiensten een rechtvaardiging zou kunnen vinden voor een inbreuk in geval van indirect tappen, dan geldt dat de hiervoor beschreven voorafgaande rechterlijke toetsing geen waarborg kan zijn voor die rechtvaardiging. Het is immers op voorhand niet duidelijk wanneer de 'target' contact heeft met zijn advocaat. Door het invoeren van een systeem van nummer-herkenning kan op betrekkelijk eenvoudige wijze worden voldaan aan de eisen van artikel 8, tweede lid EVRM en wordt voorkomen dat inbreuken op het verschoningsrecht van advocaten onomkeerbaar plaats hebben.

In 2011 is reeds een systeem van nummerherkenning ingevoerd voor het tappen van telefoongesprekken tussen cliënten en hun advocaten door de nationale politie. Dit systeem is tot stand gekomen door een goede en nauwe samenwerking tussen de minister van V&J, de nationale politie, het Openbaar Ministerie en de NOvA. Nummerherkenning zorgt ervoor dat telefoongesprekken tussen cliënten en advocaten niet real-time of naderhand worden afgeluisterd door de nationale politie. Via het systeem van nummerherkenning kunnen advocaten telefoonnummers aanmelden. Deze geheimhoudernummers geeft de NOvA vervolgens door aan de nationale politie. De politie verwerkt de nummers in hun database van alle geheimhoudersnummers. De nummers worden hierna automatisch herkend en kunnen niet real-time of naderhand worden afgeluisterd.

Sinds medio 2013 is ook in samenwerking met de NOvA een systeem van nummerherkenning bij de Dienst Justitiële Inrichtingen ("DJI") ingevoerd. Het systeem van DJI werkt anders dan dat van de nationale politie. Alle gesprekken die een gedetineerde voert vanuit een inrichting van DJI worden opgenomen. Bij gesprekken naar een geheimhoudernummer wordt opname vóór totstandkoming van het gesprek verhinderd; er kan ook niet real-time worden meegeluisterd. Ook aan DJI geeft de NOvA iedere dag alle nummers van advocaten zonder vermelding door, die vervolgens worden verwerkt in het systeem van DJI.

Een vergelijkbaar systeem kan naar verwachting op betrekkelijk eenvoudige en gelijke wijze worden ingevoerd bij de inlichtingen- en veiligheidsdiensten. De NOvA is graag bereid - gelijk als bij de invoering van de systemen bij de nationale politie en DJI - zich hiervoor in te zetten en daarover met u in overleg te treden.

Met de meeste hoogachting,
namens de algemene raad,

W.F. Hendriksen
Algemeen deken Nederlandse orde van advocaten

Cc: minister van Defensie, mevrouw J.A. Hennis-Plasschaert

Bijlage: advies adviescommissies NOvA

NEDERLANDSE ORDE VAN ADVOCATEN

Van	:	adviescommissie strafrecht
Datum	:	31 augustus 2015
Betreft	:	**wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX (versie juni 2015)**

Samenvatting

- Doordat een onafhankelijk controle orgaan dat de mogelijkheid heeft de toepassing van bijzondere bevoegdheden door de AIVD en de MIVD te toetsen en onrechtmatige toepassing te voorkomen c.q. te beëindigen ontbreekt, voldoet het wetsvoorstel niet aan een systeem van checks and balances dat in een rechtsstaat met betrekking tot de verhouding tussen de overheid en de persoonlijke levenssfeer van de burger wordt vereist. De ACS beveelt aan een onafhankelijk orgaan in te stellen dat onafhankelijke en voorafgaande controle kan uitoefenen op de toepassing door de AIVD van bijzondere bevoegdheden. Dat onafhankelijke orgaan moet beschikken over de mogelijkheid potentieel onrechtmatige situaties te voorkomen en onrechtmatige situaties te beëindigen.
- De wijze waarop de huidige WIV 2002 wordt toegepast laat toe dat zonder enige voorafgaande onafhankelijke controle vertrouwelijke communicatie tussen een advocaat en zijn cliënt ter kennis komt en blijft van de overheid. Dat druist in tegen het rechtstatelijk karakter van de Nederlandse samenleving en is naar de mening van de ACS in strijd met het EVRM. De ACS beveelt met klem aan dat een specifieke regeling met betrekking tot onafhankelijke, rechterlijke controle wordt ingevoerd waardoor wordt gewaarborgd dat directe onderschepping van verschoningsgerechtigde informatie wordt voorkomen en dat ongewild verkregen 'bijvangst' niet ter kennis komt van de overheid, maar wordt vernietigd. Alleen op deze wijze wordt ernstige afbreuk aan de Nederlandse rechtsstaat voorkomen. Andere landen kennen een dergelijke controle al.
- Alle toepassingen van bijzondere bevoegdheden door AIVD of MIVD die (kunnen) leiden tot het direct kennis nemen door de overheid van vertrouwelijke communicatie tussen de advocaat en zijn cliënt dienen voorafgaand door een onafhankelijke rechter te worden getoetst. Het systeem van nummerherkenning dient ook te worden toegepast op AIVD en MIVD taps zodat 'bijvangst' van communicatie tussen advocaat en cliënt wordt voorkomen.
- Vertrouwelijke communicatie tussen de advocaat en zijn cliënt die de AIVD of de MIVD desondanks (indirect) verkrijgt dient, zonder kennisneming door die diensten, te worden voorgelegd aan een toetsingsorgaan dat eenzelfde geheimhoudingsplicht en verschoningsrecht heeft en toetst of de advocaat in kwestie ontoelaatbaar heeft gehandeld. Alleen in het laatste geval wordt de betreffende informatie alsnog in handen van de overheid gegeven. Doet dit geval zich niet voor dan wordt de betreffende informatie alsnog vernietigd.
- De ACS beveelt aan de burger een volwaardig recht tot effectieve correctie van onjuiste registraties te geven.

Inleiding

Taak en werkgebied van de AIVD[1] hebben vooral betrekking op het verkrijgen, onderscheppen, of anderszins verzamelen, het bewaren, verstrekken, vergelijken, analyseren of anderszins verwerken van informatie (in de ruimste zin van het woord) die van belang kan zijn voor de nationale veiligheid. Een dergelijke taakstelling botst vroeg of laat met een aantal grondrechten

[1] Waar in dit advies wordt gesproken over de AIVD wordt ook diens militaire evenknie, de MIVD, bedoeld.

(recht op eerbiediging van de persoonlijke levenssfeer, bescherming van het huisrecht, bescherming van het briefgeheim).

Waar grondrechten dreigen te (moeten) worden beperkt is het in een rechtsstaat vanzelfsprekend dat de gevallen waarin dat, noodzakelijkerwijs, wordt toegestaan duidelijk in een wet worden vast gelegd en even duidelijk worden begrensd teneinde te voorkomen dat de grondwettelijke regel in de praktijk een uitzondering wordt. Even vanzelfsprekend is het in een rechtsstaat dat aan bevoegdheden die een beperking van grondrechten tot gevolg kunnen hebben een systeem van toezicht wordt gekoppeld dat effectief onnodige beperkingen kan voorkomen en even effectief kan controleren dat die overheid dergelijke vergaande bevoegdheden op juiste wijze toepast. Onnodige beperking van grondrechten van de burger ten opzichte van de overheid dient immers te allen tijde te worden voorkomen.
Beginselen als noodzakelijkheid, doelbinding, proportionaliteit en subsidiariteit spelen bij het toewijzen van bevoegdheden, maar vooral bij de uitoefening daarvan een grote rol. Dat zijn open normen die door de betreffende overheidsfunctionarissen welhaast per definitie ruimer zullen worden geïnterpreteerd en toegepast dan de wetgever bedoeld heeft. Effectieve controle daarop dient in een rechtsstaat dan ook *onafhankelijke* controle te zijn.

De aard van de AIVD werkzaamheden brengt mee dat een groot deel van die werkzaamheden - alsmede de resultaten daarvan - in de ogen van de AIVD vertrouwelijk moet blijven omdat het prijsgeven van die informatie op zich ook een bedreiging van de nationale veiligheid zou zijn. In feite is sprake van een ondoorzichtige 'black box' waarbinnen vergaande bevoegdheden worden uitgeoefend zonder de gebruikelijke transparante controle op de uitoefening van die bevoegdheden ten gevolge waarvan de Staat belangrijke grondrechten van de burger willens en wetens schendt (ten gunste van in de ogen van de Staat zwaarwegender belangen).

We hebben hier dus te maken met de klassieke situatie waarin een grote overheid (privé)rechten van een enkele individuele burger schendt waarbij de wijze waarop die schending plaats vindt bovendien 'geheim', 'schimmig' en in ieder geval niet transparant is. Het is juist deze klassieke situatie die aanleiding is geweest om tegenover dergelijke vergaande bevoegdheden een effectief systeem van checks and balances in het leven te roepen zodat de rechten van de burger tenminste niet onnodig worden geschonden.

<u>Checks and Balances nu onvoldoende</u>

Het systeem van checks and balances in de huidige WIV 2002 bestaat uit de volgende componenten. Voor het gebruik van (vergaande) bevoegdheden is toestemming vooraf nodig van de Minister. De Minister informeert de Tweede Kamer en over vertrouwelijke zaken informeert hij de Commissie voor de Inlichtingen- en Veiligheidsdiensten ("CIVD") van de Tweede Kamer. De CIVD zelf is tot strikte geheimhouding verplicht. *"Zo wordt informatie die zicht geeft op het actuele kennisniveau van de diensten en door de diensten aangewende middelen in concrete aangelegenheden sinds jaar en dag (uitsluitend) met de CIVD gedeeld."* [2]Langs deze weg vindt controle van het parlement plaats.
De Tweede kamer heeft voorts invloed doordat zij een bindende[3] voordracht doet voor de leden van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten ("CTIVD"). De CTIVD is onafhankelijk en gespecialiseerd. Zij oefent rechtmatigheidstoezicht uit, maar alleen achteraf.

[2] MvT op wetsvoorstel WIV 2015, p. 152; artikel 8 lid 4 WIV 2002.
[3] In feite slechts beperkt bindend want als het kabinet de voorgedragen kandidaten niet geschikt vindt, vraagt zij de Kamer om een nieuwe voordracht te doen.

Een ieder die betrokken is bij de uitvoering van de WIV 2002 is verplicht om inlichtingen te verstrekken aan deze commissie en de commissie kan getuigen en deskundigen voor zich laten verschijnen om verklaringen af te leggen.[4] Aanbevelingen van de CTIVD zijn echter niet bindend. Daarnaast heeft de CTIVD een klachtadviesfunctie in (bestuursrechtelijke) klachtprocedures. Klachten kunnen ook aan de Nationale Ombudsman worden voorgelegd, maar dat gebeurt in de praktijk zelden.
De Algemene Rekenkamer is belast met (financiële) rechtmatigheids- en doelmatigheidscontrole.

Het huidige controle systeem brengt mee dat de Minister een oordeel van de CITVD dat de uitoefening van een bijzondere bevoegdheid, hetzij in het algemeen, hetzij in een individueel geval, onrechtmatig is naast zich neer kan leggen. De AIVD kan de uitoefening van zo'n bevoegdheid in dat geval gewoon voortzetten. Dat gebeurt in de praktijk ook. Is dat de effectieve controle die in een rechtsstaat gewenst is?

Evaluatiecommissie Dessens

Nee, antwoordde de Evaluatiecommissie ("Commissie Dessens") die de uitvoering van de WIV 2002 evalueerde en in 2013 rapporteerde. Volgens de Commissie behoeft *de governance ten aanzien van de AIVD versterking omdat een versterking van de governance bij [draagt] aan de rechtsstatelijke waarborgen in het stelsel van sturing en toezicht op de I&V-diensten.*[5]

De Commissie Dessens acht het toezicht op de inzet van bijzondere bevoegdheden[6] onvoldoende en beveelt, teneinde het toezicht 'EVRM-proof' te doen zijn, aan *"om het toezicht achteraf te versterken. In de visie van de evaluatiecommissie zal verstevigd toezicht (achteraf), gecombineerd met beter vormgegeven sturing (vooraf) en andere toestemmingsvereisten resulteren in een betere samenhang van waarborgen bij de inzet van bijzondere bevoegdheden. De evaluatiecommissie beveelt daarbij aan om de rechtmatigheidsoordelen van de CTIVD een juridisch bindende kracht te geven. De evaluatiecommissie vindt dat het bindend rechtmatigheidsoordeel van de CTIVD moet zien op alle bijzondere bevoegdheden. De evaluatiecommissie acht het namelijk niet wenselijk dat de Wiv de mogelijkheid openlaat dat ministers een dergelijk rechtmatigheidsoordeel van de CTIVD naast zich neer leggen. Als de CTIVD tot de conclusie komt dat een afgegeven last onrechtmatig is, moet de dienst de uitvoering van deze bijzondere bevoegdheid, voor zover deze op dat moment al is aangevangen, direct staken."*[7]

Voorts acht de Commissie Dessens invoering van een correctierecht geboden: "*De evaluatiecommissie beveelt verder aan om in hoofdstuk 4 van de Wiv te expliciteren dat degene die kennis heeft genomen van gegevens kan verzoeken om eventuele fouten daarin te laten herstellen, de gegevens te laten aanvullen, of te laten vernietigen.*"[8]

Het wetsvoorstel neemt belangrijke aanbevelingen Commissie Dessens niet over

De aanbeveling om de CTIVD een bindend rechtmatigheidsoordeel te geven wordt niet overgenomen omdat het kabinet van mening is dat de ministers volledig verantwoordelijk (moeten)

[4] Maar om die medewerking te kunnen verlenen en/of te kunnen getuigen hebben zij die bij de uitvoering van de WIV 2002 betrokken zijn wel de voorafgaande toestemming van de Minister nodig om hun geheimhoudingsplicht te kunnen schenden.
[5] Rapport Commissie Dessens, p. 169.
[6] Zoals het betreden van een woning zonder dat de bewoner dit weet, of het afluisteren van een telefoon (artikel 20 WIV 2002 en 25 wetsvoorstel).
[7] Rapport Commissie Dessens, p. 173.
[8] Rapport Commissie Dessens, p. 175.

blijven voor de operationele activiteiten van de diensten en daarvoor ook ten volle verantwoording afleggen aan de beide Kamers der Staten-Generaal.

> *" Dit uitgangspunt brengt met zich dat aan de CTIVD niet de bevoegdheid is verleend om bindende besluiten te nemen ten aanzien van het opereren van de diensten. Mocht de CTIVD tijdens haar werkzaamheden op iets stuiten waarvan zij van mening is dat dit dient te stoppen dan kan zij de betreffende minister daarvan op de hoogte stellen. Het is vervolgens aan de minister om een besluit te nemen en daarover verantwoording af te leggen.".*

Aldus de Memorie van Toelichting.[9]

Deze redenering ontgaat de ACS volledig. Niet valt in te zien waarom er - naast parlementaire controle - niet ook onafhankelijke niet-politieke controle zou kunnen zijn. Dit klemt temeer nu de Minister geen toetsing vooraf toestaat en aan toetsing achteraf geen bindend karakter wil geven. Als compensatie en *"om het stelsel EVRM-proof te doen zijn"*[10] stellen de ministers voor om ter versterking van het toezicht op het verlenen van toestemming tot toepassing van bijzondere bevoegdheden in de wet vast te leggen dat de minister verplicht is zijn mening te heroverwegen:

> *"Dit houdt in dat als de CTIVD van oordeel is dat een door de minister verleende toestemming voor de inzet van een bijzondere bevoegdheid onrechtmatig is, de minister deze verplicht is opnieuw te bezien."*[11]

De ACS constateert dat ook het kabinet hier erkent dat het huidige controle systeem niet EVRM proof is, maar constateert tegelijkertijd dat de geboden 'oplossing' niet meer dan een sigaar uit eigen doos is. Het is immers volstrekt vanzelfsprekend - dat zou het in ieder geval moeten zijn - dat een minister naar aanleiding van een onrechtmatigheidsoordeel van een onafhankelijke commissie van toezicht zich serieus afvraagt of hij zijn eerdere, inmiddels als onrechtmatig gekwalificeerde, standpunt nog wel kan handhaven. Uit dit standpunt van het kabinet kan de ACS niet anders afleiden dan dat *effectieve onafhankelijke* controle zo veel mogelijk buiten de deur wordt gehouden.

Ook wordt geen volledig correctierecht toegekend. Degene die na inzage van door de AIVD geregistreerde gegevens tot de conclusie komt dat die registratie (geheel of gedeeltelijk) onjuist is kan daarover een verklaring insturen, die bij de geregistreerde gegevens moet worden bewaard. Deze oplossing is sympathiek in gevallen waarin niet onmiskenbaar kan worden vast gesteld dat de registratie onjuist is, maar toont ook een principiële onwil om eventuele gemaakte fouten gewoon te erkennen en daarmee het rechtsstatelijk karakter van de regeling te vergroten.

<u>Beginselen bij toezicht op inlichtingendiensten</u>

Het in het wetsvoorstel gepresenteerde systeem van toezicht voldoet in meerdere opzichten niet aaneen effectief systeem van checks and balances. Het Instituut voor informatierecht ("IViR") van de Universiteit van Amsterdam heeft na onderzoek tien beginselen beschreven waaraan toezicht op nationale veiligheidsdiensten zou moeten voldoen teneinde effectieve rechtstatelijke controle te

[9] MvT, p. 157.
[10] MvT, p. 158.
[11] MvT, p. 158; wetsvoorstel artikel 102.

kunnen waarborgen.[12] Na onderzoek van de jurisprudentie van het Europese Hof voor de Rechten van de Mens ("EHRM") komt men onder meer tot de volgende uitgangspunten:

Het toezicht moet zowel parlementair als onafhankelijk en niet parlementair zijn. Het moet alle fasen van de uitoefening van de bevoegdheden omvatten: zowel vooraf, tijdens als na de uitoefening van de bijzondere bevoegdheden. Zowel op het verzamelen als het bewaren, het verwerken, het analyseren en het gebruik van de data dient effectief toezicht te worden uitgeoefend. Onafhankelijk toezicht betekent dat het betreffende orgaan niet verbonden is met de diensten zelf of de overheid. Omdat het risico op misbruik van bevoegdheden waarbij gebruik wordt gemaakt van nagenoeg ongelimiteerde technologieën groot is en dat misbruik al snel onomkeerbare consequenties voor de burger kan hebben, moet het toezicht vooraf gaan aan het concreet inzetten van bijzondere bevoegdheden. Het controlerend orgaan moet de bevoegdheid hebben onrechtmatigheden te voorkomen respectievelijk te stoppen. Ondanks het geheime karakter van de activiteiten dient er toch een vorm van toezicht op tegenspraak te zijn, desnoods door in de procedure een speciale, onafhankelijke belangenbehartiger in te bouwen, die een oordeel heeft vanuit het perspectief van het rechtstatelijk belang en/of het belang van betrokken burgers. Het toezicht moet voldoende secretariële ondersteuning hebben om haar taken effectief te kunnen uitoefenen. Het gebruik van bijzondere bevoegdheden moet direct aan de toezichthouder, het parlement en zo spoedig mogelijk aan de betrokken burger worden gemeld. Entiteiten die door de diensten worden ingeschakeld om informatie te verkrijgen moeten de mogelijkheid hebben dit publiekelijk bekend te maken.

