COLLEGE VOOR
DE RECHTEN
VAN DE MENS

ADVIES

Conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..

aan de Minister-President, de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de Minister van Veiligheid en Justitie en de Minister van Defensie
naar aanleiding van de internetconsultatie van 2 juli 2015 tot 1 augustus 2015

31 augustus 2015

SAMENVATTING

De belangrijkste wijziging in de bevoegdheden van de inlichtingen- en veiligheidsdiensten die het conceptwetsvoorstel brengt is de uitbreiding van bevoegdheden om ongericht telecommunicatie en andere gegevensoverdracht te kunnen onderscheppen. Het gaat om het onderscheppen van grote hoeveelheden informatie van een onbegrensde groep mensen die niet onder verdenking staan. Dit kan een grote impact hebben op de privacy van alle Nederlanders. De voorgestelde bepalingen over het toezicht op de veiligheidsdiensten raken ook aan het recht op een effectief rechtsmiddel.

Inbreuken op het recht op privacy zijn slechts gerechtvaardigd indien er een duidelijke en nauwkeurige wettelijke basis is. Voorts dient de wettelijke basis waarborgen te bevatten tegen misbruik. Daarnaast dient te worden aangetoond dat de voorgestelde uitbreiding van bevoegdheden noodzakelijk en proportioneel zijn.

Het College is van oordeel dat het conceptwetsvoorstel in de huidige vorm op onderstaande onderdelen tekort schiet en doet hierbij de volgende aanbevelingen.

- <u>De noodzakelijkheid</u>
  De noodzaak van de uitbreiding van de bevoegdheden voor de diensten is onvoldoende overtuigend aangetoond, mede omdat uit diverse internationale onderzoeken blijkt dat de effectiviteit van grootschalige monitoring van telecommunicatie vanuit nationale-veiligheidsperspectief ernstig kan worden betwijfeld.
  Het College beveelt aan de noodzakelijkheid en in het bijzonder de effectiviteit van de voorgestelde uitbreiding van de interceptiebevoegdheden nader te onderbouwen.

- <u>Wettelijke basis/voorzienbaarheid</u>
  Er is geen sprake van een voldoende duidelijke en nauwkeurige wettelijke basis. Het doelcriterium ‘in het belang van de nationale veiligheid’ is onvoldoende duidelijk. Voorts wordt in het wetsvoorstel niet aangegeven welke misdrijven aanleiding kunnen zijn voor interceptie en ten aanzien van welke categorieën interceptie kan worden ingezet.
  Het College beveelt derhalve aan de aard van de (dreigende) misdrijven aan te geven die aanleiding kunnen vormen voor de interceptie van telecommunicatie en een omschrijving op te nemen van de categorieën mensen waartegen de interceptiebevoegdheden kunnen worden ingezet.

  Het College signaleert dat zowel in de wettekst als in de memorie van toelichting in zeer abstracte termen over de te creëren bevoegdheden wordt gesproken. Deze wijze van formuleren heeft tot consequentie dat de omvang en privacy-impact van die bevoegdheden feitelijk niet te overzien is. De technische mogelijkheden voor gegevensuitwisseling ontwikkelen zich momenteel zo enorm snel, dat de wetgever nu nog niet kan weten welke vormen van gegevensoverdracht op basis van deze wettekst allemaal onderschept zouden kunnen worden. Dat doet vragen rijzen omtrent de voorzienbaarheid van de wettelijke bepalingen en maakt een noodzakelijkheids- en proportionaliteitstoets van de bevoegdheidstoekenning in wezen onmogelijk.
  Het College beveelt aan om tenminste in de memorie van toelichting de strekking en aard van de bijzondere bevoegdheden van de diensten te verhelderen in bewoordingen die ook voor minder ingewijden in het jargon van de diensten te begrijpen zijn en in het licht van gegevensuitwisselingsmogelijkheden die nu reeds

in ontwikkeling zijn, zodat de (potentiële) omvang en impact inzichtelijker worden.

- Voorafgaande toestemming
  Het wetsvoorstel voorziet in voorafgaande toestemming door een Minister in plaats van door een onafhankelijke instantie. Het gaat hier echter om grootschalige data-onderscheppingsoperaties die mogelijk grote groepen mensen kunnen raken. Het College is daarom van mening dat een voorafgaande toetsing door een rechter of een onafhankelijke instantie de voorkeur heeft. Het is een betere garantie voor de weging van de verschillende belangen en het oordeel over de noodzaak, subsidiariteit en proportionaliteit van een dergelijke operatie.
  Het College beveelt aan wettelijk vast te leggen dat een onafhankelijke instantie steeds voorafgaande toestemming dient te verlenen voor de inzet van de bijzonder bevoegdheden van de diensten, in het bijzonder voor gerichte en ongerichte onderschepping van telecommunicatiedata.

- Rechtmatigheidstoezicht door CTIVD
  Ingevolge het conceptwetsvoorstel is de minister niet verplicht oordelen ven de toezichthoudende instantie CTIVD op te volgen. Vanwege het heimelijke karakter van operaties van diensten, acht het College het van belang dat de oordelen over de rechtmatigheid van het handelen van de diensten (los van klachten) van het CTIVD juridisch bindende kracht krijgen. Het College vindt het onbegrijpelijk dat het conceptwetsvoorstel en de memorie van toelichting ten aanzien van dit punt geen acht slaan op de recente ontwikkelingen in zowel de rechtspraak van het EHRM als de meer brede internationale ontwikkeling die onder meer tot uiting komt aanbevelingen en rapporten van VN- en Raad van Europa-instanties. Daarin wordt consequent gehamerd op de noodzaak van een onafhankelijke toezichthouder die, ook los van klachtprocedures, bindende rechtmatigheidsoordelen kan geven
  Het College beveelt aan de oordelen in het kader van het rechtmatigheidstoezicht door de CTIVD juridisch bindend te maken.

- Positie verschoningsgerechtigden
  In het conceptwetsvoorstel ontbreekt een speciale bepaling voor de inzet van bijzondere bevoegdheden jegens verschoningsgerechtigden zoals advocaten of artsen. Dit is een gemis omdat het gaat om bijzondere, kwetsbare en afhankelijke situaties waarin naast het recht op privacy ook het recht op toegankelijke gezondheidszorg en het recht op vertrouwelijke communicatie met advocaten een rol spelen.
  De noodzaak tot het treffen van waarborgen voor de positie van verschoningsgerechtigden versterkt de hierboven geformuleerde aanbeveling van het College om de inzet van communicatie-interceptie door de diensten bij verschoningsgerechtigden afhankelijk te maken van toestemming door de rechter of een andere onafhankelijke instantie (zoals voor journalisten wel in het conceptwetsvoorstel is geregeld).

1 Inleiding

Op 2 juli 2015 is het conceptwetsvoorstel 'Wet op de Inlichtingen- en veiligheidsdiensten 20..' gepubliceerd en opengesteld voor internetconsultatie. Het conceptwetsvoorstel beoogt de huidige Wet op de inlichtingen en veiligheidsdiensten 2002 (Wiv) in zijn geheel te vervangen. De belangrijkste wijziging is dat de Nederlandse inlichtingen- en veiligheidsdiensten (hierna: de diensten) de bevoegdheid krijgen ook op de kabel ongericht telecommunicatie te onderscheppen en dat de bijzondere bevoegdheden van de diensten op een technologie-onafhankelijke manier worden geformuleerd. Daarnaast zijn een aantal wijzigingen aangebracht in het toezicht op de diensten door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD).

Ingevolge artikel 5, tweede lid, van de Wet College voor de Rechten van de Mens heeft het College de bevoegdheid te adviseren over wetsvoorstellen die betrekking hebben op de rechten van de mens. De bevoegdheden die de veiligheidsdiensten ingevolge het onderhavige wetsvoorstel hebben raken in het bijzonder aan het recht op bescherming van de persoonlijke levenssfeer, dat onder meer gegarandeerd wordt door art. 8 van het Europees Verdrag inzake de rechten van de mens en de fundamentele vrijheden (EVRM). Vooral de voorgestelde uitbreiding van de bevoegdheden van de diensten kan een grote impact hebben op de privacy van alle Nederlanders. Het op grote schaal heimelijk monitoren van telecommunicatie betekent niet alleen een enorme directe inbreuk op het recht op privacy, maar levert ook een indirecte aantasting op van diverse andere grondrechten. Door organen van de Verenigde Naties, de Raad van Europa en de Europese Unie is gewezen op het gevaar van een *chilling effect* op de vrijheid van meningsuiting, de vrijheid van vereniging en vergadering en de godsdienstvrijheid. Daarnaast levert een dergelijke praktijk een aantasting op van het recht op een eerlijk proces, onder meer omdat de vertrouwelijkheid van de communicatie tussen advocaten en hun cliënten onvoldoende is gegarandeerd, waardoor de *equality of arms* in gerechtelijke procedures in het geding zou kunnen komen.[1]
De voorgestelde bepalingen met betrekking tot het toezicht op de diensten raken tevens aan het recht op een effectief rechtsmiddel (art. 13 EVRM), het recht van ieder mens om zich bij een onafhankelijke instantie teweer te stellen tegen een vermeende ongerechtvaardigde aantasting van zijn of haar grondrechten. De inrichting van een goed systeem van toezicht op de diensten is niet alleen van belang om ongerechtvaardigde inbreuken op bepaalde mensenrechten te voorkomen, maar dient ook en vooral om het publiek vertrouwen in het optreden van de diensten te waarborgen. Het gaat immers om in het geheim uitgeoefende bevoegdheden die diep kunnen ingrijpen in het privéleven van mensen. Dit publiek vertrouwen in het optreden van de overheid en de inlichtingendiensten staat wereldwijd onder druk, onder meer vanwege de onthullingen van de Amerikaanse klokkenluider Edward Snowden die duidelijk hebben gemaakt dat inlichtingendiensten in de VS en in diverse andere landen de grenzen van hun wettelijke bevoegdheden hebben opgezocht en ook overschreden. Ook het blazoen van de Nederlandse diensten is wat dit betreft niet volledig schoon.

[1] Zie o.m. *Democratic and effective oversight of national security services*, Issue paper published by the Council of Europe Commissioner for Human Rights, Strasbourg: Council of Europe, May 2015; European Parliament, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, 21 February 2014, Doc. No. A7-0139/2014; Report of the Office of the UN High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37, 30 June 2014. Vgl. op dit punt de conclusies van het HvJ EU in zaak C-293/12 (*Digital Rights Ireland*) t.a.v. de algemene bewaarplicht voor telecombedrijven en internet service providers van de zogenoemde verkeersgegevens van al hun klanten.

Derhalve heeft het College besloten een advies uit te brengen over dit wetsvoorstel. In dit advies zal worden ingegaan op de aspecten van het conceptwetvoorstel die vanuit het perspectief van de genoemde mensenrechten het meest relevant zijn: de uitbreiding van de interceptiebevoegdheden, de toestemmingverlening voor de inzet van bijzondere bevoegdheden (waaronder de interceptiebevoegdheden) en het externe toezicht op de uitoefening van die bevoegdheden.