EHRM

Ook het EVRM acht het recht op privacy niet absoluut. Inbreuken, bijvoorbeeld ten behoeve van de nationale veiligheid, zijn toelaatbaar, maar gewaakt moet worden voor elke vorm van onnodige inbreuk. Het EHRM ziet het enkele bestaan van wetgeving die het beperken van privacy rechten toestaat al als een inmenging van de overheid in het privé leven, ten aanzien waarvan adequate en effectieve maatregelen tegen inbreuk noodzakelijk zijn. Inbreuk op het privéleven is alleen toegestaan indien dit *strikt* noodzakelijk is.[13] Op een terrein waar misbruik van bevoegdheden in individuele gevallen in potentie zo gemakkelijk is en schadelijke consequenties voor de maatschappij kan hebben, heeft het EHRM voorkeur voor een onafhankelijke rechter als controle instantie omdat daarmee onafhankelijkheid, onpartijdigheid en een adequate procedure het best gediend zijn. Controle door een ander orgaan dan een rechter wordt niet uitgesloten, mits daardoor equivalente waarborgen kunnen worden gegeven.[14] Dit laatste is bij de huidige CTIVD en in het wetsvoorstel niet het geval omdat deze niet de mogelijkheid heeft om onrechtmatigheden te voorkomen en te stoppen. [15]

Zelfs wanneer de nationale veiligheid in het geding is moet er een mogelijkheid zijn om de stelling van de overheid dat de nationale veiligheid gevaar loopt, en de bevoegdheden dus terecht zijn ingezet, effectief kunnen worden tegengesproken.[16]

---

[12] Ten Standards for Oversight and Transparancy of National Intelligence Services, Institute for Information Law, University of Amsterdam, www.ivir.nl.
[13] Klass c.a.vs. Duitsland (EHRM 6 september 1978, nr. 5029/71), par. 41, 42.
[14] Klass c.a. vs. Duitsland (EHRM 6 september 1978, nr. 5029/71), par. 55; Kennedy vs VK (EHRM 18 mei 2010, nr. 26839/05) par. 167-169, Iordachi c.a. vs. Moldavië (EHRM 10 februari 2009, nr. 25198/02), par 40.
[15] Deze enkele omstandigheid lijkt voor het EHRM al tot een onacceptabele situatie te leiden: Dumitru Popescu vs. Roemenië (EHRM, 26 april 2007, nr. 49234/99 en 71525/01), par. 77; Association "21 december 1989" c.a. vs. Roemenië (EHRM 24 mei 2011, nr. 33810/07), par. 120; Klass c.a. vs. Duitsland (EHRM 6 september 1978, nr. 5029/71), par. 21, 53, 56; en S. and Marper vs. VK (EHRM 4 december 2008, nr. 30562/04 en 30566/04), par. 119.
[16] Al-Nashif vs. Bulgarije (EHRM 20 juni 2002, nr. 50963/99), par. 123.

"Onafhankelijk" betekent dat de controle volledig vrij en zonder enige druk of instructie kan plaats vinden, aldus het Hof van Justitie. [17] Het EHRM benadrukt het belang van onafhankelijk toezicht bij het binnenhalen van data.[18] Dat impliceert dus *voorafgaand* toezicht.

Over de vraag of het huidige toezicht voldoende onafhankelijk is valt dus nog wel te discussiëren. Dat lijkt niet het geval bij de vraag of onafhankelijke controle mee brengt dat de toezichthouder ook de mogelijkheid moet hebben onrechtmatige situaties te voorkomen c.q. te beëindigen. Het antwoord daarop is ronduit bevestigend.

De ACS moet dan ook concluderen dat het in het wetsvoorstel gepresenteerde systeem van toezicht niet aan de minimale eisen voor controle van inlichtingendiensten voldoet doordat geen controle vooraf mogelijk wordt gemaakt en doordat het controle orgaan niet de bevoegdheid heeft onrechtmatige situaties te voorkomen c.q. te stoppen, waardoor het niet meer dan een papieren tijger is. Dit knaagt aan het karakter van een rechtsstaat, te meer omdat door dit falende systeem ook onnodige inbreuken worden gemaakt op een andere hoeksteen van een rechtsstaat, namelijk de waarborging van de vertrouwelijkheid van de communicatie tussen een advocaat en zijn cliënt.

Het onderscheppen van verschoningsgerechtelijke informatie

Juist in de afgelopen maanden is gebleken dat de AIVD ook communicatie tussen advocaten en hun cliënten onderschept, de betreffende vertrouwelijke informatie verwerkt en (soms) doorgeeft aan het openbaar ministerie. Het verschoningsrecht wordt daarmee door de overheid bewust geschonden zonder enige onafhankelijke controle vooraf, laat staan dat sprake is van *rechterlijke* controle vooraf. Dit is een volstrekte breuk met de door de Hoge Raad zorgvuldig opgestelde regels waaraan voldaan moet zijn om het openbaar ministerie in strafzaken toe te staan een inbreuk op het verschoningsrecht te maken. Deze vaste jurisprudentie van de Hoge Raad houdt rekening met het gegeven dat direct al sprake is van een onomkeerbare inbreuk op de vertrouwelijkheid zodra een derde zonder toestemming van de advocaat inzage heeft gekregen in verschoningsgerechtigde informatie. Volgens deze regels bepaalt daarom de advocaat in eerste instantie of het gevraagde materiaal onder zijn verschoningsrecht valt. De deken van de Orde van Advocaten neemt daarin eveneens een standpunt in. Dat standpunt moet door de overheid worden eerbiedigd tenzij dat standpunt redelijkerwijs niet juist *kan* zijn. Zijn partijen het hier niet over eens, dan beslist de rechter in een klaagschrift procedure. Zolang de rechter niet onherroepelijk heeft beslist blijft de informatie in een verzegelde enveloppe. Het verschoningsrecht kan in dit systeem alleen worden doorbroken in gevallen waarbij er
aanwijzingen zijn dat de advocaat zelf betrokken is bij strafbare feiten in samenwerking met zijn cliënt waardoor sprake is van misbruik van het verschoningsrecht.

Teneinde de vertrouwelijke informatie met een advocaat te beschermen tegen 'bijvangst' bij het tappen van nummers van verdachten, is sinds een aantal jaren het systeem van nummerherkenning ingevoerd. Als het openbaar ministerie bij de uitvoering van een tap op een telefoonnummer van een advocaat stuit, dan herkent het systeem dat nummer en wordt het gesprek niet opgenomen. Dit systeem is ingevoerd omdat het openbaar ministerie in de praktijk niet in staat bleek te garanderen dat in taps (op nummers van verdachte personen) opgevangen gesprekken met advocaten werden verwijderd en niet werden uitgewerkt met als gevolg dat de vertrouwelijkheid van communicatie met een advocaat niet kon worden gewaarborgd.

[17] Commissie vs. Duitsland (Hof van Justitie 9 maart 2010, nr. C-518/07), par 18.
[18] M.M. vs. VK (EHRM 13 november 2012, nr. 24029/07), par. 206.

Belang vertrouwelijkheid advocaten communicatie in een rechtstaat

Dat de Hoge Raad de borging van vertrouwelijke communicatie op deze manier (rechterlijke controle vóórdat de overheid in uitzonderingsgevallen eventueel over de informatie komt te beschikken) heeft ingericht heeft te maken met het bijzondere rechtstatelijke karakter van verschoningsgerechtigde informatie. Aan een rechtsstaat is inherent dat eenieder zich vrijelijk en zonder vrees voor openbaarmaking tot een advocaat moet kunnen wenden, zowel voor juridisch advies (het bepalen van zijn rechtspositie) als voor het voeren van een procedure. In beide gevallen worden aangelegenheden van dermate persoonlijke aard besproken dat - onder andere - de overheid daarmee niets te maken mag hebben. Daarom hebben de betreffende vertrouwenspersonen een beroepsgeheim met bijbehorende geheimhoudingsplicht en verschoningsrecht.
Het beroepsgeheim van de advocaat volgt uit zijn functie van raadsman en bijstandsverlener in rechte. Eenieder moet er op kunnen vertrouwen dat zijn rechtspositie niet zal worden aangetast doordat hij zich tot een advocaat wendt. Client en advocaat moeten er op kunnen rekenen dat niemand anders kennis zal nemen van hun gedachtenwisseling. Het is dan ook een rechtsstatelijk uitgangspunt dat alle communicatie tussen cliënt en advocaat vertrouwelijk is en blijft. Dit is onder meer vast gelegd in artikel 4 van de EU Richtlijn (2013/48/EU)[19], dat betrekking heeft op strafprocedures.
Hieruit volgt dat uitzonderingen op dat beginsel uitsluitend toelaatbaar zijn indien deze bij wet zijn voorzien en noodzakelijk in het belang van (bijvoorbeeld) de nationale veiligheid. Bovendien volgt uit het rechtsstatelijk beginsel van machtenscheiding dat *voorafgaande* controle op de toepassing van zulke uitzonderingen nodig is, onafhankelijk van het orgaan dat tot die toepassing besluit. Anders zou onvoldoende waarborg tegen misbruik van de bevoegdheden bestaan en daarmee hoe dan ook een zeker 'chilling effect' op het vertrouwen dat op het beroepsgeheim van advocaten geen onterechte inbreuken worden gemaakt.

Waarborging vertrouwelijkheid bij huidige WIV 2002 en bij wetsvoorstel onvoldoende

Van een vergelijkbaar zorgvuldig systeem als door de Hoge Raad is ontwikkeld en dat ervoor waakt dat vertrouwelijke communicatie tussen een advocaat en zijn cliënt niet ter kennis van de overheid komt is noch bij de huidige WIV noch bij het wetsvoorstel enige sprake. Er is immers niet voorzien in voorafgaande onafhankelijke controle en het toezichtsorgaan is niet bij machte onrechtmatige onderscheppingen van vertrouwelijke informatie te voorkomen of te beëindigen. En aan de advocaat in kwestie wordt - geheel anders dan in het door de Hoge Raad opgetuigde systeem - door de AIVD helemaal niets gevraagd. Integendeel, de AIVD doet zijn best om de advocaat geheel in het ongewisse te laten over het feit dat de overheid beschikt over de vertrouwelijke communicatie.
Sterker nog, uit een recent aan de civiele rechter voorgelegde casus blijkt dat het bestaande onafhankelijke toezicht op het onderscheppen van verschoningsgerechtigde informatie door de AIVD en de Minister werd genegeerd. Het huidige toezicht heeft geen enkele effectieve werking. In de periode september 2012 - augustus 2013 constateerde de CTIVD dat bij twee AIVD operaties sprake was van het uitwerken van gesprekken met verschoningsgerechtigden. Zij is van oordeel dat dit

[19] *"De lidstaten eerbiedigen het vertrouwelijke karakter van de communicatie tussen de verdachten of beklaagden en hun advocaat bij de uitoefening van het recht op toegang tot een advocaat op grond van deze richtlijn. Die communicatie omvat ontmoetingen, briefwisseling, telefoongesprekken en elke andere vorm van communicatie die krachtens het nationale recht is toegestaan."* De geheimhoudingsplicht is in Nederland vastgelegd in artikel 10a lid 1 sub e en 11a Advocatenwet en in de Gedragsregels voor advocaten (regel 6). Schending van de geheimhoudingsplicht is strafbaar op grond van artikel 272 wetboek van strafrecht. Het ter handhaving van de geheimhoudingsplicht benodigde verschoningsrecht ligt vast in artikel 218 wetboek van strafvordering en artikel 165 lid 2 sub b wetboek van burgerlijke rechtsvordering.

uitwerken in beide gevallen niet proportioneel was (niet nodig dus) en daarmee onrechtmatig. In een van deze gevallen constateert de CTIVD dat de AIVD er *bewust* op gericht was kennis te nemen van de verschoningsgerechtigde gesprekken (de AIVD zocht dus bewust naar deze 'bijvangst', waardoor van echte '*bij*vangst' geen sprake meer is.[20] De opmerkingen van de CTIVD hebben er niet toe geleid dat het uitwerken van vertrouwelijke gesprekken werd gestaakt. Aan een situatie die door een onafhankelijke, gespecialiseerde commissie als onrechtmatig werd gekwalificeerd, kwam desondanks geen einde.

De civiele rechter moest er aan te pas komen om te voorkomen dat deze evident onrechtmatige situatie zonder meer zou worden voortgezet. Maar de rechter kon natuurlijk niet meer voorkomen dat vertrouwelijke informatie bij de overheid terecht kwam want dat was al geschied en is onomkeerbaar. In een door een advocatenkantoor en de Nederlandse Vereniging van Strafrechtadvocaten aangespannen voorlopige voorzieningen procedure oordeelde de rechtbank Den Haag op 1 juli 2015 dat de Staat:

(1) het (direct en indirect) tappen, ontvangen, opnemen, afluisteren en uitwerken van elke vorm van communicatie van en met advocaten te staken en gestaakt te houden,
(2) ter bescherming van het verschoningsrecht van advocaten een onafhankelijk orgaan in het leven moet roepen dat in ieder geval de bevoegdheid heeft om de uitoefening van bijzondere bevoegdheden te voorkomen of te beëindigen (bindend dus) en
(3) uit de inzet van bijzondere bevoegdheden verkregen verschoningsgerechtigde informatie, zonder dat een voorafgaande onafhankelijke toets met betrekking tot de rechtmatigheid heeft plaats gevonden, niet meer aan het openbaar ministerie mag verstrekken.[21]

<u>Onafhankelijk voorafgaand rechterlijk toezicht is nodig in een rechtsstaat</u>

De ACS pleit er dan ook voor dat specifieke maatregelen worden genomen om via de wet te waarborgen dat sprake is van effectieve, voorafgaande controle op elke (toepassing van een) bevoegdheid van de AIVD welke mee kan brengen dat vertrouwelijke communicatie van een advocaat, direct of indirect, bewust of onbewust, bijvangst of hoofdvangst ter kennis van de AIVD komt. Die controle moet worden uitgeoefend door een onafhankelijk orgaan dat geen binding heeft met (een onderdeel van) het ministerie en in staat is tot een onpartijdig oordeel. Dat controlerend orgaan dient bovendien de effectieve mogelijkheid te hebben om potentieel onrechtmatige situaties en situaties waarbij niet voldaan wordt aan noodzakelijkheid, doelbinding, proportionaliteit of subsidiariteit te voorkomen, te (doen) staken en gestaakt te houden. Zijn oordelen zijn dus bindend.

Gelet op de eisen die aan een dergelijk controlerend orgaan gesteld moeten worden komt al gauw de onafhankelijke rechter in beeld. En waarom ook niet? Opvallend is dat de rechter in het wetsvoorstel al in twee gevallen een rol speelt. Het zonder toestemming van betrokkenen openen van brieven is slechts mogelijk nadat de rechtbank Den Haag daartoe een voorafgaande last heeft gegeven.[22] En de uitoefening van bijzondere bevoegdheden jegens een journalist, waarbij die uitoefening gericht is op
het achterhalen van de bron van de journalist, is slechts toegestaan na voorafgaande toestemming van de rechtbank Den Haag.[23]

[20] CTIVD Toezichtsrapport (nr. 40) inzake de inzet van de afluisterbevoegdheid tot de selectie van sigint door de AIVD. September 2012-augustus 2013, gepubliceerd op 6 augustus 2014 en aangehaald in de uitspraak van de rechtbank Den Haag d.d. 1 juli 2015.
[21] Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436.
[22] Artikel 29 van het wetsvoorstel.
[23] Artikel 24 lid 4 van het wetsvoorstel.

Het ligt daarom voor de hand de onafhankelijke, voorafgaande controle en bevoegdheden om onrechtmatige situaties te voorkomen en te beëindigen in handen te leggen van een, eventueel te specialiseren, rechter. Om kennisneming door de AIVD van bijvangst te voorkomen zou overwogen kunnen worden het systeem van nummerherkenning ook toe te passen op AIVD tapgesprekken. Met betrekking tot de toetsing van 'bijvangst' kan gedacht worden aan interventie van een onafhankelijk toezichtsorgaan van de Orde zelf waarbij alleen deze toezichthouder de inhoud van die communicatie verneemt en - zo nodig - selecteert. Constateert deze toezichthouder dat sprake is van ontoelaatbare betrokkenheid van de advocaat waardoor sprake is van misbruik van het verschoningsrecht, dan kan het de betreffende onderdelen van de communicatie selecteren.
Een specifieke regeling voor verschoningsgerechtigde informatie is niet alleen wenselijk, maar ook nodig om redenen die door de rechtbank Den Haag in haar uitspraak als volgt worden omschreven[24]:

> *"(...) inbreuk op het verschoningsrecht van zowel journalisten als advocaten [heeft]ernstige gevolgen voor de beginselen van de democratische rechtsstaat. De enkele mogelijkheid van inbreuken op het verschoningsrecht van advocaten raakt aan de vertrouwelijkheid van de communicatie tussen advocaten en hun cliënten en daarmee aan het recht op een effectieve verdediging en de toegankelijkheid van advocaten. Daarmee is deze inbreuk in zekere zin ook onomkeerbaar. Gelet op de grote gevolgen van (mogelijke) inbreuken op het verschoningsrecht van advocaten en nu misbruik in individuele gevallen potentieel gemakkelijk is, is de voorzieningenrechter van oordeel dat, overeenkomstig de overwegingen van het EHRM in § 98 van de Telegraafzaak[25], het zeer wenselijk ('desirable') is dat er onafhankelijk toezicht is op de uitoefening van de bijzondere bevoegdheden, waarbij het toezichthoudende orgaan onder meer de bevoegdheid moet hebben om de uitoefening van die bijzondere bevoegdheden tegen te gaan of te beëindigen.*

In zijn schriftelijke reactie aan de Kamer op de uitspraak van de rechtbank Den Haag heeft de minister inmiddels laten weten dat *"het kabinet wil voorzien in een vorm van onafhankelijke toetsing bij het tappen van advocaten."*[26] Of hij daarbij voorafgaande toetsing van een onafhankelijke rechter in gedachten heeft is niet duidelijk.

De ACS beveelt aan dat die toetsing zowel het directe als het indirecte tappen van advocatengesprekken zal omvatten en neemt aan dat de Orde van Advocaten gelegenheid krijgt input hierop te geven. Gelet (1) op het bijzondere karakter van verschoningsgerechtigde informatie, (2) op de waarde van een volledige bescherming daarvan in een rechtsstaat en (3) op het feit dat het wetsvoorstel al een rol geeft aan de onafhankelijke rechter bij het briefgeheim en bij de bronbescherming van journalisten, zou het naar de mening van de ACS ronduit onverstandig en onbegrijpelijk zijn als deze controlefunctie niet in handen van de onafhankelijke rechter zou worden gelegd. De ACS voelt zich hierin gesteund door het Europese Hof, die het in een zaak tegen Nederland[27] als volgt formuleerde:

---

[24] Zie ook de brief van 26 mei 2015 van het Nederlandse Juristen Comité voor de Mensenrechten (NJCM) aan de rechtbank waarin een overzicht wordt gegeven van de jurisprudentie van het EHRM en de voorstellen van de Orde voor een onafhankelijke, voorafgaande toetsing ter waarborging van de vertrouwelijkheid van advocaat - cliënt communicatie wordt gesteund.