2 Uitbreiding van de interceptiebevoegdheden en uitoefening van de overige bijzondere bevoegdheden van de diensten

2.1 Wat houdt de uitbreiding van de interceptiebevoegdheden in?

Zoals opgemerkt is de belangrijkste wijziging in het conceptwetsvoorstel dat de diensten meer bevoegdheden krijgen om ongericht 'in de bulk' telecommunicatie te onderscheppen, namelijk ook op de kabel (zie art. 33 van het conceptwetsvoorstel). Het gaat hier om het grootschalig 'aftappen' van alle data die via een bepaalde kabelverbinding worden verzonden. Onder de huidige Wiv mogen de diensten alleen ongericht data onderscheppen die via niet-kabelgebonden kanalen ('via de lucht': radiofrequenties, satellietverkeer, etc.) worden gecommuniceerd, terwijl ruim 90 procent van de communicatie tegenwoordig via de kabel gaat. Het conceptwetsvoorstel biedt veiligheidsdiensten de mogelijkheid om op grote schaal alle telecommunicatie van iedereen te onderscheppen, ten behoeve van een tevoren bepaald doel. De toestemming hiervoor moet door de betrokken minister (van BZK of van Defensie) worden verleend. De toestemming geldt voor een periode van maximaal 12 maanden, maar kan telkens worden verlengd voor eenzelfde periode (art. 33 lid 2).
Het gaat om een uitbreiding van de bevoegdheid tot *ongerichte* data mining. Anders dan bij onderscheppen van *gerichte* telecommunicatie gaat het hier dus om het onderscheppen van grote hoeveelheden informatie van een onbegrensde groep mensen die niet onder verdenking staat, of tevoren op grond van enigerlei uiting of gedraging is geïdentificeerd als een potentieel gevaar voor de nationale veiligheid. In essentie gaat het om het onderscheppen van telecommunicatie van iedereen.

Het is nu juist dit grootschalige en massale karakter van het verzamelen van telecommunicatiegegevens dat het Europees Hof van Justitie in de dataretentie-zaak[2] tot de conclusie bracht dat er sprake was van een disproportionele inbreuk op het recht op privacy.[3] De memorie van toelichting (MvT) bij het conceptwetsvoorstel lijkt het grootschalige en massale karakter van de interceptie van communicatiedata enigszins te verhullen door op p. 63 te spreken van 'doelgerichte verwerving van telecommunicatie' en dit te presenteren als een onderdeel van de waarborgen die in het nieuwe normatieve kader voor interceptie zijn ingebouwd. Deze doelgerichtheid van de telecommunicatieverwerving levert echter niet of nauwelijks een beperking van de grootschaligheid of massaliteit van die verwerving op, ook al moet op grond van art. 24 lid 6, volgens de uitleg gegeven op p. 67 van de MvT, het doel van een interceptieoperatie zo precies mogelijk, en niet slechts in globale termen, worden geformuleerd.
Ten aanzien van ongerichte interceptie van zogenoemde metadata is sprake van voortschrijdend juridisch inzicht. Niet langer wordt gedacht dat dit een minder indringende inbreuk op de privacy oplevert, omdat bij de gegevensonderschepping niet

[2] HvJ EU, zaak C-293/12 (*Digital Rights Ireland)*
[3] Dit arrest had weliswaar geen betrekking op interceptie van telecommunicatiegegevens door inlichtingen- en veiligheidsdiensten, maar op de in de EU-dataretentierichtlijn opgenomen bewaarplicht voor telecomproviders, maar wat betreft de massaliteit en grootschaligheid gaat het om vergelijkbare gegevensverzamelingspraktijken.

gelijk sprake is van kennisneming van de inhoud van de communicatie. Voor het vaststellen van de ernst van de inbreuk is evenzeer van belang de schaal waarop gegevens worden verzameld en hoe ingrijpend de gehanteerde ontsluitingsmethodiek is voor de privacy van de burger. Bulk-interceptie en de toepassing van verfijnde methodieken van metadata-analyse kunnen onder omstandigheden ingrijpender zijn dan een kortstondige interceptie van de inhoud van de telecommunicatie, zo stelt ook het kabinet in zijn brief aan de Tweede Kamer van 11 maart 2014.[4]

Alom wordt tegenwoordig ingezien en erkend dat ook ongerichte interceptie een enorme impact kan hebben op de privacy. De *UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* schreef in een rapport gepubliceerd in september 2014 over dergelijke massale afluisterbevoegdheden het volgende: "langdurige, massale en ongerichte interceptie van alle telecommunicatie of metadata via een bepaald kanaal doet de kern van het recht op privacy volledig teniet. De inbreuk op het telecommunicatiegeheim is dan immers niet langer de uitzondering, maar de regel."[5] Dit leidt tot de conclusie dat ten aanzien van ongerichte interceptie vanuit een mensenrechtenkader minstens even strikte waarborgen - zo niet zwaardere - waarborgen dienen te gelden als ten aanzien van gerichte interceptie.

2.2 Mensenrechtenkader

Bij het conceptwetsvoorstel is vooral het recht op bescherming van de persoonlijke levenssfeer in het geding. Met het uitoefenen van bijzondere bevoegdheden als aftappen van telefoons (art. 32), observeren en volgen van personen (art. 25), doorzoeken van besloten plaatsen of afgesloten voorwerpen (art. 27), DNA-onderzoek (art. 28), openen van brieven (art. 29), het *hacken* van computers (art. 30) en het gericht en ongericht onderscheppen van telecommunicatie en andere vormen van gegevensoverdracht (art. 32 en 33) wordt inbreuk gemaakt op het privéleven van burgers.

Inbreuken op het recht op bescherming van de persoonlijke levenssfeer zijn gerechtvaardigd indien deze bij wet zijn voorzien. Dit houdt in dat de inbreuk gebaseerd moet zijn op een wettelijke grondslag die voldoende duidelijk en nauwkeurig is (de voorzienbaarheidseis). De wettelijke basis dient voorts waarborgen te bevatten tegen misbruik, oneigenlijk gebruik of ongerechtvaardigd gebruik van de privacy-aantastende bevoegdheden en voorwaarden te stellen aan het bewaren van de verzamelde gegevens en het delen daarvan met andere (overheids)instanties. Daarnaast dient bij de introductie van nieuwe privacy-aantastende bevoegdheden te worden aangetoond dat deze noodzakelijk en proportioneel zijn.

2.3 Noodzaak uitbreiding interceptiebevoegdheden voldoende aangetoond?

Zoals de CTIVD in haar jaarverslag 2014/15[6] heeft opgemerkt, is in Nederland nauwelijks discussie over de vraag in hoeverre uitbreiding van de interceptiebevoegdheden van de diensten noodzakelijk is. Zoals blijkt uit het rapport-Dessens dat de uitbreiding

[4] http://www.rijksoverheid.nl/nieuws/2014/03/11/kabinetsreactie-commissie-dessens-en-ctivd-rapport.html
[5] UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Report 23 September 2014, UN Doc. A/69/397, para. 20 en 25.
[6] Jaarverslag CTIVD 2014-2015, p. 28; te raadplegen op: http://www.ctivd.nl/documenten/jaarverslagen/2014/04/30/jaarverslag-2014.

aanbeveelt[7] en uit de MvT bij het conceptwetsvoorstel, is het belangrijkste argument dat de toegestane niet-kabelgerichte interceptiebevoegdheid slechts 10% van het huidige telecomverkeer beslaat. Verder wordt in zowel het rapport-Dessens als de MvT eigenlijk niet of nauwelijks beargumenteerd waarom de diensten niet buiten deze bevoegdheid zouden kunnen. Het blijft bij de enigszins cryptische frase dat 'de diensten zicht dienen te hebben op de dreigingen waaraan de samenleving en de staat in het digitale domein kunnen worden blootgesteld'.[8] Niet duidelijk wordt of de noodzaak van dit 'zicht hebben op' dwingt tot massale communicatie- of data-interceptie. Bovendien lijkt zowel aan het rapport-Dessens als aan de MvT de veronderstelling ten grondslag te liggen dat de bevoegdheid tot ongerichte interceptie van kabelgebonden telecommunicatie bij de WIV-herziening van 2002 al zou zijn gecreëerd, als toen zou zijn voorzien dat de communicatie via dit kanaal zo'n enorme vlucht zou nemen. Het College wijst erop dat een belangrijke reden voor onderscheid tussen interceptie van kabelgebonden en niet-kabelgebonden communicatie in het verleden ook was dat de niet-kabelgebonden communicatie naar zijn aard een veel minder afgeschermd karakter heeft, omdat de betreffende signalen in beginsel zonder veel moeite door iedereen die over de geschikte apparatuur beschikt 'uit de lucht' opgevangen kunnen worden. Het is dus helemaal niet zo logisch om het onderscheppen van kabelgebonden en niet-kabelgebonden telecommunicatie op gelijke voet mogelijk te maken, want het gaat om onvergelijkbare communicatiekanalen.
Een belang dat een rol zou kunnen spelen bij de bevoegdheid tot ongerichte interceptie is de positie van de Nederlandse diensten in de samenwerking met buitenlandse diensten: verzamelde gegevens vormen een 'ruilmiddel' in de contacten met andere diensten. In het in juli 2015 gepubliceerde onderzoeksrapport van de CTIVD over de samenwerking van de militaire inlichtingen- en veiligheidsdienst (MIVD) met buitenlandse diensten formuleert de CTIVD dit als volgt:

> "Het is voor de MIVD van belang zorg te dragen voor een voldoende groot aanbod van uitruilbare inlichtingen. Het bijhouden van de quid-pro-quo-balans – de kwantitatieve en kwalitatieve verhouding tussen hetgeen is verstrekt en hetgeen is verkregen – is van wezenlijk belang voor de MIVD in het bepalen van de eigen positie ten opzichte van de buitenlandse diensten."[9]

Dit argument wordt in de MvT echter niet genoemd en het is ook maar de vraag of dit zodanig zwaar weegt dat het de inbreuk op de persoonlijke levenssfeer van grote aantallen burgers kan rechtvaardigen. In haar jaarverslag 2014/15 concludeerde de CTIVD de noodzaak van de uitbreiding van de interceptiebevoegdheden nog niet voldoende was aangetoond. Het College constateert dat ook in de MvT bij het conceptwetsvoorstel nog geen duidelijke en zwaarwegende redenen worden aangevoerd.
Onderdeel van de noodzakelijkheidstoets is het vereiste van effectiviteit van de grootschalige ongerichte communicatiedata-interceptie. Daarbij is, zo blijkt ook uit allerlei internationale onderzoeken, grote vraagtekens te plaatsen. Zo laat Amerikaans onderzoek zien dat er geen enkele situatie is geweest waarin massale ongerichte interceptie van telecommunicatie heeft geleid tot het voorkomen van een terroristische aanslag in Amerika. En slechts eenmaal, aldus dit onderzoek, heeft een dergelijke operatie geleid tot het opsporen van een verdachte, waarbij het de vraag is of dit ook niet op een andere wijze had gekund.[10]

---

[7] Commissie-Dessens, Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 – Naar een nieuwe balans tussen bevoegdheden en waarborgen, rapport uitgebracht op 2 december 2013 (*Kamerstukken II* 2013-2014, 33 820, nr.2, pag 76 e.v.)
[8] MvT p. 63.
[9] CTIVD-toezichtsrapport nr. 22b, over de samenwerking van de MIVD met buitenlandse inlichtingen- en veiligheidsdiensten, juridische bijlage, p. 10.
[10] 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*

Dit leidt tot het volgende belangrijke element uit de noodzakelijkheidstoets, namelijk of het beoogde doel (de nationale veiligheid) niet op andere manieren kan worden bereikt die minder impact hebben op de privacy (het subsidiariteitsvereiste). In de MvT wordt geen aandacht besteed aan eventuele alternatieve methoden voor het massaal onderscheppen van telecommunicatie.
Ook bij de proportionaliteit van ongerichte (bulk)interceptie zijn kritische vraagtekens te zetten. Het gaat immers om het onderscheppen van grote hoeveelheden telecommunicatie van een onbegrensd aantal mensen op wie geen enkele vorm van verdenking rust. Naar zijn aard is dit een zeer ernstige inbreuk op het recht op privacy die uitsluitend gelegitimeerd is als is aangetoond dat de gehanteerde methoden effectief zijn.