[25] Paragraaf 98: The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see Klass and Others v. Germany, 6 September 1978, § 56, Series A no. 28, and Kennedy, cited above, § 167). Daarnaast kan ook nog gewezen worden op de EHRM uitspraak inzake Aalmoes c.a. vs. Nederland (EHRM 25 november 2004, nr. 16169/02).

[26] Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, r.o. 4.10.

[27] Aalmoes and others vs The Netherlands, 25 november 2004, 16269/02. Zie ook De Telegraaf vs The Netherlands, 22 november 2012, nr. 39315/06, par. 98 en Kennedy vs UK, EHRM 18 mei 2010, nr. 26839/05, par. 167.

"....the Court considers that it is clearly in the general interest that any person who wishes to consult a lawyer should be free to do so under conditions which favour full and uninhibited discussion. It is for this reason that the lawyer-client relationship is, in principle, privileged (see Foxley v. the United Kingdom, no. 33274/96, § 43, 20 June 2000). The suggestion that information conveyed by or to a lawyer in the latter's professional capacity is susceptible to interception, particularly by criminal investigation authorities who may have a direct interest in obtaining such information, is not in keeping with the principles of confidentiality and professional privilege attaching to relations between a lawyer and his or her clients. It is for this reason that, in principle, lawyers have in their professional contacts with clients a reasonable expectation of protection and respect for their professional privacy.

In order to secure respect for this reasonable expectation, it is therefore required that the interception of telecommunications be subject to an adequate system of supervision. In this area, faced with evolving and sophisticated technology and the possibility of human error or abuse, the Court considers that it is in principle desirable to entrust the supervisory control to a judge."

Deze zaak ging over indirect tappen ten gevolge van de uitoefening van *strafvorderlijke* bevoegdheden, niet over geheime inlichtingen- en veiligheidsdiensten. Het EHRM onderkent dat opsporingsinstanties een direct belang kunnen hebben bij dergelijke informatie. Het EHRM onderkent voorts dat in de wereld van onderschepping van communicatie de technologie grote sprongen maakt, waardoor steeds meer onderschept kan worden, en onderkent dat menselijke fouten en misbruik door de overheid reëel zijn. Om al deze redenen acht het Hof controle door de rechter wenselijk. Dit moet dan temeer gelden voor onderscheppingen door de AIVD, simpelweg omdat de AIVD minder transparant is dan opsporingsinstanties. Deze omstandigheid pleit er te meer voor een onafhankelijke rechter in te schakelen bij het voorafgaande toezicht op het gebruik van bijzondere bevoegdheden waarbij vertrouwelijke advocaat - cliënt communicatie betrokken is. De Minister suggereert nog gebruik te maken van de mogelijkheid om vertrouwelijk materiaal van advocaten, dat ter kennis van de AIVD is gekomen, niet aan het OM ter beschikking te stellen zodat die informatie niet voor het bewijs in strafzaken kan worden gebruikt. Daarmee miskent de Minister echter het rechtsstatelijk karakter van de vertrouwelijkheid van de communicatie tussen de advocaat en zijn cliënt. Het enkele feit dat de mogelijkheid wordt geboden of in stand gelaten dát een overheidsfunctionaris, zoals een medewerker van de AIVD, door direct of indirect tappen kennis krijgt van die vertrouwelijke informatie doet al afbreuk aan de Nederlandse rechtsstaat. Om die reden is dit al niet toegestaan en moeten we het ook niet willen.
Bewijsuitsluiting neemt bovendien niet weg dát de vertrouwelijkheid van de communicatie al onomkeerbaar is geschonden op het moment dat de AIVD daarvan kennis krijgt. Juist om dit te kunnen voorkomen is - met betrekking tot communicatie welke langs strafvorderlijke weg ter kennis van de overheid is gekomen - ten aanzien van indirect tappen ('bijvangst') het systeem van nummerherkenning ingevoerd. Alleen langs deze weg is een inbreuk op die vertrouwelijkheid door de overheid te waarborgen.

De Minister suggereert voorts, of houdt het beeld in stand, dat het onder geen enkele omstandigheid kunnen kennis nemen van communicatie tussen de advocaat en de cliënt tot onaanvaardbare veiligheidsrisico's zou kunnen leiden. Deze stelling wordt geponeerd alsof de juistheid daarvan vanzelfsprekend is, maar dat is niet het geval. Niet valt in te zien dat communicatie tussen de advocaat en zijn cliënt tot onaanvaardbare veiligheidsrisico's leidt. De Minister licht de stelling nergens toe, laat staan dat hij deze stelling aannemelijk maakt.

Bovendien moet uitgangspunt zijn dat de overheid erop dient te vertrouwen dat advocaten hun communicatie met cliënten niet voor onrechtmatige doeleinden gebruiken. Daarvoor is alle reden: advocaten worden vóórdat zij worden beëdigd gescreend en staan onder disciplinair toezicht. Tegenover het privilege van de vertrouwelijkheid, dat zoals boven beschreven om rechtstatelijke redenen is verleend, staat immers ook de verantwoordelijkheid om daarmee zorgvuldig om te gaan. Ook dat is vast gelegd in de wet.[28] In een eventuele tuchtprocedure en bij een verzoek tot inlichtingen of een onderzoek van de deken is de advocaat verplicht alle benodigde inlichtingen te verstrekken en kan hij zich niet op zijn geheimhoudingsplicht beroepen[29]. Langs deze weg kan getoetst worden of een advocaat op zorgvuldige wijze met zijn verschoningsrecht om gaat.

Bovendien moet worden bedacht dat de enkele mogelijkheid van misbruik, zelfs volgens de minimumwaarborgen van het EVRM, nog niet op weegt tegen de noodzaak de vertrouwelijkheid van de communicatie tussen advocaat en cliënt te beschermen[30]. Anders zou die rechtstatelijke vertrouwelijkheid binnen de kortste keren worden uitgehold. Omdát vertrouwelijkheid een noodzaak is, heeft de overheid een positieve verplichting om er voor te zorgen dat die vertrouwelijkheid effectief gewaarborgd wordt. Dit wetsvoorstel biedt geen enkele waarborg voor die vertrouwelijkheid en doet daarom afbreuk aan de Nederlandse rechtsstaat.

Indien - in een geval dat sprake is van betrokkenheid bij ernstige strafbare feiten van de advocaat zelf - een controle mogelijkheid al noodzakelijk zou worden geacht, dan dient zo'n controle te geschieden op een wijze welke garandeert dat door die controle de overheid niet alsnog op de hoogte raakt van individuele vertrouwelijke communicatie tussen een advocaat en zijn cliënt. Gedacht kan dan worden aan een vorm van tussenkomst door een onafhankelijk toezichtsorgaan van de Orde zelf waarbij alleen deze toezichthouder de inhoud van die communicatie verneemt en - zo nodig - selecteert. Constateert deze toezichthouder dat sprake is van bedoelde betrokkenheid van de advocaat waardoor sprake is van misbruik van het verschoningsrecht, dan kan het de betreffende onderdelen van de communicatie selecteren.
Alleen door een dergelijk stelsel van checks and balances kan worden voorkomen dat burgers - zoals bij aanvaarding van het wetsvoorstel het geval zou zijn - *te allen tijde* hebben te vrezen dat zij door de AIVD of de MIVD kunnen worden afgeluisterd wanneer zij communiceren met een advocaat. Die vrees en het 'chilling effect' daarvan zou de rechtsstaat ernstige schade berokkenen. Het is minst genomen opmerkelijk dat een kabinet dat enerzijds Den Haag als juridische hoofdstad (verder) wil profileren anderzijds zo gemakzuchtig met deze vertrouwelijkheid om gaat. Met de mond wordt het belang van waarborging van de rechtsstaat met zijn checks and balances beleden, maar als het op zelf toepassen aankomt geeft het kabinet niet thuis.

De ACS constateert dat er bij verscheidene maatschappelijke organisaties substantiële kritiek bestaat over de wijze waarop de AIVD in de praktijk met persoonlijke gegevens van individuele burgers om gaat. Die kritiek is samen te vatten onder de noemer dat het wetsvoorstel de AIVD te veel en te vergaande bevoegdheden geeft om persoonsgegevens te verwerken zonder dat daartoe strikte noodzaak bestaat en zonder dat daarbij is voorzien in voldoende effectief en onafhankelijk toezicht. Niet tegemoet komen aan deze kritiek zal het aanzien van de AIVD nog verder verslechteren.

---

[28] De advocaat moet *"onafhankelijk ten opzichte van zijn cliënt zijn (...) integer zijn en zich onthouden van enig handelen dat een behoorlijk advocaat niet betaamt"* (artikel 10 lid 1 sub a en d Advocatenwet).
[29] Gedragsregel 37
[30] EHRM 25 maart 1992, Campbell vs UK, par. 52

INTERNETCONSULTATIE
WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Status per 20150901

1.	**INLEIDING/ HISTORIE**	Uit de voorgeschiedenis van de Wet op de inlichtingen en veiligheidsdiensten (hierna te noemen: 'WIV') blijkt dat na de terroristische aanslagen van 11 september 2001 ('9/11') de behoefte naar terrorismebestrijding binnen Europa is versterkt. De brief van toenmalig President George W. Bush aan de Europese Commissie droeg uiteindelijk bij aan de expliciete grondslag voor onder meer dataretentie en samenwerkingen tussen de inlichtingen- en veiligheidsdiensten en politiediensten. '9/11' heeft niet alleen invloed gehad op de inlichtingen en veiligheidsdiensten, maar ook op de reikwijdte van dataretentie, met als gevolg dat die niet alleen tot terrorismebestrijding diende maar ook bevoegdheden met betrekking tot de vervolging van (andere) strafbare feiten omvat. 9/11 heeft geleid tot de vraag naar de noodzaak voor en de mogelijkheid van effectieve, technisch onafhankelijke reguleringsinstrumenten die voor het uitbreiden van opsporingsbevoegdheden om terrorismebestrijding te waarborgen. In de Verenigde Staten heeft Obama in de zomer van 2014, naar aanleiding van Snowden een onafhankelijk comité Clarke ingeschakeld, dat heeft onderzocht in hoeverre het post-9/11 staatsveiligheidsbeleid zich verhoudt tot de Amerikaanse en universele grondrechten. Een groot deel van de aanbevelingen in het rapport 'Liberty and Security in a Changing World' over verbetering in de drempel van het verzamelen van data, verbetering van de gerechtelijke toetsing van verzoeken, minimalisatie van data, relevantie van de data, duur van dataretentie en transparantie is begin 2014 al doorgevoerd in wet- en regelgeving en recent is de Amerikaanse Freedom Act in werking getreden, waarin deze verbeterpunten verzameld en gestructureerd zijn. In Europa was na de Snowden-onthullingen de Dataretentierichtlijn en daarop gebaseerde c.q. daaraan gerelateerde nationale wet- en regelgeving niet aangepast of onder het vergrootglas gelegd. Hoewel het in de rede had gelegen dat zowel Europese als nationale wet- en regelgevers zelf een herijking van dataretentie hadden toegepast, moest het Europees Hof van Justitie er aan te pas komen om de Dataretentierichtlijn ongeldig te verklaren. Het Europese Hof stelt terecht vast dat de Dataretentierichtlijn onvoldoende waarborgen geeft voor de grondrechten zoals in het bijzonder het recht op bescherming van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Verder geeft het Europese Hof een aantal fundamentele handvatten, die hieronder eveneens als essentiële aanbevelingen worden gesteld voor de wetgever om onderhavige WIV wetswijziging onder de loupe te nemen en structureel aan te passen zodat het op z'n minst voldoen aan die fundamentele beginselen. Immers, ook de volgende keer zal het Europese Hof een wet – inclusief enige wijziging van de WIV – daarop gaan toetsen.

2.	**DOEL WETSWIJZIGING**	In Nederland heeft de overheid de afgelopen jaren al diverse wetsvoorstellen omtrent privacy, cybersecurity, meldplichten, data-lekken en dataretentie gedaan, waarbij iedere keer blijkt dat dit een complex samenspel van vraagstukken, overlappende spanningsvelden en conflicterende rechten en plichten is. Het zou in de lijn der verwachting liggen dat de wetgever op basis van alle bovenstaande informatie lering trekt en de evidente raamwerken gebruikt om de overlappende spanningsvelden beter te kunnen coördineren en zorgen voor een duidelijke lijn op gebied van toegang, bescherming van persoonsgegevens en de nationale veiligheid. De WIV is sinds de inwerkingtreding in 2002 al verschillende malen geëvalueerd en ingeperkt. Volgens de minister Binnenlandse zaken en koninkrijksrelaties (BZK) biedt de huidige WIV onvoldoende mogelijkheden voor het gebruik van nieuwe technologische ontwikkelingen in de informatie en communicatietechnologie, en blijkt de huidige WIV in de praktijk onvoldoende technologisch neutraal te zijn, reden waarom de WIV aangepast te worden.
3.	**CONCEPT WETSWIJZIGING**	De taken en bevoegdheid van de Algemene Inlichtingen- en Veiligheidsdiensten en de Militaire Inlichtingen en Veiligheidsdiensten (hierna gezamenlijk: '*Veiligheidsdiensten*') wil de minister BZK meer laten aansluiten op de huidige en nieuwe technologische ontwikkelen zoals het verzamelen en verwerken van (persoons)gegevens door de Veiligheidsdiensten voor onderzoek en data-analyse in het kader van de nationale veiligheid. De minister BZK geeft aan zich ervan bewust te zijn dat deze taken een beperking vormen op het recht op eerbiediging van de persoonlijke levenssfeer en legt in de memorie van toelichting op het wetsvoorstel WIV uit dat de persoonlijke levenssfeer onder voorwaarden kan worden beperkt ter bescherming van de nationale veiligheid. In alle gevallen moet daarbij worden voldaan aan de eisen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit, aldus de minister. Deze waarborgen zouden er voor moeten zorgen dat de inbreuk op de persoonlijke levenssfeer die de inzet van bijzondere bevoegdheden in het belang van de nationale veiligheid tot gevolg kan hebben, in balans is met het recht op bescherming van de persoonlijke levenssfeer van de burger waarmee het wetsvoorstel WIV volgens de minister aan de wettelijke vereisten voldoet. Helaas is dat nog niet correct en accuraat. De minister gaat er gemakshalve aan voorbij dat niet alleen de bovengenoemde waarborgen voor het verwerken van persoonsgegevens door de Veiligheidsdiensten in acht genomen moeten worden, maar het massaal verzamelen van persoonsgevoelige informatie dient van geval tot geval bekeken te worden, dient alleen strikt noodzakelijk te zijn, en zal feitelijk in geen enkele geval gerechtvaardigd zijn. Daarnaast dient de verzameling van gegevens op z'n minst (a) beperkt te worden tot het absolute minimum (data-minimalisatie), (b) alleen gebruikt voor een duidelijk en nauwkeurig omschreven doel waarbij er sprake is een daadwerkelijke bedreiging van de openbare veiligheid (doel en proportionaliteit van gebruik), en (c) de verzamelde

		gegevens slechts beperkt bewaard te worden èn vervolgens direct en permanent vernietigd te worden (dataretentie en data-vernietiging). Kort gezegd zou het gebruik van persoonsgegevens verzameld door communicatie- en telecommunicatiediensten door Veiligheidsdiensten neer komen op de volgende vier stadia: (a) beschikbaarheid, (b) toegang, (c) dataretentie en (d) het gebruik. Deze stadia worden ook aangeduid als Data Life Cycle. Dit verzamelbegrip is in 2014 mede opgenomen in de, in samenspraak met de Europese Commissie (in het bijzonder DG Connect en DG Justice) en ENISA, door de Drafting Group van de EC Cloud Select Industry Group, opgestelde Cloud Service Level Agreement Standardisation Guidelines, en wordt eveneens verwerkt in de nieuwe ISO/IEC 19086 normen. In het bijzonder wordt hier verwezen naar de Hoofdstukken 2, 5.3, 6.3 en 6.4 en 6.5 van die Guidelines. Arthur's Legal is een van de experts van voornoemde Drafting Group, en is mede-auteur van voornoemde Guidelines en ISO/IEC normen.
4.	**DATA LIFE CYCLE**	In het kader van de nationale veiligheid mogen de Veiligheidsdiensten binnen geldende wet- en regelgeving (persoons)gegevens verzamelen en verwerken over het communicatie- en telecommunicatieverkeer van gebruikers. Hierdoor blijven ook alle communicatie- en telecomproviders verplicht tot het verzamelen en **beschikbaar** houden van gegevens van alle burgers. Aanbieders van clouddiensten zijn met de huidige wet niet verplicht om gegevens te bewaren, maar door de medewerkingsverplichting voor de aanbieders van clouddiensten zouden zij nu toch verplicht worden gegevens beschikbaar te houden zoals de inhoud van een mailbox van een gebruiker, voicemail of andere gegevens die in data-opslagdiensten zijn opgeslagen. Het Europese Hof van Justitie heeft in haar arrest over de Dataretentierichtlijn hierover geen bezwaren aangegeven met het oog op de veiligheid en het belang van terrorisme bestrijding. Wel geeft het Europese Hof van Justitie aan dat de categorieën van de data nauwkeurig moeten worden omschreven. Volgens artikel 52 lid 1 van het Handvest moeten beperkingen op het in dit Handvest erkende rechten en vrijheden, als artikel 7 en 8, bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen, en kunnen, met inachtneming van het **evenredigheidsbeginsel**, alleen beperkingen worden gesteld indien zij **noodzakelijk** zijn en daadwerkelijk aan door de EU erkende doelstellingen van het algemeen belang of aan de eisen van de bescherming van rechten en vrijheden van anderen, beantwoorden. Het Hof geeft hiervoor in ieder geval de volgende fundamentele handvatten: (i) Er dient er een **verband** te bestaan tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. (ro. 59) (ii) De toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens moet **onderworpen zijn aan enige voorafgaande controle door een rechterlijke instantie** of een onafhankelijk administratieve instantie die hierover uitspraak doet en waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel. (ro 60)

(iii) Het **bewaartermijn** moet worden verkort en op basis van objectieve criteria worden vastgesteld om proportionaliteit te waarborgen. (ro 64)

(iv) Er moeten duidelijke en precieze regels betreffende de reikwijdte en de toepassing van de maatregelen opgesteld worden die minimale vereisten opleggen ten aanzien van de toegang tot en exploitatie van de gegevens, zodat personen van wie gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens **doeltreffend worden beschermd tegen het risico van misbruik, elke onrechtmatige raadpleging en onrechtmatig gebruik**. (ro 66)

De **toegang** tot informatie dient onder meer volgens het Europese Hof van Justitie in datzelfde arrest te worden onderworpen aan een **onafhankelijke toets**. De wetgever heeft in dit wetvoorstel WIV, de minister als enige deze bevoegdheid gegeven, waarbij er geen sprake is van een gerechtelijke toetsing van de gegevens en data door een onafhankelijk orgaan. Daarnaast hoeft niet altijd de minister toestemming te geven voor het intern of extern verstrekken van gegevens, de verantwoordelijke van de dienst mag dat ook, zowel nationaal als internationaal. Dit is onwenselijk. Juist omdat de grootste zorgen omtrent bescherming van persoonsgegevens is dat de overheid ongehinderd kan mee-/afluisteren en het cross-over data gebruik van de overheid (nationaal en internationaal). Geen enkele wet mag natuurlijk nieuwe (Nederlandse) Prism/Patriot- of Freedom Act en dataretentie issues veroorzaken.