Het College beveelt aan de noodzakelijkheid, en in het bijzonder de effectiviteit, van de voorgestelde uitbreiding van de interceptiebevoegdheden nader te onderbouwen.

2.4 Voorzienbaarheid

Het conceptwetsvoorstel biedt een wettelijke basis voor het uitoefenen van een aantal (bijzondere) bevoegdheden door de diensten waarbij inbreuk wordt gemaakt op het privéleven van burgers. Zoals hierboven reeds is aangegeven geldt ten aanzien van de wettelijke basis de zogenoemde voorzienbaarheidseis. Deze houdt in dat in de wet voldoende duidelijk en precies moet zijn aangegeven onder welke omstandigheden de grondrechtenbeperkende maatregel kan worden toegepast, zodat de burger kan weten in welke situatie of bij welke vormen van gedrag hij te maken kan krijgen met de toepassing van die maatregel.[11]
Op basis van het conceptwetsvoorstel (art. 23) mogen de bevoegdheden worden uitgeoefend 'in het kader van een goede taakuitoefening van de veiligheidsdiensten' en – onder bepaalde voorwaarden - 'ter ondersteuning hiervan'. Ingevolge art. 8 en 10 van het conceptwetsvoorstel voeren de veiligheidsdiensten hun taken uit in het belang van de nationale veiligheid. Al eerder, in zijn advies over de aanpassing van art. 13 Grondwet, wees het College op het onbepaalde karakter van de term 'nationale veiligheid'. Ook bij de grondwetsherziening van 2006 is hier uitgebreid over gediscussieerd. Mede gezien het feit dat in het conceptwetsvoorstel alle activiteiten van de diensten worden geacht gericht te zijn op het belang van de nationale veiligheid heeft dit begrip als doelcriterium voor de beperking van een grondrecht als gevolg van de activiteiten van de diensten een geringe normatieve kracht. Nu kan daarbij worden opgemerkt, zoals de MvT op p. 188-189 doet, dat de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) ruimte laat voor de inzet van 'secret surveillance' ten behoeve van de bescherming van de nationale veiligheid en dat de staat daarbij een redelijk ruime 'margin of appreciation' wordt gegund, ook al omdat de noodzaak tot heimelijke uitoefening van de bijzondere bevoegdheden van de diensten met zich brengt dat deze niet altijd op een even precieze manier wettelijk kunnen worden ingekaderd als bevoegdheden die in het openbaar worden uitgeoefend. Dat neemt echter niet weg dat het EHRM in zijn jurisprudentie ook bij dit soort bevoegdheden hecht aan een zo precies mogelijke juridische inkadering, om de burger te beschermen tegen willekeur.
In diverse uitspraken over geheime surveillance door veiligheidsdiensten – ook over ongerichte interceptie – heeft het EHRM een aantal minimumwaarborgen vastgesteld die in

---

Intelligence Surveillance Court, 23 January 2014, https://www.pclob.gov/library.html, p. 11; US National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, January 2015, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[11] Zie voor deze eis in de context van de uitoefening van bevoegdheden door inlichtingen- en veiligheidsdiensten o.m. EHRM 4 mei 2000, no. 28341/95 (*Rotaru t. Roemenië*), § 52; EHRM 1 juli 2008, no. 58243/00 (*Liberty e.a. t. VK*), § 59; EHRM 10 februari 2009, no. 25198/02 (*Iordachi e.a. t. Moldavië*), § 37.

de nationale wetgeving moeten zijn opgenomen.[12] Een van deze waarborgen is dat de nationale wetgeving regels dient te bevatten over de aard van de (dreigende) misdrijven die aanleiding kunnen vormen voor de interceptie van telecommunicatie en een definitie moet geven van de categorieën mensen waartegen de interceptiebevoegdheid kan worden ingezet. Het College meent dat dit in het conceptwetsvoorstel op onvoldoende wijze gebeurt. Weliswaar kan dit aspect meegewogen worden in de algemene noodzakelijkheidseis die in art. 24 is opgenomen en in het afwegingskader gegeven in art. 43 en 44. Daarmee is de bedoelde door het EVRM vereiste waarborg echter nog niet op voldoende specifieke wijze gegarandeerd. Het College wijst in dit verband op het arrest *Liberty e.a. t. VK* uit 2008 waarin het EHRM oordeelde dat de toenmalige Britse wetgeving niet aan deze voorwaarden voldeed, omdat deze geen wezenlijke grenzen stelde aan de omvang van de data-onderschepping (d.w.z. aan de hoeveelheid te onderscheppen gegevens of de typen communicatiekanalen die uitgeluisterd mochten worden) en de toestemmingverlening voor interceptie in handen legde van de verantwoordelijke minister, die daarvoor toestemming kon geven indien hij dit nodig achtte ten behoeve van enkele in tamelijk abstracte termen omschreven belangen, zoals 'de nationale veiligheid', het voorkomen of opsporen van 'ernstige misdrijven' of de bescherming van 'het economisch welzijn van het land'. Deze vaagheid van de Britse wetgeving, samen met het feit dat er geen kenbare regels waren over de zoektermen waarmee de onderschepte communicatie doorzocht kon worden, zorgde ervoor dat het Hof een schending van het EVRM vaststelde.[13]

Het College beveelt derhalve aan de aard van de (dreigende) misdrijven aan te geven die aanleiding kunnen vormen voor de interceptie van telecommunicatie en een omschrijving op te nemen van de categorieën mensen waartegen de interceptiebevoegdheden kunnen worden ingezet.

Het valt het College op dat, zowel in de wettekst als in de MvT, in zeer abstracte termen over de te creëren bevoegdheden wordt gesproken. In het licht van het bereiken van een 'techniekonafhankelijke' formulering van de bevoegdheden valt dat voor de wettekst nog wel te billijken. De MvT zou dan echter moeten voorzien in een uitleg van de strekking en aard van de bevoegdheden in begrijpelijke taal, zodat het ook voor niet-ingewijden in het jargon van de diensten duidelijk wordt hoe omvangrijk of indringend de bevoegdheden zijn. Daarin slaagt de MvT nu niet. Zo blijft bijvoorbeeld onduidelijk welke vormen van 'gegevensoverdracht door middel van een geautomatiseerd werk' allemaal onderschept kunnen worden op basis van art. 32 en 33. Het ligt voor de hand om hierbij in ieder geval te denken aan e-mailverkeer en *social media*-berichten. Echter, nu de voortschrijdende technologie allerlei nieuwe vormen van gegevensuitwisseling (denk aan: 'the internet of things') mogelijk maakt, vallen ook onder de voorgestelde bevoegdheidsbepaling. En gelet op de snelle ontwikkelingen op dit terrein valt niet te overzien welke vormen van telecommunicatie/gegevensoverdracht in de nabije toekomst mogelijk zijn. De techniekonafhankelijke formulering van de voorgestelde wettelijke bepaling zorgt zo ook voor een onbegrensdheid van de interceptiebevoegdheid, waarbij op dit moment voor een technisch niet-ingewijde volstrekt niet te voorzien is wat de omvang van die bevoegdheid – en de impact daarvan op de privacy – in de toekomst zal zijn. Het College acht het van belang dat de MvT meer inzicht geeft op dit punt, omdat anders het kabinet de verdenking

[12] EHRM 29 juni 2006, no. 54934/00 (*Weber en Saravia t. Duitsland*), § 95: 'In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.'

[13] EHRM 1 juli 2008, no. 58243/00 (*Liberty e.a. t. VK*), § 64-67.

op zich laadt dat het een bewuste keuze is om geen helderheid te verschaffen. Als die duidelijkheid niet wordt verschaft is het ook niet mogelijk om een gefundeerde noodzakelijkheids- en proportionaliteitstoets uit te voeren met betrekking tot de bevoegdheidstoekenning.

et College beveelt aan om tenminste in de memorie van toelichting de strekking en aard van de bijzondere bevoegdheden van de diensten te verhelderen in bewoordingen die ook voor minder ingewijden in het jargon van de diensten te begrijpen zijn en in het licht van gegevensuitwisselingsmogelijkheden die nu reeds in ontwikkeling zijn, zodat de (potentiële) omvang en impact inzichtelijker worden.

2.5 Waarborgen

De eis van waarborgen tegen misbruik of ongerechtvaardigd gebruik van bevoegdheden die een inbreuk opleveren op het recht op bescherming van de persoonlijke levenssfeer, vertaalt zich in de jurisprudentie van het EHRM vooral in een verplichting tot het in stand houden van een adequaat systeem van onafhankelijk toezicht op de bevoegdhedenuitoefening door de diensten.[14] Juist vanwege het heimelijke karakter van *surveillance* operaties door inlichtingen- en veiligheidsdiensten heeft het EHRM al in zijn vroegste jurisprudentie het belang van effectieve controle en toezicht op de diensten benadrukt.[15] De ontoereikende wijze waarop het toezicht op de Nederlandse diensten in het conceptwetsvoorstel wordt vormgegeven vormt een zodanig essentieel onderdeel van de beoordeling door het College dat deze in de onderstaande paragraaf uitvoerig wordt toegelicht.

3 De inrichting van het toezicht op de diensten en de bevoegdheden van de CTIVD

3.1 Voorafgaande toestemming door een onafhankelijke instantie

In het algemeen kan worden gesteld dat het EHRM in zijn jurisprudentie, mede vanwege het heimelijke karakter van de uitoefening van de bijzondere bevoegdheden door de diensten, meermaals een sterke voorkeur heeft uitgesproken voor voorafgaande toetsing van de inzet van dergelijke bevoegdheden door de onafhankelijke rechter.[16] Het College constateert dat in het conceptwetsvoorstel wordt vastgehouden aan het huidige systeem waarin niet een onafhankelijke instantie, maar de betrokken minister toestemming verleent voor de inzet van bijzondere bevoegdheden. Uitsluitend ten aanzien van het openen van brieven en het gebruik van bijzondere bevoegdheden gericht op het achterhalen van de bron van een journalist voorziet het conceptwetvoorstel in een voorafgaande toestemming door de rechter.[17]
Op p. 190 van de MvT geeft het kabinet aan dat voorafgaande rechterlijke toetsing niet dwingend uit de EHRM-jurisprudentie voortvloeit. Het verwijst hierbij naar het EHRM-

[14] Zie hierover o.m. European Commission for Democracy through Law (Venice Commission), *Report on the Democratic Oversight of the Security Services*, CDL-AD(2007)016, Strasbourg 11 June 2007 en *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006, Strasbourg 7 April 2015.
[15] EHRM 6 september 1978, no. 5029/71 (*Klass e.a. t. Duitsland*), § 34-36.
[16] O.m. EHRM 6 september 1978, no. 5029/71 (*Klass e.a. t. Duitsland*), § 34-36; EHRM 29 juni 2006, no. 54934/00 (*Weber en Saravia t. Duitsland*), § 32; EHRM 26 april 2007, no. 71525/01 (*Dumitru Popescu t. Roemenië*); EHRM 10 februari 2009, no. 25198/02 (*Iordachi e.a. t. Moldavië*), § 40.
[17] Dit als gevolg van het feit dat Nederland op dit punt veroordeeld werd in EHRM 22 februari 2013, no. 39315/06 (*Telegraaf e.a. t. Nederland*).