Wat betreft **dataretentie** wordt daar in de WIV praktisch geen aandacht aangegeven. In het kader van de nationale veiligheid mogen gegevens minimaal drie maanden en maximaal twaalf maanden bewaard worden, en worden verlengd met drie jaar. Echter, er dient een onderscheid te worden gemaakt tussen noodzakelijke/relevante informatie, oftewel een minimum vereiste. Dit minimum vereiste dient wederom te worden getoetst door een onafhankelijke gerechtelijke instantie. Uit de aanbevelingen van het comité Clarke volgt dat verzamelen en bewaren van data relevant dient te zijn voor het doel waarvoor de data zijn verzameld. Dat houdt in dat bij een opsporingsonderzoek de eerste toestemming door een gerechtelijk orgaan breed kan zijn voor een bepaalde tijd, na afloop van de bepaalde tijd zou de Veiligheidsdienst weer terug naar het gerechtelijk orgaan moeten gaan voor toestemming voor de relevante data. De verlening van de bewaartermijn dient eveneens getoetst te worden door een onafhankelijk orgaan.

Het **gebruik** van de data wordt zowel intern als extern mogelijk gemaakt door de Veiligheidsdiensten over en weer. Uit onderzoek dat bijvoorbeeld bij de Politiewet massaal fouten in worden gemaakt, wegens de onduidelijke scheidslijn tussen het Wetboek van Strafvordering en de Politiewet. Dit heeft ertoe geleid dat een politieambtenaar in feite toegang heeft tot alle gegevens van alle burgers. Daarnaast blijkt de notificatieplicht van art. 126bb Wetboek van Strafvordering in de praktijk massaal te worden genegeerd, omdat dit geen prioriteit kent binnen het Openbaar Ministerie, en dit op geen enkel moment wordt getoetst. En dit is nog maar een onderdeel waarop de bijzondere bevoegdheden van de Veiligheidsdiensten op zien.

		De Veiligheidsdiensten kunnen de persoonsgevoelige informatie ook aan derden overdragen in het kader van het bieden van hulp en overleg voeren met soortgelijke diensten. Het bevorderen van de nationale en internationale samenwerking voor opsporingen heeft er mede voor gezorgd dat in de praktijk het principe 'voor wat hoort wat' tussen de diensten is ontstaan. De praktijk van het over en weer uitwisselen van data met buitenlandse opsporingsinstanties onder andere via de afspraken onder Mutual Legal Assistance Treaty ('MLAT') waarbij Nederland partij is versterken de gerezen inbreuken op privacy, en de daardoor ontstane, grote maatschappelijke zorgen bij burgers betreffende overheidsinterventie. Doordat de Veiligheidsdiensten steeds meer elektronische communicatiemiddelen onderzoeken en ook gebruik van maken voor het verzamelen van (persoons)gegevens wordt in het wetsvoorstel WIV de middelen (o.a. hacken) die openstaan voor data-analyse door Veiligheidsdiensten technologisch neutraal gemaakt. Het is bij de minister BZK bekend dat met deze manier er onvermijdelijk gegevens van personen die niet de aandacht van de diensten hebben ook worden verwerkt, omdat deze nu eenmaal een logisch en onlosmakelijk onderdeel uitmaken van een gegevensbestand, die noodzakelijk is om de data-analyse mogelijk te maken, aldus de minister BZK. Met name deze **'bijvangst'** van de data-analyse kunnen de Veiligheidsdiensten delen met een beperkte kring van derden, zoals (internationale) Veiligheidsdiensten. Bovendien is dergelijke bijvangst niet nodig en noodzakelijk in het kader van de nationale veiligheid en niet noodzakelijk om met derden te delen. De Minister kan via dit kanaal ongehinderd meeluisteren en cross-over data gebruiken via deze nieuwe bevoegdheden. Hiermee bevestigt het wetsvoorstel WIV dat de wetgever blijkbaar graag wil dat de Veiligheidsdiensten massaal alle soorten gegevens van alle burgers kunnen verzamelen onder het mom van nationale veiligheid. Dusdanige overheidsinterventie onder het mom van nationale veiligheid is niet rechtvaardig als de privacy waarborgen achterwege worden gelaten. Het is ook in strijd met nationale en Europese wet- en regelgeving.
5.	**CONCLUSIE**	De doelstelling van de wetswijziging zou een balans moeten zijn tussen (i) de toegangsbevoegdheden van Veiligheidsdiensten in belang van de nationale veiligheid en (ii) het recht op bescherming van de persoonlijke levenssfeer van de burger en bescherming van persoonsgegevens. Deze doelstelling wordt echter niet gehaald met het onderhavige wetsvoorstel, met name omdat de wetswijziging (i) onvoldoende de waarborgen van legitimiteit, noodzakelijkheid, proportionaliteit en subsidiariteit met massaal verzamelen van data niet naleeft, (ii) de data en toegang niet objectief en gerechtelijk wordt getoetst, en (iii) onvoldoende het primaire doel – bescherming van persoonsgegevens en de persoonlijke levenssfeer van de burgers – dient. De bescherming van de nationale veiligheid en democratie mag in geen geval een direct of indirect excuus zijn voor de onbeperkte monitoring en analyse van persoonsgegevens zonder enige onafhankelijke toetsing op proportionaliteit, data minimalisatie, dataretentie, en geheimhouding daarvan.

		Zo blijft voor toegang tot (persoons)gegevens in het kader van de nationale veiligheid, de minister als enige bevoegd. Dit is geen gerechtelijk onafhankelijk toezicht, een systeem dat zelfs in de Verenigde Staten wordt gehandhaafd, welke inmiddels dus zelfs is verbeterd. Kort gezegd dient het gebruik van informatie door de Veiligheidsdiensten getoetst en gedefinieerd te worden als onderdeel van de Data Life Cycle.
6.	**EXTRA AANBEVELING**	Om het gebruik van gegevens en data door de Veiligheidsdiensten te kwalificeren en te toetsen kan men de heldere opzet voor standaardisatie van data-management, (persoons)gegevensbescherming en informatiebeveiliging waarborgen voor cloud gebruikers, de Privacy Level Agreement (PLA v2.0) als basis gebruiken, opgesteld in opdracht van de Cloud Security Alliance en gesteund door gerenommeerde Europese instanties en organisaties. Arthur's Legal heeft hieraan als co-auteur bijgedragen. Deze PLA is een basisleidraad/raamwerk om te kunnen voldoen aan de EC en nationale regelgeving over de bescherming van persoonsgegevens. Vanwege de elkaar snel opvolgende ontwikkelingen op gebied van technologie en gerelateerde zaken dient extra rekening gehouden te worden met standaardisatie die op z'n minst technologisch model neutraal is en wereldwijd toepasbaarheid is, en een uniform begripsgebruik kent, zonder daarbij inbreuk te maken op de huidige wet- en regelgeving. Dat is eigenlijk makkelijker dan men denkt. Het is te betreuren dat die gedachte, basis en structuur in het huidige wetsvoorstel niet is terug te vinden.
7.	**NADERE TOELICHTING**	Arthur's Legal is graag bereid de voorgaande opmerkingen en aanbevelingen desgewenst toe te lichten.

Arthur's Legal, Amsterdam v20150901 / WIV

de Nationale ombudsman

De heer dr. R.H.A. Plasterk
Minister van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011
2500 EA DEN HAAG

Postadres
Postbus 93122
2509 AC Den Haag
Bezoekadres
Bezuidenhoutseweg 151
2594 AG Den Haag
Tel: (070) 356 35 63
Fax: (070) 361 50 72
secretariaat@nationaleombudsman.nl
www.nationaleombudsman.nl
Doorkiesnummer
(070) 3563 680
Datum
26 augustus 2015
Ons nummer
No 2015/300
Uw brief
26 juni 2015
Uw kenmerk
2015-0000352550
Bijlagen
1
Behandelend medewerker
Munish Ramlal
Onderwerp
Conceptwetsvoorstel op de inlichtingen- en veiligheidsdiensten

Geachte heer Plasterk,

Bij brief van 26 juni jl. hebt u de Nationale ombudsman gevraagd om een reactie op het conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20xx (verder: conceptwetsvoorstel Wiv). Met de inzet van de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten wordt doorgaans inbreuk gemaakt op grondrechten van burgers, waaronder het recht op privacy. In dat geval is een stelsel van adequate en effectieve waarborgen en rechtsbescherming door onafhankelijke instanties vereist tegen misbruik van die bevoegdheden. Voorop staat wat mij betreft dat een verruiming van de bevoegdheden van de diensten om een verscherping van de rechtsbescherming vraagt. Klachtbehandeling maakt daarvan deel uit. In mijn schriftelijke reactie beperk ik me tot dit aspect van het conceptwetsvoorstel. Dit onderwerp raakt immers aan de kern van het werk van de Nationale ombudsman. Kort gezegd vind ik de positionering van de klachtbehandeling in een aparte kamer bij de CTIVD onverantwoord. Het risico bestaat dat de klachtbehandeling niet onafhankelijk en onpartijdig is, terwijl de verruimde bevoegdheden te meer onafhankelijke rechtsbescherming vereisen. Ik pleit ervoor om de klachtbehandeling onder te brengen bij een evident onafhankelijk en onpartijdig instituut.

Wetsvoorbereiding
In het wetvoorstel wordt een wetgevingskeuze gemaakt die de bevoegdheid van de Nationale ombudsman verandert. In een dergelijk geval ligt het in de lijn om actief contact te zoeken. Daar zijn bovendien eerder werkafspraken over gemaakt. Dat is bij dit wetsvoorstel niet gebeurd en dat betreur ik zoals ik u bij brief van 8 juli jl. heb laten weten (zie bijlage). Ik zou graag geïnformeerd willen worden over de aanpassingen die u doorvoert op basis van de internetconsultatie.

Huidig stelsel klachtbehandeling
Zoals bekend, kunnen burgers bij u een klacht indienen over de AIVD en bij de minister van Defensie over de MIVD. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (verder: CTIVD) onderzoekt in beide gevallen de klacht en schrijft een niet-bindend advies, eventueel voorzien van aanbevelingen. Op basis van dit advies reageert de verantwoordelijke minister op de klacht. Dit is de eerstelijns klachtbehandeling. Als de betreffende burger het niet eens is met de reactie van de minister, kan de burger een klacht indienen bij de Nationale ombudsman: de tweedelijns klachtbehandeling. Op jaarbasis behandelt de Nationale ombudsman circa 2 klachten over de AIVD en 1 klacht

over de MIVD. Het aantal gevallen is dus beperkt. De ombudsman vormt het sluitstuk voor klachten over de inlichtingen- en veiligheids-diensten. Het huidige, normale regime voor klachtbehandeling is verankerd in de Grondwet en de Algemene wet bestuursrecht (artikel 78a Grondwet en Hoofdstuk 9 van de Algemene wet bestuursrecht). In uw concept-wetsvoorstel wijkt u af van deze wettelijke structuur.

Commissie Dessens
In 2013 verrichtte de Commissie Dessens onderzoek naar de werking van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002). In het advies wordt uitgebreid ingegaan op toezicht en klachtbehandeling. Om deze te versterken, stelt de commissie voor de CTIVD te positioneren als onafhankelijke toezichthouder en klachtbehandelaar. De CTIVD zou twee kamers moeten krijgen: een toezichtkamer en een kamer voor klachtbehandeling. De toezichtkamer zou tot bindende uitspraken moeten komen. De kamer voor klachtbehandeling zou niet-bindende oordelen uitspreken. De Nationale ombudsman krijgt in dit stelsel een rol op de achtergrond. Een burger kan de Nationale ombudsman altijd nog vragen om onderzoek in te stellen. De ombudsman kan zelf beslissen of daartoe aanleiding bestaat of niet.

Conceptwetsvoorstel
In uw conceptwetsvoorstel moet een burger met een klacht over een van de inlichtingen- en veiligheidsdiensten zich wenden tot de betreffende minister.
De desbetreffende minister heeft dan de gelegenheid om zijn zienswijze op de klacht te formuleren. Na deze zienswijze, kan de burger een klacht indienen bij de CTIVD. De klachtenkamer van de CTIVD gaat de klacht onderzoeken en komt tot een oordeel dat bindend is. Na dit oordeel is er geen verdere klachtbehandeling meer en houdt de klachtbehandeling op. De bevoegdheid van de Nationale ombudsman om te oordelen over klachten die betrekking hebben op de AIVD en de MIVD komt daarmee te vervallen. In zoverre wordt het advies van de commissie Dessens om een gang naar de Nationale ombudsman open te houden, niet overgenomen.

Inhoudelijke punten

Risico van afhankelijkheid en partijdigheid
Aan het voorgestelde stelsel van toezicht en klachtbehandeling zitten kanten waar ik vraagtekens bij plaats. Met name heb ik grote moeite met het onderbrengen van zowel het toezicht als de klachtbehandeling bij één organisatie: de CTIVD. Zoals de commissie Dessens en ook de Raad van State hebben overwogen, impliceert een klacht over de handelwijze of bejegening door een dienst ook het toezicht daarop. Bij een gegronde klacht heeft ook de toezichthouder gefaald. Een strikte scheiding van toezicht en onafhankelijke klachtbehandeling zou de schijn van partijdigheid en afhankelijkheid vermijden. Bij klachtbehandeling zijn onafhankelijkheid en onpartijdigheid essentieel. Daarom dient elke schijn van en risico op afhankelijkheid en partijdigheid te worden vermeden. Een burger moet niet terecht komen bij een

klachtbehandelaar die verbonden is met de toezichthouder. Het enkel procedureel scheiden van een kamer voor toezicht en een kamer voor klachtbehandeling is onvoldoende. Een procedurele scheiding is niet zichtbaar. De burger ziet feitelijk één organisatie, met één naam, gevestigd in één bedrijfspand. Het verwijt dat 'de slager zijn eigen vlees keurt' ligt in de lijn der verwachtingen. Ik wil dat de burger het gevoel én de waarborg krijgt dat de klachtbehandeling op een objectieve wijze door een volledig onafhankelijk en onpartijdig instituut plaatsvindt. Ik adviseer u om de klachtbehandeling zo te regelen dat deze daadwerkelijk en zichtbaar gescheiden plaatsvindt van het toezicht.

Mijn voorstel is om de klachtbehandeling onder te brengen bij een onafhankelijk instituut zoals de Nationale ombudsman. De klachtenkamer kan in dat geval ondergebracht worden bij het bureau van de Nationale ombudsman. De ombudsman beschikt in dat geval ook over de benodigde onbeperkte onderzoeksbevoegdheden. Op deze manier worden de voordelen van uw wetsvoorstel behouden en wordt het nadeel van de schijn van en risico op afhankelijkheid en partijdigheid weggenomen. Tevens wordt hiermee aangesloten bij de door de wet voorgeschreven gebruikelijke systematiek voor klachtbehandeling (ex 78a Grondwet en hoofdstuk 9 van de Awb).

Ik ben mij ervan bewust dat er ook praktische of financiële bezwaren bestaan tegen het volledig afscheiden van de klachtbehandeling. Daarbij denk ik aan de benodigde geheimhouding en toegang tot alle staatsgeheime informatie en gaande operaties, de voor het onderzoek vereiste en schaarse kennis en expertise, in verhouding tot de daarmee gepaard gaande kosten. Het beperkt aantal klachten rechtvaardigt evenmin een dure en groots opgezette oplossing. Daarmee rekening houdend zouden zo veel mogelijk de huidige organisatiestructuren benut moeten worden. Ten behoeve van de geheimhouding zouden de dossiers bij de CTIVD kunnen blijven. De Nationale ombudsman krijgt dan de mogelijkheid onderzoek ter plaatse te gelasten en de dossiers bij de CTIVD te raadplegen. Ten einde te beschikken over de voor het onderzoek benodigde kennis, zouden deskundigen, zoals onderzoekers van de CTIVD, kunnen worden geraadpleegd als getuige-deskundigen. Ten overvloede verwijs ik nog naar de kennis en expertise die in de afgelopen jaren is opgedaan binnen mijn bureau waarbij speciaal opgeleide en gescreende medewerkers zorg dragen voor de klachtbehandeling.

Bindende uitspraken
Ik betreur dat de toezichtkamer van de CITVD geen bindende uitspraken kan doen, zoals door de commissie Dessens aanbevolen. De AIVD en de MIVD kunnen met uw nieuwe wetgevingskader ongericht en massaal informatie onderscheppen, analyseren en bewaren van alle burgers in Nederland. Dit is een grote stap op een glijdende schaal en kan worden gekwalificeerd als 'big data analysis'. Als ombudsman vind ik het daarom belangrijk dat de toezichthouder bindende oordelen kan vellen en in staat is om handelingen van de AIVD en MIVD stop te zetten.

de Nationale ombudsman

Ons nummer
No 2015/300

Onderzoek uit eigen beweging
In uw wetsvoorstel is het niet mogelijk voor de klachtbehandelingskamer om een onderzoek uit eigen beweging in te stellen. Dat zou botsen met de bevoegdheid van de toezichtkamer van de CTIVD om een onderzoek uit eigen beweging in te stellen in het kader van het rechtmatigheidstoezicht. Mijn voorstel voor onafhankelijke klachtbehandelaar heft deze botsing op. De CTIVD kan dan een onderzoek uit eigen beweging starten op basis van het eigen mandaat van de rechtmatigheidstoetsing. De onafhankelijke klachtbehandelaar, zoals de Nationale ombudsman , kan dan eveneens een onderzoek uit eigen beweging starten. In dat geval wordt enkel de behoorlijkheid van het handelen van de diensten onderzocht.

Kortom
In uw conceptwetsvoorstel krijgen de inlichtingen- en veiligheidsdiensten ruimere, verregaande bevoegdheden. Des te belangrijker is een goed functionerend systeem van onafhankelijke rechtsbescherming, waarvan klachtbehandeling een onderdeel is. De klachtbehandeling is in uw conceptwetsvoorstel ondergebracht als kamer bij de CTIVD terwijl dezelfde instantie zich bezighoudt met het rechtmatigheidstoezicht. Dat moet wat mij betreft echt anders. Een burger moet niet terecht komen bij een klachtbehandelaar die verbonden is met de toezichthouder, want elke schijn van en risico op afhankelijkheid en partijdigheid dient te worden vermeden. Ik stel voor om de klachtenkamer los te maken van de CTIVD en onder te brengen bij een onafhankelijk instituut zoals de Nationale ombudsman.

Met vriendelijke groet,
de Nationale ombudsman,

Reinier van Zutphen

2108201508057 - 3

de Nationale ombudsman

De heer dr. R.H.A. Plasterk
Minister van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011
2500 EA DEN HAAG

Postadres
Postbus 93122
2509 AC Den Haag
Bezoekadres
Bezuidenhoutseweg 151
2594 AG Den Haag
Tel: (070) 356 35 63
Fax: (070) 360 75 72
secretariaat@nationaleombudsman.nl
www.nationaleombudsman.nl
Doorkiesnummer
(070) 356 36 80
Datum
8 juli 2015
Ons nummer
No 2015/261
Uw brief

Uw kenmerk

Bijlagen

Behandelend medewerker
Munish Ramlal
Onderwerp
Conceptwetsvoorstel Wet op de Inlichtingen- en Veiligheidsdiensten

Geachte heer Plasterk,

Het kabinet heeft op 26 juni jl. ingestemd met het conceptwetsvoorstel Wet op de Inlichtingen- en Veiligheidsdiensten, voorbereid door uw ministerie. In dit wetsvoorstel verliest de Nationale ombudsman de bevoegdheid om klachten te behandelen over de AIVD en de MIVD. Ik vind dat uw departement mij hierover eerder en beter had moeten informeren. Dat lag ook voor de hand omdat met de directeur van uw directie Constitutionele Zaken en Wetgeving (CZW) hierover reeds een werkafspraak lag. Het is namelijk niet de eerste keer dat de Nationale ombudsman geconfronteerd wordt met een conceptwetsvoorstel waarin de burger niet langer bij hem terecht kan. CZW zou alert zijn op conceptwetgeving die raakte aan de positie van de ombudsman.

Het eerste voorval betreft de wijziging van de Notariswet. De ombudsman moest via het Staatsblad vernemen dat de wet gewijzigd was en dat hij niet langer bevoegd was om een categorie klachten over notarissen te behandelen. De tweede situatie deed zich voor bij de ambtelijke voorbereiding van de Gerechtsdeurwaarderswet. De ombudsman moest via het beleidsveld vernemen dat er een wetswijziging in de maak was waardoor burgers niet langer naar de ombudsman zouden kunnen gaan, maar het moesten doen met een geschillencommissie. Dat zou een achteruitgang betekenen in de kwaliteit en laagdrempeligheid van de klachtbehandeling.

Nu doet zich dus een derde geval voor bij de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv). Via informele contacten kwam ik erachter dat de burger met een klacht over de AIVD of de MIVD niet langer bij de ombudsman terecht zou kunnen. Deze moet onder het wetsvoorstel terecht bij de Commissie van Toezicht (CTIVD) voor zijn klacht. Ik vind dat niet zuiver. Toezichthoudende activiteiten van de CTIVD kunnen zich gaan mengen met klachtbehandelings-activiteiten. Dat is vanuit onafhankelijk klachtbehandeling onwenselijk. Om vervolgens dat weer te voorkomen, zal de CTIVD allerlei organisatorische voorzieningen moeten treffen. Dat lijkt me nodeloos complicerend. Ik zal dit punt nog uitgebreider onder uw aandacht brengen via een aparte brief na de zomer, waarin ik reageer op het conceptwetsvoorstel.

[redacted]

de Nationale ombudsman

Ons nummer
No 2015/261

Kortom: ik wil graag een eerdere gelegenheid om mee te denken over conceptwetgeving die raakt aan de bevoegdheden van de Nationale ombudsman. Dat stelt mij in de gelegenheid om mijn kennis in te brengen over klachtbehandeling en het burgerperspectief, zodat goed geïnformeerde keuzes gemaakt worden over de positionering en inrichting van klachtbehandeling. Nu komt de ombudsman pas in beeld bij de internetconsultatie. Ik vind een eerdere betrokkenheid meer in lijn met de positie van een Hoog College van Staat. Graag verzoek ik u om binnen uw organisatie hiervoor aandacht te vragen.

Met vriendelijke groet,
de Nationale ombudsman,

Reinier van Zutphen

NEDERLAND ICT

Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties
De heer dr. R.H.A. Plasterk
Postbus 20011
2500 EA DEN HAAG

Woerden, 31 augustus 2015

Betreft : Reactie Nederland ICT op consultatie wetsvoorstel Wiv
Kenmerk : 40289/LdB/AdJ/JB

Geachte heer Plasterk,

Nederland ICT is de brancheverenigingen van ruim 550 ICT-bedrijven in Nederland. Met een achterban die bijna € 30 miljard omzet en meer dan 250.000 medewerkers telt, is Nederland ICT de belangenbehartiger en vertegenwoordiger van de Nederlandse ICT-sector.

De inzet van ICT draagt bij aan 60 procent van de economische groei in Nederland. 70 procent van alle innovaties is ICT-gerelateerd. Nederland is een aantrekkelijk vestigingsland vanwege haar hoge ICT dichtheid en sterke digitale infrastructuur. Netwerkeffecten zorgen ervoor dat wereldwijd een relatief klein aantal landen een disproportioneel aandeel in de digitale infrastructuur heeft. Nederland heeft daardoor naast de mainports Schiphol en Rotterdam ook twee internet mainports: 's werelds nummer twee internet exchange en 's werelds nummer negen[1]. Nederland profileert zich als vestigingsland mede daardoor terecht als Europese koploper en Digital Gateway to Europe[2]. Het sterke en open Nederlandse digitale ecosysteem heeft een aanzuigende werking op innovatieve bedrijven en zorgt daarmee voor een uitstekende uitgangspositie voor Nederland in de transitie naar vergaande digitalisering van de wereldeconomie.

Deze economische groei wordt mede mogelijk gemaakt door flankerend beleid van de overheid. De overheid richt zich op het stellen van randvoorwaarden en ordenen van deze markt opdat digitale innovatie en groei over de volle breedte van de Nederlandse economie kan plaatsvinden. Belangrijke randvoorwaarden voor de overheid zijn[3]:

- Voldoende concurrentie in de markt zodat een dynamiek van continue investeringen en innovaties blijft bestaan;
- Vrijheid, waaronder hier wordt verstaan keuzevrijheid voor gebruikers, vrij van oneigenlijke invloed van overheden, bedrijven en overige belangengroepen;
- Betrouwbaarheid van netwerken en diensten, in het bijzonder integriteit (juistheid van informatie, geen veiligheidsinbreuken), continuïteit (geen storingen of uitval) en bescherming van persoonsgegevens.

[1] https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size
[2] http://investinholland.com/infrastructure/broadband/
[3] Voortgangsrapportage uitwerking visie op Telecom, internet en media. Kamerstuk, 26643 nr. 345

Borging van deze randvoorwaarden zorgen voor een aantrekkelijk ondernemingsklimaat en vertrouwen onder burgers en bedrijven. Hierdoor kunnen we blijvend profiteren van de toegevoegde waarde van ICT en blijft Nederland een aantrekkelijke vestigingsplaats. Om onze koploperspositie te behouden is het van belang als overheid terughoudend te zijn met het doen van voorstellen die nadelig zijn voor het vertrouwen van burgers en bedrijven, het ondernemingsklimaat en daarmee voor de positie van Nederland als ICT vestigingsland.

Het voorstel van de herziening van de Wet op de inlichtingen- en veiligheidsdiensten is naar de mening van Nederland ICT zo'n voorstel. Het voorstel gaat voorbij aan het beoogde doel van 'technologie onafhankelijk maken van de interceptie', tast de betrouwbaarheid van netwerken en diensten aan, en beperkt de hierboven genoemde vrijheid.

Reactie Nederland ICT op Wiv

Nederland ICT maakt zich ernstige zorgen over de gevolgen van het voorstel voor de nieuwe Wet op de Inlichtingen en Veiligheidsdiensten (Wiv). De nieuwe wet geeft de inlichtingen- en veiligheidsdiensten de bevoegdheid tot massale interceptie van kabelgebonden communicatie.

Nederland ICT heeft grote twijfels over het nut en noodzaak, de transparantie en proportionaliteit, de reikwijdte en toerekening van kosten, de praktische uitvoerbaarheid en het juridisch toetsingskader van de nieuwe bevoegdheden en daarmee het draagvlak voor een dergelijk ingrijpend wetsvoorstel.

De door de wet opgelegde eisen aan een groot aantal bedrijven zullen resulteren in een verlies aan vertrouwen van burgers en bedrijven, in toegenomen onzekerheid en financiële druk voor het bedrijfsleven, minder innovatie, risico's voor de betrouwbaarheid en integriteit van dienstverlening en verslechtering van het internationale imago van Nederlandse als Digital Gateway to Europe.

Belangrijkste bezwaren

De reikwijdte van de nieuwe bevoegdheden is erg groot: in essentie valt elke aanbieder van een dienst die over het internet gegevens uitwisselt, wat voor gegevens dan ook, binnen het kader van de wet.

Het voorgestelde systeem voldoet volgens Nederland ICT niet aan minimale maatschappelijke en rechtsstatelijke verantwoording en toetsing die nodig is om zo'n ingrijpend middel, rechtmatig, te kunnen invoeren. Ook de benodigde transparantie om nut en noodzaak van de programma's van de diensten te kunnen beoordelen ontbreekt voor het huidige voorstel.

Het voorstel geeft geen technische details over de manier waarop de integriteit, beschikbaarheid en vertrouwelijkheid van de getapte data gewaarborgd wordt. Aanbieders krijgen geen compensatie voor schade of verstoring dienstverlening aan gebruikers naar aanleiding van handelen van inlichtingen- en veiligheidsdiensten. Bovendien is, door de geheimhoudingsplicht, de toegankelijkheid van toetsing door een rechter bij een mogelijk bezwaar voor aanbieders in het geding.

Het voorstel is verder onduidelijk over de vraag of het ontsleutelbevel (aanbieders worden geacht mee te werken aan ontsleuteling van versleutelde informatie) het inbouwen van backdoors mogelijk

maakt. Gezien de weerstand die in de nasleep van de onthullingen van Snowden wereldwijd heerst tegen dit soort bevoegdheden zou dit funest zijn voor het vertrouwen van burgers en bedrijven in de integriteit van hun data en daarmee het internet, en zodoende voor de positie van Nederland als aantrekkelijke ICT-vestigingsplaats. De economische schade door het verlies aan vertrouwen in digitale diensten was in de VS groot. Het is zeer onwaarschijnlijk dat dit in Nederland anders zal zijn.

De huidige infrastructuur is niet toegerust op massale interceptie van gegevens. Om te voldoen aan de last voor bulk interceptie zal een kostbare nieuwe interceptie-infrastructuur ontworpen, ontwikkeld, gebouwd en getest moeten worden specifiek voor elk bedrijf.

Het voorstel legt alle kosten bij private partijen, waarbij het in veel gevallen onduidelijk blijft wanneer en hoe bedrijven investeringen moeten doen om de last tot aftappen te faciliteren. Dit heeft een grote remmende werking op de innovatiekracht en de groeipotentie van met name kleine dienstverleners en startups. Uit het wetsvoorstel blijkt dat er zodoende binnen de diensten geen noodzaak is tot het doen van een effectieve proportionaliteitstoets. Een tap dagen langer laten lopen, of het aansluiten van verschillende taps in de hoop op een hit kost de AIVD of de MIVD niets. Het gevaar van '*overreach*' is dan ook prominent aanwezig.

Concluderend
Nederland ICT vraagt de minister het voorstel in de huidige bewoordingen te heroverwegen en samen met de sector na te denken over een wetsvoorstel dat op meer draagvlak bij burgers en bedrijven kan rekenen.

Nederland ICT pleit er voor om bij het opleggen van dergelijke verplichtingen voor het bedrijfsleven altijd de kosten via de Rijksbegroting te laten lopen. Niet alleen is er zodoende democratisch toezicht op de kosten, ook worden de diensten er door financiële overwegingen toe gedwongen hun activiteiten scherp en doelgericht in te zetten. De proportionaliteit is hierdoor beter geborgd.

Meer specifiek vraagt Nederland ICT de minister, in overleg met zijn collega's van Veiligheid en Justitie en Economische Zaken, om:

- Een gedegen onderbouwing van nut en noodzaak van een dergelijk ingrijpend wetsvoorstel.
- Een voorstel hoe in de toekomst op een transparante wijze inzicht gegeven wordt in de reikwijdte van de bevoegdheden van inlichtingen- en veiligheidsdiensten en de wijze waarop deze hun taak uitoefenen. Dit teneinde het vertrouwen van burgers en bedrijven in de integriteit van hun data, het internet en daarmee de digitale economie als geheel te waarborgen.
- Een analyse van het effect dat het wetsvoorstel zal hebben op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

Nederland ICT bedankt u voor de mogelijkheid om te reageren op het voorontwerp voor het wetsvoorstel Wiv. Als u naar aanleiding van deze opmerkingen vragen heeft, ben ik natuurlijk graag bereid een nadere toelichting te geven.

NEDERLAND ICT

In de bijgesloten bijlage treft u een nadere reactie aan op specifieke onderdelen van het voorstel.

Met vriendelijke groet,
Nederland ICT

Lotte de Bruijn,
directeur.

bijlage: 1

BIJLAGE 1.

Nederland ICT vindt het huidige voorstel juridisch problematisch en vaak niet duidelijk. In onderstaande tekst staan de punten die voor Nederland ICT primair onduidelijk zijn. Zonder nadere toelichting is het voor Nederland ICT niet mogelijk het voorstel en de implicaties er van volledig te kunnen inschatten en afdoende te wegen. We vragen de minister daarom bij elk van deze punten een nadere toelichting:

1. Kabelgebonden telecommunicatie:
Ongerichte interceptie was ingevolge artikel 27 Wiv 2002 alleen mogelijk bij niet-kabelgebonden telecommunicatie. In het onderliggende voorstel komt het onderscheid tussen kabel- en niet-kabelgebonden telecommunicatie te vervallen. Met de motivering '*[dat] de basis van het onderscheid tussen de ether en de kabel niet meer te rijmen valt met de voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie*' gaat men voorbij aan de reden waarom de Wiv 2002 alleen niet-kabelgebonden telecommunicatie toestaat.

Ingevolge artikel 10 EVRM bestaat er een 'ontvangstvrijheid' die door de AIVD en de MIVD wordt gebruikt om via het adagium '*de ether is vrij*', Inmarsat- dan wel andere satellietcommunicatie op te vangen en te verwerken. Dit kan door in de naaste omgeving van bijvoorbeeld een Inmarsat basisstation een schotel van de AIVD en/of MIVD te zetten. Alle gegevens komen zo, zonder medewerking of medeweten van de satellietprovider beschikbaar.

Voor het aftappen van kabelgebonden communicatie is een ingreep in de fysieke infrastructuur nodig. Hulp van de netwerkbeheerder is daarbij noodzakelijk, omdat de gegevens niet simpel voor een ieder zijn op te vangen. Het voorstel breidt het adagium '*de ether is vrij*' zonder onderbouwde nut en noodzaak analyse, en zonder een doeltreffend toetsingskader, uit tot '*alle communicatie is vrij*'.

Nederland ICT verzoekt de minister nut en noodzaak nader toe te lichten.

2. Reikwijdte:
Het voorgestelde artikel 31 onder a. geeft een eerste inzicht tot de groep van bedrijven die door deze wet aangesproken kunnen worden: **een aanbieder van een communicatiedienst** wordt gedefinieerd als elke (rechts-)persoon die aan de gebruik van zijn dienst '*de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens opslaat ten behoeve van een zodanige dienst, of de gebruikers van die dienst.*' Het begrip 'communicatiedienst' plaatst niet alleen de huidige openbare elektronische communicatiediensten en –netwerken zoals gedefinieerd in de Telecomwet onder de reikwijdte van het voorstel, maar breidt deze uit tot besloten netwerken en –diensten (oa. Surfnet en interne bedrijfsnetwerken), maar verder vallen ook aanbieders van webhostingdiensten, beheerders van websites en aanbieders van online opslag, email of spraakdiensten onder deze nieuwe definitie. Maar zelfs 'zelfrijdende voertuigen' en ' connected cars' kunnen door het voorstel binnen deze definitie vallen en in dat geval 'in bulk' gevolgd worden. Deze nieuwe toepassingen maken namelijk inherent gebruik van communicatienetwerken en bieden ook communicatiefuncties voor mensen onderling. Niet alleen communicatie tussen mensen en tussen mensen en on-line diensten worden nu bulk aftapbaar, maar ook alles wat in de wereld van '*Internet of Things*' gaat komen. In essentie valt **elke** aanbieder van een dienst die over het internet

gegevens, wat voor gegevens dan ook, uitwisselt onder de reikwijdte van het voorstel. Gegevens thuis, in de auto, in het ziekenhuis, echt alles wat een verbinding met het internet heeft, of is aangesloten op een eigen netwerk.

Het voorgestelde artikel 32 eerste lid geeft een tweede aanduiding van de omvang van de reikwijdte van dit voorstel. De te onderscheppen gegevens zijn '*elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk*'. Alle output van geautomatiseerde werken is blijkbaar potentieel interessant voor de diensten en kan op deze manier ontsloten worden.

Het voorgestelde artikel 33 ten slotte komt in de plaats van de vroegere artikelen 25, 26 en 27, Wiv 2002, waarbij verkennen door middel van ongerichte interceptie van de niet-kabelgebonden telecommunicatie geoorloofd was, mits deze communicatie zijn oorsprong of bestemming in andere landen had. In het onderliggende voorstel is deze laatste beperking, voor AIVD en/of de MIVD, zonder verdere motivatie komen te vervallen.

Nederland ICT verzoekt de minister bovengenoemde keuzes nader te motiveren.

3. Bulk interceptie (digitaal sleepnet):
Het voorgestelde artikel 33 lid 1 van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) legt verplichtingen op over 'bulk interceptie'. Men spreekt van "*elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk*". Het gaat hier om niet gerichte interceptie.

Artikel 4 van het Besluit aftappen openbare telecommunicatienetwerken en -diensten stelt "*Bij ministeriële regeling kunnen nadere regels inzake technische aftapbaarheid worden gesteld met betrekking tot de bij die regeling aan te wijzen openbare telecommunicatienetwerken en openbare telecommunicatiediensten.*"

In de Regeling aftappen openbare telecommunicatienetwerken en -diensten, wordt in art. 8 de aftapbaarheid van internettoegang dan wel diensten beperkt tot :
1°. de accountnaam van de gebruiker dan wel een ander identificerend nummer, dat door de aanbieder ten behoeve van de dienstverlening aan de gebruiker wordt gehanteerd, of
2°. het adres voor elektronische post dat door de aanbieder ten behoeve van de dienstverlening aan de gebruiker wordt gehanteerd.

In het onderliggende voorstel zal, volgens de Memorie van Toelichting, bij een last tot bulk intercept '*nader aangegeven dienen te worden welk deel van de kabelinfrastructuur het betreft en wat voor soort verkeer [er] dient te worden geïntercepteerd*'. De huidige interceptie infrastructuur ziet niet op 'bulk interceptie'. Het is derhalve niet mogelijk om de huidige infrastructuur een-op-een te gebruiken voor deze bulk-interceptie. Om te voldoen aan een last voor bulk interceptie zal een kostbare nieuwe unieke interceptie infrastructuur ontworpen, ontwikkeld, gebouwd en getest moeten worden voor elk specifiek bedrijf. Waarbij er grote kans is dat kosten en werkzaamheden gedupliceerd worden aangezien er een geheimhouding rust op het ontvangen van een last.

Nederland ICT verzoekt de minister meer informatie te geven over de wijze waarop de last tot bulk interceptie technisch dient te worden uitgevoerd door *alle* communicatiedienstaanbieders en welke

kosten hier naar verwachting mee zijn gemoeid. Ook vraagt Nederland ICT de minister deze kosten te vergelijken met soortgelijke nalevingskosten voor bedrijven in andere EU-landen.