arrest *Kennedy t. het Verenigd Koninkrijk* uit 2010. Daarmee gaat het kabinet echter voorbij aan de duidelijke voorkeur voor rechterlijke toestemmingverlening die het EHRM ook na 2010 nog verschillende keren heeft uitgesproken[18] en die ook in *Kennedy* vooropstaat.[19] In het recente *issue paper* van de mensenrechtencommissaris van de Raad van Europa over effectief toezicht op de inlichtingen- en veiligheidsdiensten meldt deze dat de meeste landen in Europa inmiddels een systeem van voorafgaande rechterlijke toestemming voor de inzet van bijzondere bevoegdheden kennen.[20] Landen als Zweden, Duitsland en België kennen een systeem waarin de autorisatie voor de inzet van de bijzondere bevoegdheden niet is belegd bij de gewone rechter, maar bij een specifieke onafhankelijke toezichtinstantie. Ook in het Verenigd Koninkrijk is enkele maanden geleden het voorstel gelanceerd om de toestemmingverlening te beleggen bij een onafhankelijke semi-rechterlijke toezichtcommissie.[21] Door vast te houden aan ministeriële toestemming plaatst Nederland zich op dit punt in de Europese achterhoede en wordt een risicovolle koers ingezet. Immers, naarmate zich binnen Europa een grotere consensus aftekent, is het zeer wel mogelijk dat het EHRM autorisatie door een onafhankelijke autoriteit als dwingende eis voortvloeiend uit art. 8 EVRM zal gaan zien en tot de conclusie komt dat de Nederlandse wetgeving hier tekort schiet.
De *Venice Commission* van de Raad van Europa wees er al in 2007 op dat ministeriële toestemming weliswaar als een waarborg kan worden gepresenteerd, maar niet een heel krachtige waarborg vormt vanwege de informatie- en kennisachterstand die een minister doorgaans heeft ten opzichte van de diensten: *'the monopoly of specialist knowledge possessed by the agency will itself grant the agency a considerable degree of autonomy in practice from governmental control'*.[22] Het principe van ministeriële verantwoordelijkheid en de daarmee samenhangende verantwoordingsplicht jegens het parlement wordt door de *Venice Commission* in het algemeen niet als gezien als voldoende om te waarborgen dat het optreden van de diensten binnen de mensenrechtelijke grenzen blijft.[23] Parlementaire controle is weliswaar van belang, maar in aanvulling hierop valt rechtmatigheidscontrole door een onafhankelijke gespecialiseerde toezichthouder te prefereren, zo stelt ook de Mensenrechtencommissaris van de Raad van Europa: *'Expert oversight bodies are generally better placed to undertake the ongoing, detailed and politically neutral screening that human rights protection requires'*.[24]
De VN-Hoge Commissaris voor de Mensenrechten wees er in 2014 op dat in het proces van toestemmingverlening de 'public interest advocacy', de toets of de data-interceptie te rechtvaardigen valt in het licht van de relevante mensenrechten, goed gewaarborgd dient te zijn. Dat kan in zijn ogen het beste door voorafgaande rechterlijke toetsing.[25] In lijn met de opmerkingen van de *Venice Commission* en de Mensenrechtencommissaris van de Raad van Europa wijst het College erop dat er ook veel voor te zeggen valt om deze voorafgaande toetsing in handen te leggen van een gespecialiseerde instantie, mits die

[18] EHRM 8 maart 2011, no. 12739/05 (*Goranova-Karaeneva t. Bulgarije*), § 49-50; EHRM 27 november 2012, no. 7222/05 (*Savovi t. Bulgarije*), § 56, EHRM 15 januari 2015, no. 68955/11 (*Dragojević t. Kroatië*), § 92-93.
[19] EHRM 18 mei 2010, no. 26839/05 (*Kennedy t. VK*), § 167.
[20] *Democratic and effective oversight of national security services*, Issue paper published by the Council of Europe Commissioner for Human Rights, Strasbourg: Council of Europe, May 2015.
[21] *A Question of Trust*. Report of the Investigatory Powers Review by David Anderson Q.C., Independent Reviewer of Terrorism Legislation, Presented to the Prime Minister pursuant to section 7 of the Data Retention and Investigatory Powers Act 2014, London: June 2015, te raadplegen via https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/.
[22] Venice Commission 2007 (zie noot 14), § 78.
[23] *Ibidem*.
[24] *Democratic and effective oversight of national security services*, Issue paper published by the Council of Europe Commissioner for Human Rights, Strasbourg: Council of Europe, May 2015, p. 62.
[25] Report of the Office of the UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/27/37, 30 June 2014, § 38.

instantie qua onafhankelijkheid en bevoegdheden dan met een rechter te vergelijken is. Meer dan de gewone rechter zal zo'n gespecialiseerde instantie in staat zijn om technische en juridische expertise op te bouwen waardoor de preventieve toetsing een meer inhoudelijk karakter kan krijgen.
Het ontbreekt in de MvT aan een toelichting waarom is vastgehouden aan ministeriële toestemmingverlening. De MvT noemt geen argumenten waarom een preventieve toets door een onafhankelijk orgaan op onoverkomelijke bezwaren zou stuiten. Niet duidelijk wordt gemaakt waarom een dergelijke toets wel kan worden ingevoerd bij het openen van fysieke post en bij journalisten, en niet 'overall' voor alle telecommunicatie. Uitsluitend in zijn reactie op het de jaarrapportage van het College[26] heeft het kabinet aangegeven dat het vindt dat het de minister is die de toestemming moet geven vanwege het internationale aspect van de taakuitvoering van de veiligheidsdiensten. De verantwoordelijkheid voor de mogelijk daaruit voortvloeiende risico's dient in de ogen van het kabinet in alle gevallen te worden gedragen door de minister en niet door de rechter. Het gaat hier echter om grootschalige data-onderscheppingsoperaties die mogelijk grote groepen mensen kunnen raken. Het College is daarom van mening dat een voorafgaande toetsing door een rechter of een onafhankelijke instantie de voorkeur heeft. Het is een betere garantie voor de weging van de verschillende belangen en het oordeel over de noodzaak, subsidiariteit en proportionaliteit van een dergelijke operatie. Zeker nu ook in andere met Nederland vergelijkbare landen de toestemmingverlening bij een onafhankelijke autoriteit is belegd, valt niet in te zien waarom dat in Nederland niet zou kunnen.