4. Deep Packet Inspectie:
Artikel 33 eerste lid geeft tevens de mogelijkheid om netwerkmonitoring of netwerkdetectie activiteiten te ontplooien door middel van *Deep Packet Inspection (DPI)- apparatuur*[4]. Onduidelijk is hoe de netwerkdetectie zich verhoudt tot het Nationaal Detectie Netwerk van de NCSC waar de AIVD en de MIVD ook bij zijn aangesloten. Tevens is onduidelijk of de detectie voor defensieve en/of offensieve doeleinden wordt gebruikt.

Het voorstel maakt tevens niet duidelijk of netwerkmonitoring en -detectie een activiteit is die de diensten als aangeboden dienst van de aanbieder kunnen eisen, of dat deze activiteit door de AIVD en/of de MIVD zelf opgezet en uitgevoerd wordt op data die door middel van bulk intercept aan hen geleverd wordt. De memorie van toelichting spreekt van een combinatie-last. Dit lijkt erop te duiden dat netwerkmonitoring en -detectie door de aanbieder opgezet en uitgevoerd dient te worden.

Nederland ICT vraagt om een verduidelijking op dit onderdeel.

5. Wanneer aftapbaar zijn ?
Uit het voorstel blijkt niet dat men analoog aan Tw 13.1 lid 1, aanbieders van communicatiediensten verplicht hun communicatiediensten uitsluitend beschikbaar te stellen aan gebruikers indien deze aftapbaar zijn. Dit duidt erop dat de medewerkingsplicht, en de daar aan gekoppelde investeringen pas dienen te worden gedaan op het moment dat deze aanbieder met een last geconfronteerd wordt.

Nederland ICT vraagt een verduidelijking op dit onderdeel.

6. Hoe aftapbaar te zijn ?
Het voorstel geeft geen technische details over de manier waarop de integriteit, beschikbaarheid en vertrouwelijkheid van de getapte data gewaarborgd wordt. De ETSI-specificatie Transport of Intercepted IP Traffic (TIIT) v1.2.0 geeft technische details hoe aanbieders van openbare telecommunicatienetwerken en -diensten kunnen voldoen aan 13.1 Tw. Infrastructuuraanbieders dienen gebruik te maken van standaarden om interoperabiliteit te kunnen garanderen, het aftappen kan daardoor ook via een standaard (ETSI/TIIT) gereguleerd worden. Nu de scope wijzigt naar **elke** aanbieder van een communicatiedienst kan geen aansluiting gezocht worden bij een standaard, immers niet elke communicatiedienst ziet op interoperabiliteit, een groot aantal diensten (apps) voorziet in communicatie binnen het eigen ecosysteem. Het is niet duidelijk op welke wijze deze aanbieders moeten en kunnen voldoen aan de Wiv.

Onduidelijk blijft derhalve wat en wanneer men dient te investeren. Vooral voor kleinere innovatieve communicatiediensten aanbieders (start-ups) kan een verplichte investering, net als haar product populair wordt (binnen een doelgroep of land dat een aandachtsgebied van de AIVD en/of de MIVD is, dan wel is opgenomen in het (geheime) aanwijzingsbesluit) funest zijn voor verdere doorontwikkeling. Voor Nederland als start-up land is zo'n dreigende verplichte investering suboptimaal.

[4] idem, p.71

Nederland ICT vraagt de minister om een nadere toelichting.

7. Hoelang aftapbaar?
Het voorstel geeft aan dat een aanbieder nog 12 maanden na de beëindiging van de last zijn infrastructuur aftapbaar moeten houden (art. 37 lid 3 WIV). Dit is disproportioneel, aangezien deze taplasten, door de diensten, gemotiveerd beëindigd dienen te worden. Enige motivering dan wel een kosten/baten afwegingskader ontbreekt volledig.

Nederland ICT vraagt de minister om een nadere motivering.

8. Aansprakelijkheid?
In het voorstel ontbreekt tevens enig aansprakelijkheidsregime ten aanzien van vergoeding van schade door het directe of indirecte handelen of nalaten van de inlichtingen- en veiligheidsdiensten. Het installeren van een interceptievoorziening kan leiden tot een verstoring van de dienstverlening aan klanten. Het nemen van financiële verantwoordelijkheid voor haar eigen handelingen zou een goede afweging over wel of niet ingrijpen moeten ondersteunen.

Een extra moeilijkheid is de geheimhouding die rust op een last tot meewerken. Rechtspraak wijst uit dat op de overheid een zware aansprakelijkheid rust voor haar publiekrechtelijke (rechts)handelingen. Door de geheimhouding is de toegang tot de rechter voor een aanbieder van communicatiediensten in het geding.

Nederland ICT verzoekt om een eenduidige aansprakelijkheidsregeling en een eenduidige regeling waarbij toegang tot de rechter, vooraf, verzekerd is.

9. Toezicht:
Zoals uit het voorgaande blijkt, is Nederland ICT van mening dat bevoegdheden die zo diep ingrijpen op de Nederlandse burger en het bedrijfsleven omgeven moeten zijn met een uitermate stringent system van checks en balances. Alleen artikel 29 voorziet in een systeem van onafhankelijke bindende toetsing. Pas bij een contentieuze procedure, waarbij er analoog aan de Amerikaanse FISA procedure sprake is van een '*Public Advocate*'[5] kan het toetsingssysteem als adequaat worden aangemerkt. Het voorgestelde systeem voor de overige bepalingen voldoet volgens Nederland ICT niet aan minimale maatschappelijke en rechtsstatelijke verantwoording die nodig is om zo'n ingrijpend middel, rechtmatig, te kunnen invoeren.

Nederland ICT vraagt de minister alsnog een adequaat toetsingssysteem in het wetsvoorstel op te nemen.

10. Transparantie:
Naast toezicht is transparantie een belangrijke voorwaarde voor acceptatie van verregaande bevoegdheden. Het WRR rapport "*De publieke kern van het Internet. Naar een buitenlands internetbeleid.*[6]" geeft aan dat '*transparantie op een -noodzakelijkerwijs- hoog niveau zou kunnen helpen om nut en noodzaak van bepaalde programma's van de diensten op nationaal niveau te beoordelen [..]*'[7]. Nederland ICT sluit zich graag aan bij deze conclusie. Transparantie zoals in België

[5] http://illinoislawreview.org/wp-content/ilr-content/articles/2015/3/Poorbaugh.pdf , p.1391
[6] http://www.wrr.nl/publicaties/publicatie/article/de-publieke-kern-van-het-internet-1/
[7] WRR. De publieke kern van het Internet. Naar een buitenlands internetbeleid, p.108

door de BIM commissie[8] of de G-10-Kommission[9] in Duitsland maakt dat nut en noodzaak duidelijk gemaakt kunnen worden en er draagvlak ontstaat. Iets dat nu ontbreekt voor het huidige voorstel.

Nederland ICT vraagt de minister nader uit te werken hoe meer transparantie kan worden geboden over nut en noodzaak van bulkinterceptie en de wijze waarop communicatiedienstaanbieders hierover kunnen communiceren met hun klanten.

11. Technologie onafhankelijk:
Een van de genoemde doelstellingen is om de wet technologie onafhankelijk te maken. Er geldt echter ingevolge artikel 29 van het voorstel een specifieke regeling voor analoge communicatie (briefgeheim) die niet geldt voor elektronische communicatie. In gevolge het briefgeheim dient de rechtbank Den Haag, op verzoek van het hoofd van de dienst, een last af te geven. Nederland ICT is van mening dat deze toetsing vooraf ook voor de interceptie van alle overige communicatie dient te worden toegepast, zeker gezien de diverse voorstellen om elektronische communicatie onder artikel 13 van de Grondwet te brengen.

Door onderscheid te maken tussen 'papier' en 'digitaal' sluit het voorstel ook niet aan bij de Archiefwet.

Uit het voorstel blijkt ook niet hoe er met Voice over IP (VoIP) data uit de sleepnet taps dient te worden omgegaan. Niet duidelijk wordt of dergelijke data onder het grondwettelijke telefoongeheim vallen. Ingevolge artikel 13 Gw, lid 2 bestaat er een telefoongeheim. Klaarblijkelijk wordt dat geheim, zonder verdere motivering, in dit voorstel afgeschaft.

Nederland ICT vraagt de minister om een nadere motivering.

12. Encryptie:
Het hiervoor genoemde WRR rapport geeft ook aan[10] dat encryptie van het dataverkeer, zowel van data in transit als van opgeslagen data, grootschalige onderschepping van data door inlichtingen- en veiligheidsdiensten zowel veel moeilijker als veel duurder maakt. Nu biedt het voorstel de mogelijkheid om een aanbieder te dwingen de communicatie te ontsleutelen, echter dat zal niet in alle gevallen zomaar kunnen.

Ter illustratie, Perfect Forward Secrecy[11] bewaart geen encryptiesleutels. Het is daardoor voor de aanbieder niet mogelijk om deze communicatiestroom ontsleuteld uit te leveren aan de diensten. In het voorstel is het onduidelijk of de zogenaamde ontsleutelbevel ook het inbouwen of (gedeeltelijk) uitschakelen van essentiële encryptiemethoden verplicht maakt voor leveranciers. Het inbouwen van zogenaamde '*backdoors*' waar alleen diensten toegang tot hebben is een illusie. Bruce Schneier, een bekende internetveiligheidsexpert stelt: "*You can't build a backdoor that only the good guys can walk through*"[12]. De onthullingen gedaan door Snowden laten zien op welke wijze inlichtingen- en veiligheidsdiensten proberen de omgeving naar hun hand te zetten. Zo werd doelbewust een encryptiealgoritme verzwakt[13].

[8] http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2013.pdf
[9] http://dip21.bundestag.de/dip21/btd/17/127/1712773.pdf
[10] idem, p.90
[11] https://nl.wikipedia.org/wiki/Perfect_forward_secrecy
[12] https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html
[13] https://www.lawfareblog.com/nsas-subversion-nists-algorithm

De onthullingen van Snowden hebben een enorme economische impact op Amerikaanse technologiebedrijven. Dit heeft ertoe geleid dat Obama het beleid heeft gewijzigd: '*the mass collection of phone data will be sharply curtailed*'[14]. Gezien de algehele weerstand tegen deze mogelijke bevoegdheden wereldwijd en zeker in de V.S. zou introductie van deze bevoegdheid in Nederland funest zijn voor Nederland als ICT standplaats. In dit licht is het vreemd dat Nederland nu juist de mogelijkheden voor massasurveillance, zonder verdere inhoudelijke motivatie introduceert. De economische gevolgen zullen niet anders zijn dan in Amerika[15].

Saillant is de conclusie "*The biggest difference between initial worst-case projections in 2013 of revenue loss of $180 billion and the current $47 billion projection is that customers took encryption into their own hands, said Forrester.*" De opbrengsten van bulk interceptie kunnen derhalve door het en masse gebruik van encryptie door eindgebruikers naar verwachting niet opwegen tegen de kosten. Door de encryptie bij gebruikers te laten, kan een dienstenaanbieder niet voldoen aan de ontsleutelplicht. Het is immers alleen de klant die de encryptiesleutel heeft.

Nederland ICT vraagt de minister in te gaan op de gevolgen van toenemende encryptie door de eindgebruiker voor dit wetsvoorstel, en nader te onderbouwen wat het effect van het wetsvoorstel zal zijn op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

13. Proportionaliteitstoets:
Het voorstel geeft in de artikelen 43 en 44 een afwegingskader voor noodzakelijkheid, proportionaliteit en subsidiariteit met betrekking tot het uitoefenen van de bevoegdheden. Zo'n afwegingskader is een papieren werkelijkheid. Om het afwegingskader handen en voeten te geven pleit Nederland ICT ervoor om het kader in te bedden in een budgettair model. Dit zorgt er voor dat, door de simpele beperking van een vooraf vastgesteld of flexibel budget voor de kosten van interceptie, financiële overwegingen voor de diensten de proportionaliteitstoets mede inkleuren. Het dwingt de diensten ertoe om hun activiteiten veel scherper en doelgerichter op- en in te zetten.

Dit geeft de diensten een betere *Return-on-Investment* bij haar onderzoeken. Tevens zorgt het voor een democratische controle op de kosten van interceptie omdat het benodigde budget via de Rijksbegroting inzichtelijk is. Naast deze efficiëntere afhandeling en effectieve proportionaliteits-toetsing dient er zich nog een belangrijk economisch voordeel aan. Bedrijven kunnen blijven investeren in innovatie, en daarmee de groei van de BV Nederland faciliteren.

Nederland ICT vraagt de minister aan te geven wat de te verwachten kosten voor de verschillende communicatiedienstaanbieders zijn en waarom er voor is gekozen deze kosten bij de private partijen neer te leggen.

14. Vergoeding kosten:
Uit artikel 13.2 van de Telecomwet (Tw) volgt dat aanbieders van openbare telecommunicatienetwerken en –diensten, verplicht zijn hun netwerk aftapbaar te maken. Deze aftapbaarheid kan worden gebruikt door zowel de opsporings- alsmede de inlichtingen- en

[14] http://blogs.wsj.com/cio/2014/01/17/obama-addresses-economic-damage-caused-by-snowden-nsa-leaks/
[15] http://www.zdnet.com/article/snowden-prism-fallout-will-cost-u-s-tech-vendors-47-billion-less-than-expected/

veiligheidsdiensten. De aftapbaarheid ziet toe op een geïndividualiseerd subject. Er is daarom sprake van gerichte interceptie. De 'geïndividualiseerde' aftapbaarheid van de huidige infrastructuur is geregeld bij Besluit aftappen openbare Telecommunicatienetwerken en -diensten. De capex[16] kosten komen voor rekening van de bedrijven (Tw 13.6 lid 1). Alleen de directe opex[17] kosten voor het uitvoeren van een taplast komen voor vergoeding in aanmerking (Tw 13.6 lid 2). Artikel 32, lid 8 van het voorstel verklaart deze regeling van overeenkomstige toepassing. De Memorie van Toelichting zegt: "*Er bestaat geen aanleiding om voor deze aanbieders een (deels) afwijkende regeling te treffen*"[18].

De Telecomwet maakt onderscheid tussen communicatiediensten en -netwerken en openbare communicatiediensten en -netwerken. Het onderliggende voorstel maakt dat onderscheid niet. Alleen de openbare communicatienetwerken en -diensten vallen onder de werking van artikel 13.2 Tw. Voor de overige, niet openbare communicatienetwerken en -diensten gelden slechts de verplichtingen om mee te werken uit het Wetboek van Strafvordering en niet die uit de Telecomwet. Er bestaat voor deze groep geen verplichting om haar netwerk of dienst a priori aftapbaar te maken, tevens geeft de systematiek van strafvordering de mogelijkheid om redelijke kosten bij het Openbaar Ministerie te claimen.

De kosten van het nakomen van een vordering tot het verstrekken van gegevens, tot het medewerking verlenen aan het ontsleutelen of het bewaren en beschikbaar houden van gegevens komen op grond van het Wetboek van Strafvordering wel voor vergoeding in aanmerking.

Een zeer beperkte groep van (openbare) communicatiediensten aanbieders valt onder de Telecomwet de overige aanbieders van communicatiediensten zou onder art. 592 Wetboek van Strafvordering wel in aanmerking komen voor vergoeding van kosten. Dat onder het voorstel deze grotere groep van aanbieders hun recht op vergoeding zal worden afgenomen wordt in het geheel niet onderbouwd.

Nederland ICT vraagt de minister deze onderbouwing alsnog te leveren.

15. Capaciteit:

In het voorgaande hebben we bekeken wat de hernieuwde Wiv inhoudt voor aanbieders van communicatiediensten. Alle getapte communicatie zal door de AIVD en/of de MIVD verwerkt moeten worden.

Ongeveer 90% van alle communicatie verloopt via kabelnetwerken, terwijl de hoeveelheid gegevens elke twee tot drie jaar verdubbelt. De hoeveelheid data die de AIVD en/of de MIVD in het nieuwe voorstel moeten verwerken zal dan ook naar verwachting meer dan vertienvoudigen. Mocht het voorstel medio 2017 inwerking treden dan zou dat zelfs een vertwintigvoudiging kunnen zijn. Het is onduidelijk op welke wijze de AIVD met de huidige en voor 2017 geprognosticeerde personele capaciteit deze nieuwe stroom aan gegevens inhoudelijk op een zinvolle wijze kan analyseren. In het licht van het voorstel en de te verwachten explosie van te verwerken gegevens zal de personele capaciteit sterk dienen te worden uitgebreid met de daartoe benodigde specialistische kennis. Over

[16] https://en.wikipedia.org/wiki/Capital_expenditure
[17] https://en.wikipedia.org/wiki/Operating_expense
[18] idem, p.61

de daartoe beschikbare middelen wordt in het wetsvoorstel niet gesproken, ook wordt niet aangegeven op welke termijn de diensten denken de benodigde aanvullende specialistische kennis operationeel in te kunnen zetten. De komende Rijksbegroting zal wellicht meer inzicht geven.

Een ander scenario is dat de AIVD en/of MIVD niet geïnteresseerd zijn in het verwerken van de communicatie, maar dat ze de ruwe data als handelswaar zien. Artikel 77 lid 2 van het voorstel maakt deze zgn. bulkdata uitwisselbaar. Daarvoor is slechts eenmalig ministeriële toestemming nodig.

Onder ruwe data, ofwel ongeëvalueerde gegevens, valt bijvoorbeeld een kopie van een complete website en de in het kader van artikel 33 ontvangen en opgenomen gegevens waarop nog geen selectie is toegepast als bedoeld in artikel 35, eerste lid, van het wetsvoorstel. Overigens wordt opgemerkt dat de toestemming ook betrekking kan hebben op meerdere opeenvolgende verstrekkingen van vergelijkbare aard, zonder dat dit per geval dient te worden verleend.

Nederland ICT vraagt de minister nader toe te lichten hoe men de bulkdata, ook bij de verwachte toename, op een zinvolle manier denkt te kunnen verwerken.

Resumerend

Onder het mom van '*technologie onafhankelijk maken van de interceptie*' wordt volgens Nederland ICT onvoldoende gemotiveerd fundamentele wijzigingen aangebracht in de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze fundamentele wijzigingen worden niet gecompenseerd door enige vorm van onafhankelijk toezicht vooraf.

Nederland ICT heeft grote twijfels over het nut en noodzaak, de transparantie en proportionaliteit, de reikwijdte en toerekening van kosten, de praktische uitvoerbaarheid en het juridisch toetsingskader van de nieuwe bevoegdheden en daarmee het draagvlak voor een dergelijk ingrijpend wetsvoorstel.

Door de kosten geheel op de aanbieder af te wentelen, creëert de overheid geen geïnternaliseerd *incentive* bij de inlichtingen- en veiligheidsdiensten om *overreach* tegen te gaan.

"*In prior generations, the cost of surveillance and data acquisition constituted a useful buffer between state surveillance and privacy; resource constraints forced law enforcement to focus on a limited number of targets on a scale where judicial oversight was a practical – if imperfect- deterrent against overreach*"[19].

De door de wet opgelegde eisen aan een groot aantal bedrijven zal resulteren in een verlies aan vertrouwen van burgers en bedrijven, in toegenomen onzekerheid en financiële druk voor het bedrijfsleven, minder innovatie, risico's voor de betrouwbaarheid en integriteit van dienstverlening en verslechtering van het internationale imago van Nederlandse als Digital Gateway to Europe.

Nederland ICT pleit er voor om bij het opleggen van dergelijke verplichtingen voor het bedrijfsleven altijd de kosten via de Rijksbegroting te laten lopen. Niet alleen is er zodoende democratisch toezicht

[19] Governments as Actors, Faris and Gasser, Internetmonitor 2013, Reflections on the digital world, p.21 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2366840)

op de kosten, ook worden de diensten er door financiële overwegingen toe gedwongen hun activiteiten scherp en doelgericht in te zetten. De proportionaliteit is hierdoor beter geborgd.

Meer specifiek vraagt Nederland ICT de minister, in overleg met zijn collega's van Veiligheid en Justitie en Economische Zaken, om:

- Een gedegen onderbouwing van nut en noodzaak van een dergelijk ingrijpend wetsvoorstel.
- Een voorstel hoe in de toekomst op een transparante wijze inzicht gegeven wordt in de reikwijdte van de bevoegdheden van inlichtingen- en veiligheidsdiensten en de wijze waarop deze hun taak uitoefenen. Dit teneinde het vertrouwen van burgers en bedrijven in de integriteit van hun data, het internet en daarmee de digitale economie als geheel te waarborgen.
- Een analyse van het effect dat het wetsvoorstel zal hebben op de positie van Nederland als vestigingsplaats voor het (ICT)-bedrijfsleven als Digital Gateway to Europe.

Postbus 401
3440 AK Woerden
Pompmolenlaan 7
3447 GK Woerden

T 0348 49 36 36
F 0348 48 22 88
info@nederlandict.nl
www.nederlandict.nl

ING Bank
IBAN: NL 53 ING B 0662 590546
KvK 30174840

Weesperstraat 3
1018 DN Amsterdam
Nederland
Telefoon +31(0)208000400
Fax +31(0)207173648
info@freepressunlimited.org
www.freepressunlimited.org

Datum: 21 augustus 2015

Van: Leon Willems
Free Press Unlimited

Aan: De Minister-President, Minister van Algemene Zaken, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Defensie, de Minister van Veiligheid en Justitie

Excellenties,

Free Press Unlimited zet zich wereldwijd in voor de vrijheid van meningsuiting en de persvrijheid, fundamentele democratische rechten die sinds jaren niet meer zo sterk onder druk hebben gestaan. Ook in landen waar het slecht met de persvrijheid is gesteld, werken wij aan de creatie van een zogenaamde *enabling environment* voor de media: een omgeving waarin media veilig en ongehinderd hun werk kunnen doen, zodat burgers goed geïnformeerd blijven en op basis daarvan beslissingen kunnen nemen. 'People deserve to know' is dan ook het motto van onze organisatie.

Uitgerekend de Nederlandse overheid, waarmee wij zo nauw samenwerken om deze doelstelling te verwezenlijken, komt nu met een wetsvoorstel dat zo'n vrije omgeving voor de journalistiek in eigen land drastisch beperkt. Uw Wet op de inlichtingen- en veiligheidsdiensten 2015, die hier ter consultatie wordt aangeboden, schendt elementaire rechten en vrijheden met betrekking tot het privéleven van personen, de vrijheid van meningsuiting en de persvrijheid, vrijheden die onder andere zijn gegarandeerd in de Grondwet (artikels 7, 10 en 13), de Europees Verdrag voor de Rechten van de Mens (EVRM artikels 8 en 10), het Internationaal Vedrag inzake Burgerrechten en Politieke Rechten (IVBPR artikels 17 en 19) en jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM).

Uit de Universele Verklaring van de Rechten van de Mens van de Verenigde Naties willen we de artikel 12 naar voren halen:

> *Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet.*

Praktijken waarbij geheime diensten telefoonverkeer, e-mail, websites en andere communicatiemiddelen van onverdachte burgers mogen verzamelen, analyseren en bewaren, en die bekend staan onder de term 'massa surveillance', staan op zeer gespannen voet met genoemde verklaringen en verdragen. Datzelfde geldt voor hackersactiviteiten waarbij geheime diensten voor informatie over een 'target' ongevraagd systemen binnendringen (en beschadigen) van nietsvermoedende derden

Weesperstraat 3
1018 DN Amsterdam
Nederland
Telefoon +31(0)208000400
Fax +31(0)207173648
info@freepressunlimited.org
www.freepressunlimited.org

die nergens van worden verdacht. Toch staat de concept-WIV deze omstreden praktijken in ruime mate toe. Daar moet, zo veronderstellen wij, een zeer bijzondere reden voor zijn. Maar nergens, ook niet in hoofdstuk 9 van de Memorie van Toelichting over de grondrechtelijke en mensenrechtelijke aspecten van het wetsvoorstel, legt de wetgever uit welke buitengewoon zwaarwegende kwestie(s) het opzij schuiven van enkele van onze meest basale grondrechten rechtvaardigen.

Free Press Unlimited is niet tegen modernisering van de wetgeving op het gebied van de inlichtingen en veiligheidsdiensten. We erkennen de noodzaak om doelgericht en efficiënt onderzoek te kunnen doen naar personen of organisaties waarvan een ernstig vermoeden bestaat dat zij een gevaar vormen voor de samenleving. Dit wetsvoorstel schiet zijn doel echter ver voorbij en behandelt iedere burger als verdachte.

In deze consultatie richten wij ons op de wetsartikelen die de doelstellingen en idealen van Free Press Unlimited raken en die van invloed zijn op het functioneren van de media, op de journalistieke bronbescherming en op de vrijheid van meningsuiting in Nederland. Wij willen wijzen op het verstrekkende chilling effect (het verschijnsel waarbij journalisten en bronnen zich niet meer durven uit te spreken en burgers bepaalde nieuwsbronnen mijden uit vrees voor repercussies) dat uitgaat van dit wetsvoorstel, mocht deze in de huidige vorm worden aangenomen.

Vanuit deze overweging komt Free Press Unlimited tot de volgende drie bezwaren:

1. De wetgever dekt zich in tegen beschuldigingen van schending van de journalistieke bronbescherming door een extra waarborg te stellen: "*De uitoefening van een bevoegdheid als bedoeld in paragraaf 3.2.2 jegens een journalist, waarbij de uitoefening is gericht op het achterhalen van de bron van de journalist, is slechts toegestaan, indien de rechtbank Den Haag daartoe, op verzoek van Onze betrokken Minister, toestemming heeft verleend.*" (paragraaf 3.2.2, bijzondere bevoegdheden van de diensten, artikel 24, vierde lid). Meer hierover valt te lezen op pagina's 35 en 185 van de toelichting. Het klinkt alsof de journalistiek bronbescherming goed is gewaarborgd. Maar hoe denkt de wetgever deze te kunnen garanderen als de diensten tegelijkertijd brede bevoegdheden genieten tot het aftappen, ontvangen, opnemen en afluisteren van elke vorm van communicatie zoals bedoeld in artikel 33? Welke garantie kan de wetgever bieden dat als gevolg van de bevoegdheden in artikel 33 niet onverhoopt de communicatie tussen een journalist en diens bron wordt onderschept en de identiteit van de journalistieke bron aan het licht komt? Wij vinden in de tekst geen antwoord op die vragen en willen daarom dat artikel 33 en alle andere daartoe relevante artikelen geschrapt worden.

Weesperstraat 3
1018 DN Amsterdam
Nederland
Telefoon +31(0)208000400
Fax +31(0)207173648
info@freepressunlimited.org
www.freepressunlimited.org

FREE PRESS UNLIMITED

2. De diensten mogen mensen van wie wordt vermoed dat ze kennis dragen van de wijze van versleuteling van gegevens *verplichten* medewerking te verlenen tot het ontsleutelen van deze gegevens (artikel 30, vijfde en achtste lid). Vervolgens wordt zo'n zelfde bevoegdheid verleend als het gaat om onderzoek van communicatie (artikel 32, gericht op specifieke personen en organisaties, en artikel 33, 'massa surveillance'). Deze medewerkingsplicht krijgt nader invulling in paragraaf 3.2.2.7.6, medewerkingsplicht bij ontsleuteling communicatie, artikel 41. Heeft de wetgever nagedacht over de gevolgen van bovengenoemde bepalingen voor geautomatiseerde systemen die juist functioneren dankzij het vertrouwen van de gebruiker in de veiligheid en integriteit van het systeem, bijvoorbeeld door het gebruik van cryptografische sleutels? Free Press Unlimited denkt hierbij bijvoorbeeld aan het Nederlandse klokkenluidersplatform Publeaks. Dit platform heeft een belangrijke maatschappelijke functie die zeer onder druk komt te staan als het wetsvoorstel in de huidige vorm wordt aangenomen. Wij lezen nergens hoe de wetgever schade aan dergelijke systemen denkt te voorkomen. Wij vinden dat beveiligde systemen die in dienst staan van (pers)vrijheid en democratie niet gedwongen mogen worden hun beveiliging prijs te geven en willen daarom dat alle daartoe relevante artikelen geschrapt worden.

3. Uit het wetsvoorstel en hoofdstuk 9 van de toelichting maken wij op dat de wetgever niet heeft nagedacht over het 'chilling effect' op de persvrijheid en de vrijheid van meningsuiting. Dit zijn grondrechten die worden gewaarborgd in artikel 7 van de Grondwet, artikel 10 van het EVRM, en artikel 19 van het IVBPR. Het chilling effect ten gevolge van brede bevoegdheden tot surveillance, en de gevolgen daarvan voor het recht op vrijheid van meningsuiting en persvrijheid, zijn door de Verenigde Naties erkend, zie rapport A/HRC/23/40 (Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression). Dit geldt niet alleen voor de communicatie tussen burgers maar ook voor de nieuwsconsumptie: door de voorgestelde massa surveillance weet de overheid exact welke nieuwsbronnen door welke burgers worden geraadpleegd, van volkskrant.nl tot wikileaks.org. We vragen ons af hoe de wetgever het chilling effect van het wetsvoorstel denkt te beperken en denkt te rijmen met de principes van noodzakelijkheid, proportionaliteit en subsidiariteit en met de democratische normen en waarden. Wij vinden dat er eerst een brede maatschappelijke discussie dient plaats te vinden over deze en andere gevolgen die de conceptwet kan hebben alvorens er ook maar iets aan het parlement wordt voorgelegd.

Weesperstraat 3
1018 DN Amsterdam
Nederland

Telefoon +31(0)208000400
Fax +31(0)207173648
info@freepressunlimited.org
www.freepressunlimited.org

Free Press Unlimited is bovendien van mening dat er verdere punten van aandacht zijn die wellicht niet direct volgen uit de journalistieke focus van onze organisatie, maar die naar onze stellige overtuiging een grote inbreuk maken op kernwaarden van de Nederlandse samenleving. Daarom onderschrijft Free Press Unlimited nadrukkelijk de reacties op het huidige wetsvoorstel van gelijkgezinde organisaties uit het maatschappelijk middenveld, waaronder die van Bits of Freedom, ISOC/AMS-IX, Boekx Advocaten en Greenhost.

Free Press Unlimited verzoekt u dringend om onze aanbevelingen en de aanbevelingen van bovengenoemde organisaties mee te nemen bij de verdere parlementaire behandeling van de wetsvoorstellen. Free Press Unlimited is graag bereid nader met u van gedachten te wisselen over deze aanbevelingen.

Hoogachtend,

Leon Willems
Directeur Beleid en Programma's
Free Press Unlimited

Nederlands Juristen Comité voor de Mensenrechten
Dutch Section of the International Commission of Jurists

T.a.v. de Minister van Binnenlandse Zaken en Koninkrijksrelaties
Dr. R.H.A. Plasterk
Postbus 20011
2500 EA Den Haag

Leiden, 31 augustus 2015

Excellentie,

Het Nederlands Juristen Comité voor de Mensenrechten (hierna: het NJCM) maakt graag gebruik van de gelegenheid om inhoudelijk te reageren op het concept-wetsvoorstel dat strekt ter vervanging van de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).

Met name op het gebied van de bijzondere bevoegdheden van de diensten bevat dit concept-wetsvoorstel een aantal grote wijzigingen ten opzichte van de huidige wet. De meest ingrijpende herziening heeft betrekking op interceptie van telecommunicatie en het opvragen van telecommunicatiegegevens. Het NJCM realiseert zich dat de technologie in hoog tempo voortschrijdt en de diensten adequate toegang tot telecommunicatie noodzakelijk achten. Ook begrijpt het NJCM dat de wetgever ervoor kiest om het technische onderscheid op te heffen en thans gebruik te maken van technologieonafhankelijke formuleringen. Tegelijkertijd dienen de fundamentele rechten gewaarborgd te zijn en daarover maakt het NJCM zich zorgen. Het NJCM brengt hieronder haar belangrijkste inhoudelijke bezwaren op het wetsvoorstel naar voren.

Noodzaak, proportionaliteit en effectiviteit

Zoals u weet dienen zwaarwegende redenen van algemeen belang te bestaan om een inbreuk te rechtvaardigen op grondrechten zoals de bescherming van de persoonlijke levenssfeer (artikel 8 Gw), het briefgeheim (artikel 13 Gw) en op het recht op eerbiediging van privéleven zoals neergelegd in artikel 8 EVRM. De inbreuk dient noodzakelijk te zijn en moet voldoen aan de eisen van proportionaliteit. Dit betekent dat met de inbreuk een gerechtvaardigd doel wordt nagestreefd en dat dit doel met de maatregel daadwerkelijk kan worden bereikt. Dat de maatregel effectief bijdraagt aan de verwezenlijking van het doel is mede bepalend en de maatregel dient evenredig te zijn aan het doel.

Noodzaak

Het NJCM is van mening dat onvoldoende is gemotiveerd wat de noodzaak is van voorgestelde uitbreiding van de interceptiebevoegdheid van de diensten. Het voorstel strekt ertoe de diensten de mogelijkheid te bieden bulk te intercepteren in het kabelgebonden domein. Dit vindt plaats door met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van elke vorm van telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk met betrekking tot niet specifieke personen, organisaties en nummers: het zogenaamde sleepneteffect. Het gevolg hiervan is dat deze bevoegdheid ook kan worden toegepast op communicatie van onschuldige burgers. De enkele keuze van de wetgever om deze laatste bepaling technologieonafhankelijk te formuleren heeft grote gevolgen voor de betrokkenen. Het toepassen van een dergelijke bevoegdheid betekent namelijk de mogelijkheid tot massa-interceptie waarmee op de privacy van grote groepen onschuldige burgers in Nederland een inbreuk zal worden gemaakt.

De memorie stelt dat met de uitbreiding van de interceptiebevoegdheid uitvoering wordt gegeven aan het door het kabinet ingenomen standpunt dat de techniekafhankelijke interceptiebepalingen van de Wiv 2002 op basis van het onderscheid tussen de ether en de kabel niet meer te rijmen valt met de voortschrijdende technologische ontwikkelingen op het gebied van dataverkeer en communicatie.

Het NJCM merkt op dat in de toelichting echter gegevens ontbreken die inzicht geven in de aard, omvang en ernst van het probleem. Weliswaar wordt erop gewezen dat negentig procent van alle telecommunicatie via kabelnetwerken verloopt en dat de diensten dit als een probleem ervaren. In de toelichting komt echter niet duidelijk naar voren waarom deze bevoegdheid noodzakelijk is, waarom de bestaande bevoegdheden niet in voldoende mate volstaan en welke (ernstige) problemen de voorgestelde bevoegdheid precies gaat oplossen. Door het ontbreken van deze informatie is de noodzaak van het voorstel vooralsnog niet aangetoond – omdat niet beoordeeld kan worden in hoeverre de voorgestelde ingrijpende maatregel het doel van het voorstel rechtvaardigt. In dit kader wijst het NJCM nog op het oordeel van het Europees Hof van Justitie (hierna: Hof). Op 8 april 2014 heeft het Hof in de zaken C-293/12 en C-594/12 beslist dat Richtlijn 2006/24/EG (Dataretentierichtlijn) in zijn geheel ongeldig is wegens strijd met de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie. Het Hof oordeelde over de noodzaak van de Richtlijn dat ondanks de omstandigheid dat zij geschikt was voor het bereiken van het gestelde doel:

'the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary'.

Ditzelfde lijkt het geval te zijn bij het onderhavige wetsvoorstel, waarin de noodzaak van het verzamelen van grote hoeveelheden communicatie van onschuldige burgers ontbreekt. Ook andere internationale instanties trekken de noodzaak van dergelijke grootschalige gegevensverzamelingen in twijfel.[1] Het

[1] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Programme Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23*

NJCM meent dat op dit punt in de memorie een nadere toelichting moet worden gegeven.

Proportionaliteit

Het NJCM heeft grote twijfels of de voorgestelde zogenoemde 'doelgerichtere interceptie' wel proportioneel is. Het proportionaliteitsbeginsel brengt immers mee dat de inbreuken op de belangen van de betrokkenen niet onevenredig mogen zijn in verhouding tot het met de verwerking te dienen doel. Er dient dus een belangenafweging plaats te vinden ter beoordeling of de betreffende inmenging in de persoonlijke levenssfeer voldoet aan dit beginsel. Het NJCM is van mening dat in de memorie van toelichting onvoldoende is toegelicht waarom het bestaande wettelijke instrumentarium niet toereikend is. Onder de huidige wet hebben de diensten in dit kader de volgende bevoegdheden:

- De diensten zijn bevoegd tot het gericht aftappen, ontvangen, opnemen en afluisteren van communicatie (artikel 25);

- De diensten zijn bevoegd tot het ontvangen en opnemen van niet-kabelgebonden telecommunicatie (artikel 26);

- De diensten zijn bevoegd tot het met een technisch hulpmiddel ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie (artikel 27).

De memorie onderbouwt onvoldoende waarom de huidige wetgeving niet toereikend zou zijn. De diensten zijn al bevoegd om gericht kabelgebonden communicatie te onderscheppen. De noodzaak om de communicatie van eenieder (lees: onschuldige burgers) te onderscheppen, lijkt hiermee overbodig en niet proportioneel. In het voorstel wordt de nieuwe bevoegdheid 'doelgerichte verwerving van telecommunicatie' genoemd. Daarbij hoeft in de eerste fase geen sprake te zijn van concrete personen die een gevaar vormen voor de nationale veiligheid en onder de aandacht van de diensten vallen. In dit verband kan het doel voor het onderscheppen van communicatie van personen die hier geen aanleiding toe geven zeer ruim geformuleerd worden. Het NJCM meent dat zolang een concrete omschrijving van het doel en onderzoekssubject ontbreekt, een juiste belangenafweging niet kan worden gemaakt. Bij het ontbreken daarvan kan van proportionaliteit niet worden gesproken. Dit alles klemt te meer nu het huidige toezichtstelsel onvoldoende waarborgen biedt, waarover hieronder meer. Hiermee is echter niet gezegd dat de proportionaliteitsvraag aan de hand van de bestaande waarborgen dient te worden beantwoord.

Wat betreft de toestemming verleend op grond van artikel 24 merkt het NJCM nog het volgende op. Ex

---

January 2014, https://www.pclob.gov/library.html, p. 11., US National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, January 2015, http://www.nap.edu/catalog.php?record_id=19414, Conclusion 1, SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act, FP7-SEC-2011-284725, published on 29 May 2014m UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, report 23 September 2014, A/69/397, par. 51, 52.

artikel 24 lid 3 wordt de toestemming voor het uitoefenen van een bijzondere bevoegdheid door een dienst verleend voor een periode van maximaal drie maanden. Deze kan echter telkens voor drie maanden verlengd worden. Er wordt dus geen grens gesteld aan het aantal keren dat het verlengd kan worden. Dit geldt ook voor 'massasurveillance' op de kabel. Het NJCM is niet overtuigd van de proportionaliteit van een dergelijke eindeloze tapbevoegdheid. Het NJCM meent dat de uitoefening van deze bijzondere bevoegdheid voor betrokkenen een onevenredig nadeel kan opleveren in vergelijking met het daarmee na te streven doel. Het NJCM adviseert in de toelichting op het bovenstaande in te gaan.

Effectiviteit

Naast het gebrek aan noodzaak en proportionaliteit heeft het NJCM ook twijfels bij de effectiviteit van de uitbreiding van de interceptiebevoegdheden van de diensten. Het NJCM erkent dat er behoefte is aan een effectieve surveillance van verdachte terroristen en andere georganiseerde criminaliteit. Internationaal is niet aangetoond dat niet gerichte interceptiebevoegdheden effectief zijn. Uitgaande van onafhankelijke beoordelingen in de Verenigde Staten heeft massasurveillance echter niet bijgedragen aan de preventie van terroristische aanvallen in het belang van de nationale veiligheid.[2] Bovendien vraagt het NJCM zich af in hoeverre er doelgericht kan worden gezocht wanneer de hoeveelheid informatie en persoonsgegevens die worden verzameld steeds groter wordt. Het is de bedoeling van de wetgever om de veiligheid meer te waarborgen door alle soorten communicatie te kunnen verzamelen, maar die schaalvergroting lijkt het proces moeizamer te maken. Het NJCM betwijfelt of de voorgestelde bevoegdheid wel effectief is en ziet hierover graag een onderbouwing tegemoet.

Waarborgen

De wetgever heeft de positie en het toezicht op de toestemmingsverlening van de CTIVD in het concept-wetsvoorstel op onderdelen versterkt. Hoewel het NJCM toejuicht dat het toezicht op de toestemmingsverlening is versterkt door de wetgever, plaatsen wij enkele kanttekeningen bij het voorgestelde toezichtstelsel.

Rechterlijke toestemming vooraf

Inbreuk op het communicatiegeheim is een indringende bevoegdheid en verdient indringende bescherming. Dat brengt mee dat de waarborgen sterk moeten zijn. Het EHRM heeft de wenselijkheid onderschreven van een onafhankelijk orgaan met de bevoegdheid om de toepassing van bijzondere bevoegdheden tegen te gaan of te beëindigen.[3] Ook de commissie Dessens constateert dat

[2] https://www.newamerica.org/downloads/IS_NSA_surveillance.pdf
[3] EHRM 22 november 2012, appl.no. 39315/06 (Telegraaf Media Nederland/Nederland), r.o. 98.

'in de landen om ons heen de afgelopen decennia een ontwikkeling valt waar te nemen in de richting van meer extern toezicht vooraf op de inzet van inlichtingenmiddelen die een inbreuk maken op grondrechten. Deze ontwikkeling komt ook tot uitdrukking in een aanbeveling van de Parlementaire Assemblee van de Raad van Europa uit 1999 waarin een voorkeur wordt uitgesproken voor rechterlijk toezicht vooraf op elke inbreuk op grondrechten door I&V-diensten. Ook in de wetenschappelijke literatuur over toezicht op inlichtingen- en veiligheidsdiensten valt een zekere voorkeur te bespeuren voor preventief rechterlijk toezicht.'[4]

Het NJCM vindt, ingegeven door internationale en nationale uitspraken, dat toestemming van de minister niet voldoende is.[5] Rechterlijke toestemming vooraf is de sterkste waarborg. Het NJCM vindt dit ook voor inlichtingen- en veiligheidsdiensten de aangewezen bescherming.

Bindend toezicht

De Commissie Dessens heeft voorgesteld aan toezicht door de CTIVD achteraf bindende kracht te verlenen. Het kabinet heeft dit advies in het concept-wetsvoorstel niet overgenomen. Dit betekent dat de minister na heroverweging alsnog kan besluiten een bevoegdheid te blijven toepassen. Alhoewel de minister vervolgens ter verantwoording geroepen kan worden door de Tweede Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten (de CIVD, ook wel de 'commissie Stiekem' genoemd), wordt deze rol van het parlement bij het toezicht in het concept-wetsvoorstel niet nader ingevuld.

Hoewel rechterlijke toestemming vooraf haar voorkeur heeft, ziet het NJCM in bindend toezicht achteraf door de CTIVD een mogelijk alternatief. Bindendheid is immers een belangrijk criterium voor effectieve onafhankelijke controle. De ministeriële verantwoordelijkheid blijft zo wel degelijk intact. Het NJCM vindt de redenering van het kabinet om dit voorstel niet te volgen dan ook niet overtuigend.

Bewaartermijnen

Een andere belangrijke waarborg is die van bewaartermijnen. Het grootschalig verzamelen van communicatie moet gepaard gaan met zo snel mogelijk verwijderen van communicatie die niet direct relevant is. Het voorstel van het kabinet maakt het echter mogelijk dat de verzamelde communicatie lang bewaard blijft, zodat hier ook (bijvoorbeeld tot drie jaar nadat deze is verzameld) in teruggezocht kan worden. Het NJCM vindt dit vanuit privacyoogpunt een zeer onwenselijke situatie. Zij beveelt aan om korte en concrete bewaartermijnen te hanteren.

Klachtbehandeling

De CTIVD is in de huidige Wiv 2002 naast toezichthouder ook interne behandelaar voor klachten over de

[4] Op pagina 90 van het rapport van de commissie Dessens.
[5] EHRM 22 november 2012, appl.no. 39315/06 (Telegraaf Media Nederland/Nederland) en ECLI:NL:RBDHA:2015:7436 (Dataretentie).

AIVD en de MIVD. In het voorstel wordt zij extern klachtbehandelaar met bindende beslisbevoegdheid. Het kabinet stelt voor dan wel een organisatorische scheiding aan te brengen binnen de CTIVD. Zo wordt beoogd de rol van toezicht en van klachtbehandeling te scheiden en daarmee iedere schijn van partijdigheid weg te nemen. De Ombudsman wijst er in zijn reactie op het wetsvoorstel terecht op dat deze scheiding onvolkomen is. Een klager ziet nog steeds één organisatie, met één naam, gevestigd in één bedrijfspand. Ook het NJCM is voorstander van een zo onafhankelijk en onpartijdig mogelijke klachtbehandeling. Zij vindt het wetsvoorstel op dit punt dan ook niet overtuigend.

Samenwerking met inlichtingen- en veiligheidsdiensten van andere landen

Ten slotte merkt het NJCM nog op dat wat betreft de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen de toelichting niet ingaat op wat de Nederlandse inlichtingendiensten moeten doen met informatie die de buitenlandse inlichtingendiensten hebben verkregen met overschrijding van hun bevoegdheden. Bovendien biedt de MvT geen informatie over de beperkingen die Nederland moet stellen aan de informatiedoorstroming naar buitenlandse inlichtingendiensten. In dit kader wijst het NJCM ook op de opinie van de Werkgroep Artikel 29 voor de bescherming van persoonsgegevens waarbij wordt gepleit voor meer internationale controle op de inlichtingendiensten.[6] Het strekt tot de aanbeveling dat in de memorie van toelichting nader wordt ingegaan op de gevolgen van de uitwisseling van gegevens in de samenwerking met inlichtingen- en veiligheidsdiensten van andere landen.

Gelet op het voorgaande adviseert het NJCM het voorstel aan een kritisch onderzoek te onderwerpen en te heroverwegen.

Hoogachtend,

Marloes van Noorloos, voorzitter NJCM

Nederlands Juristen Comité voor de Mensenrechten
Postbus 778
2300 AT Leiden
Telefoon: 071-527 7748
Email: NJCM@law.leidenuniv.nl
www.njcm.nl

[6] Article 29 Data Protection Working Party, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes', 10 april 2014, 819/14/EN WP 215, http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215_en.pdf

Reactie van Stichting DHPA op het concept wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten: Versie juni 2015

Leidschendam, 30-8-2015

Excellentie,

De Dutch Hosting Provider Association ('DHPA') is een samenwerking van de 30 marktleidende hosting- en cloud providers in Nederland. De DHPA vertegenwoordigt een Nederlandse groep van bedrijven in een sector die in de afgelopen decennia is uitgegroeid van een startersmarkt naar één van de belangrijkste ter wereld. De Nederlandse hosting industrie is wereldwijd actief en faciliteert alleen al meer dan 20% van de gehele e-commerce omzet in Europa. Met het hanteren van kernwaarden als professionaliteit, kwaliteit en transparantie dragen de DHPA en haar deelnemers bij aan het vertrouwen in Nederlands als de ideale vestigingsplaats voor op Cloud gebaseerde IT, sites, applicaties e-commerce en daarmee voor de nieuwe digitale economie.

DHPA deelt de zorgen van de Stichting Digital Infrastructuur Nederland ('DINL') over de impact van het conceptwetsvoorstel voor de Wet op de Inlichtingen- en Veiligheidsdiensten (WIV). Het wetsvoorstel wordt gepresenteerd als een louter technische wijziging waarbij de ruimte van de dienst om gegevens te verzamelen wordt uitgebreid, maar uit de concept wettekst blijkt dat de bevoegdheden van de veiligheidsdiensten in aanzienlijke mate worden uitgebreid.

De potentiele impact op de Nederlandse economie en meer specifiek de technologiesector is groot en DHPA vreest dat de concurrentiepositie van de Nederlandse hostingsector ernstig zal verslechteren. DHPA ziet daarom graag een grondige onderbouwing van nut en noodzaak van de specifieke wijzigingen en uitbreidingen van bevoegdheden.
Net als bij de andere wetgeving op het gebied van handhaving en opsporing in het domein van de Online industrie, komt de uitvoering ervan voor een belangrijk deel terecht bij hosting en cloud bedrijven. In de praktijk betekent het dat deze bedrijven moeten opdraaien voor de kosten van het plaatsen van taps, het moeten bewaren en ter beschikking stellen van gegevens, de interactie met politie, justitie en de veiligheidsdiensten, en meer. Het wetsvoorstel voegt hier nog weer andere en nieuwe verplichtingen en dus kosten aan toe, terwijl er geen rekening wordt gehouden met de potentieel grote impact op de bedrijfsvoering van die bedrijven.
Naar het oordeel van DHPA ontbreekt dan ook een proportionaliteitstoetsing, die wel noodzakelijk zou zijn als de kosten door de diensten zelf zouden worden gedragen. Het komt er nu op neer dat de veiligheidsdiensten van informatie worden voorzien op kosten van deze ondernemers.

Verder acht DHPA het noodzakelijk dat een degelijke analyse wordt uitgevoerd van de economische impact van de nieuwe wet, dat wil zeggen een heldere berekening van de met

de uitvoering van de wet gemoeide directe en indirecte kosten en de gevolgen daarvan voor de bedrijven die het treft. DHPA maakt zich zorgen dat de gevolgen van deze kostenstijging- zowel vanuit het oogpunt van de directe kosten voor individuele bedrijven in de hostingsector, als de concurrentiepositie van Nederland als technologie- en internethub - zeer groot zullen zijn.

Verder ziet DHPA een 5 tal specifieke, ernstige problemen met de uitvoerbaarheid van de in het voorstel genoemde bevoegdheden, voor Nederlandse Hosting en cloud bedrijven. Wij lichten deze hier toe.

1. Inbeslagname (art 27 lid 1 sub a en lid 2 en art 42)

Bij gedeelde servers, zoals virtuele servers of cloud servers, zal inbeslagname en fysiek wegnemen van servers leiden tot onderbreking van de dienstverlening aan non-targets (i.e. organisaties of personen die geen onderwerp van onderzoek zijn). Door zo'n ingreep van de diensten zullen andere sites of toepassingen, ook kritische of die met een maatschappelijk belang, gemakkelijk onbeschikbaar kunnen raken. Het behoeft geen betoog dat dit tot een onacceptabele inbreuk op economische en maatschappelijke processen kan leiden.
De proportionaliteit van in beslag nemen van servers zal daarom vooraf moeten worden getoetst en daarbij moet rekening worden gehouden met de impact op de bedrijfsvoering van het betreffende hostingbedrijf en de belangen van andere gebruikers.
De diensten zouden naar de mening van DHPA moeten worden verplicht om bij hun interne proportionaliteitstoetsing rekening te houden met de impact op non-targets van het wegnemen van een server. Dit zou een verduidelijking van art. 43 lid 3 zijn.

2. Ontsleuteling (art 32 lid 1, 33 lid 1 en 41 lid 5)

Iedereen waarvan de diensten het redelijk vermoeden heeft dat zij kunnen meewerken aan het ontsleutelen van communicatie of berichten, kan worden gedwongen daaraan mee te werken. Concreet betekent dit dat hostingbedrijven kunnen worden verplicht de private delen van SSL-certificaten van hun klanten aan de diensten te verstrekken, het betreft dan de diensten waarvoor zij het SSL-certificaat verzorgen.
Naar het oordeel van de DHPA is dit een onacceptabele inbreuk op het vertrouwen in het certificaten systeem. Wij roepen in herinnering wat er gebeurde toen Diginotar werd gecompromitteerd – het gevolg van het feit dat (vermoedelijk) een buitenlandse inlichtingendienst over sleutels kon beschikken en zelf certificaten kon maken.
Het vrijgeven van SSL sleutels betekent ook dat verkeer van non-targets zichtbaar wordt, aangezien ook dat verkeer leesbaar wordt voor de diensten.

De plicht tot het verlenen van medewerking aan ontsleutelen zou moeten worden beperkt tot de aanbieder wiens verkeer wordt versleuteld zodat niet de hosting provider hierop kan worden aangesproken (hoéwel hiermee het probleem slechts wordt verplaatst). Daarnaast zou de proportionaliteit van een dergelijke opvraging door (bij voorkeur vooraf) moeten worden getoetst.

3. Hacking (art 30 lid 1 sub a en b, art 30 lid 2 sub b en c)

Allereerst tekent de DHPA aan dat de term 'Terughacken' soms onterecht wordt gebruikt. Het betreft immers niet de bevoegdheid voor het hacken van systemen van hackers, maar het mogen inbreken op willekeurige gecomputeriseerde apparaten, ook die van non-targets, om informatie te kunnen vergaren. Dat hacken kan dus ook gericht zijn op gedeelde servers, waarbij de diensten gebruik kunnen maken van kwetsbaarheden op delen van non-targets. Ook dit kan gemakkelijk leiden tot onderbreking van de dienstverlening van hosting providers aan die non-targets. Gedeelde servers kunnen daarnaast extra kwetsbaar worden indien de diensten daar ook backdoors installeren in het kader van de installatie van monitoringsoftware (bugs).

Het hacken van/via non-targets zou moeten worden uitgesloten door in artikel 30 *"of door tussenkomst van het geautomatiseerd werk van een derde"* te verwijderen. Daarnaast zou het installeren van backdoors verboden moeten zijn.

4. Gericht en ongericht aftappen van verkeer (artikel 32 resp. 33)

De bevoegdheden maken het voor de diensten mogelijk om in het netwerk van hosting bedrijven ongericht interceptiemiddelen in te zetten. Hosting bedrijven hebben in de regel honderden tot (tien)duizenden klanten en beheren een veelvoud aan servers. De DHPA vreest dat uitbreiding van de mogelijkheid tot (ongerichte) interceptie op deze infrastructuren een significante impact op de bedrijfsvoering van hosting providers zal hebben.

De proportionaliteit van - met name de ongerichte - aftapbevoegdheid dient dan ook te worden gewaarborgd, onder meer door een gedegen voorafgaande toetsing en door de reikwijdte, opslagtermijn en toegang te beperken en, vooral, niet zonder onafhankelijk toezicht. Verder zou naar de mening van DHPA de mogelijkheid moeten worden geboden om de uitkomst van een dergelijke proportionaliteitstoets – dus ook achteraf - via een formele procedure te betwisten.

5. Kosten

Hosting providers zullen flinke kosten moeten maken om mee te werken aan verzoeken van de diensten, zoals het begeleiden van opsporingsambtenaren bij inbeslagnames. Nu worden alleen de directe kosten van aftappen en vorderingen vergoed, het betreft marginale vergoedingen voor administratieve inspanning.

DHPA is van mening dat de door hosters gemaakte kosten bij alle medewerkingsplichten volledig dienen te worden vergoed. Het kan niet zo zijn dat een specifieke sector disproportioneel moet opdraaien voor de kosten van de verzamelwoede van de inlichtingendiensten.

6. Medewerkingsplicht

Daarnaast merkt DHPA op dat hosting providers vaak niet kunnen inloggen op de servers van haar klanten, simpelweg omdat zij niet altijd over de inloggegevens beschikken. Dit is bijvoorbeeld het geval als de klant hardware (fysieke servers) afneemt. Dit gegeven mag niet worden geïnterpreteerd als het niet voldoen aan de medewerkingsplicht. Zie artikel 40 lid 3, dat een onderzoeksplicht suggereert bij vorderingen inzake verkeers- en abonneegegevens.

7. Rechtstreekse Toegang (artikel 22)

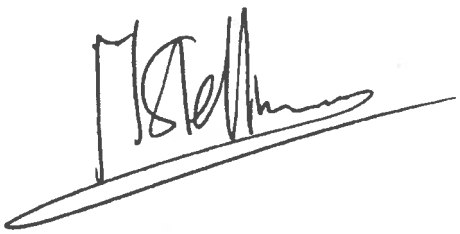
De inlichtingendiensten mogen hosting providers verzoeken om op vrijwillige basis rechtstreekse geautomatiseerde toegang tot gegevens te verlenen en bestanden te verstrekken. Dat is een wat eigenaardige bevoegdheid, die strijdig is met onder andere de WBP.

DHPA deelnemers zullen nimmer de door hun klanten aan hen toevertrouwde data delen of vrijwillig beschikbaar stellen aan de overheid of aan enige andere partij, zonder dat daar een wettelijke basis voor bestaat. Dat zou neerkomen op het overtreden van de WBP.

DHPA is van mening dat verzoeken van opsporingsdiensten altijd een wettelijke basis moeten hebben, en moeten zijn onderbouwd. Verder zouden verzoeken met betrekking tot persoonsgegevens alleen gericht mogen worden tot het bedrijf dat verantwoordelijke is in de zin van de Wet Bescherming Persoonsgegevens.

De DHPA is ten allen tijde bereid over deze onderwerpen in gesprek te gaan

Leidschendam, 30-8-2015
Namens het bestuur



M. Steltman
Directeur