Het College beveelt aan wettelijk vast te leggen dat een onafhankelijke instantie steeds voorafgaande toestemming dient te verlenen voor de inzet van de bijzonder bevoegdheden van de diensten, in het bijzonder voor gerichte en ongerichte onderschepping van telecommunicatiedata.

3.2 Het rechtmatigheidstoezicht door de CTIVD: de noodzaak van bindende oordelen

In het conceptwetsvoorstel wordt ten aanzien van het toezicht door de CTIVD een zogenoemd 'heroverwegingsstelsel' geïntroduceerd. Dit houdt in dat als de CTIVD tot de conclusie komt dat een door de minister verleende toestemming voor de inzet van bepaalde bijzondere bevoegdheid onrechtmatig is, de minister verplicht is deze te heroverwegen. De minister is echter in dit voorgestelde stelsel niet verplicht het oordeel van de CTIVD op te volgen. Wel is in het wetvoorstel bepaald dat de minister verplicht is aan de CTIVD en aan de Commissie voor Inlichtingen- en veiligheidsdiensten van de Tweede Kamer (CIVD) mede te delen als hij besluit een operatie door te laten gaan ondanks een negatief oordeel van de CTIVD. Eventueel kan de Tweede-Kamercommissie de minister dan ter verantwoording roepen, zo is de gedachte.
Het College stelt vast dat met dit heroverwegingsstelsel een essentieel onderdeel van de aanbevelingen van de Commissie-Dessens wordt genegeerd. Juist met het oog op het bewaren van een juiste balans tussen ingrijpende privacy-aantastende bevoegdheden en mensenrechtelijke waarborgen beval de Commissie-Dessens aan de uitbreiding van de interceptiebevoegdheden te koppelen aan versterking van het rechtmatigheidstoezicht door de CTIVD, door deze commissie de bevoegdheid te geven tot het uitspreken van een bindend rechtmatigheidsoordeel. In het conceptwetsvoorstel is er echter voor gekozen om alleen de oordelen van de CTIVD in het kader van de klachtbehandeling juridisch bindend te maken en niet de oordelen die de CTIVD kan geven in het kader van haar

[26] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2014/11/03/tussenrapportage-nationaal-actieplan-mensenrechten-en-kabinetsreactie-op-de-jaarrapportage-mensenrechten-in-nederland-2013-van-het-college-voor-de-rechten-van-de-mens.html.

rechtmatigheidstoezicht, dat plaatsvindt tijdens en na afloop van door de diensten uitgevoerde operaties. Door deze keuze schiet het wetsvoorstel op een essentieel onderdeel tekort. In essentie brengt het conceptwetsvoorstel geen enkele wijziging in de bevoegdheden van de CTIVD voor wat betreft de uitoefening van het rechtmatigheidstoezicht.
De eis dat een onafhankelijke toezichthouder bindende oordelen moet kunnen geven in klachtprocedures over het optreden van de diensten is, zoals de MvT ook aangeeft, ondubbelzinnig geformuleerd in diverse arresten van het EHRM.[27] Deze eis vloeit voort uit het recht op een effectief rechtsmiddel van art. 13 EVRM. De eisen die uit dit recht voortvloeien zijn echter ook relevant voor de inrichting van het rechtmatigheidstoezicht door de onafhankelijke toezichthouder dat los van het indienen van klachten plaatsvindt. Dit rechtmatigheidstoezicht dient namelijk in belangrijke mate als vervanger van een door de betrokkene in te roepen rechtsmiddel. Het heimelijke karakter van de operaties van de diensten brengt immers met zich dat betrokken onwetend zullen zijn over jegens hen gemaakte privacy-inbreuken, waardoor de stap naar het inroepen van een rechtsmiddel niet gezet wordt. Het College acht het dan ook logisch om de effectiviteitseisen zoals die in de EHRM-jurisprudentie geformuleerd zijn voor klachtprocedures ook toe te passen op het rechtmatigheidstoezicht dat plaatsvindt los van een ingediende klacht. Indien de eis van een juridisch bindend oordeel alleen zou gelden voor oordelen op klachtprocedures zou dat grote afbreuk doen aan de effectiviteit van het toezicht, terwijl nu juist die effectiviteit in de recente Straatsburgse jurisprudentie over het toezicht op inlichtingen- en veiligheidsdiensten zo centraal wordt gesteld.[28] Zeker daar waar voorafgaande autorisatie door een onafhankelijke instantie voor de inzet van bijzondere bevoegdheden ontbreekt, hecht het EHRM sterk aan een onafhankelijke toezichthouder die bindende beslissingen kan nemen. De op p. 200 van de MvT neergelegde opvatting van het kabinet dat het conceptwetsvoorstel zorgt voor geheel EVRM-conforme bevoegdheden voor de CTIVD deelt het College niet. Juist vanwege het massale karakter van ongerichte telecommunicatieonderschepping acht het College het in het bijzonder bij deze bevoegdheid van essentieel belang dat de juridische bindendheid van rechtmatigheidsoordelen niet beperkt blijft tot de oordelen op – sporadisch ingediende – klachten. Dat die keuze in het conceptwetsvoorstel niet gemaakt wordt vindt het College, ook vanwege de ontwikkeling die de EHRM-jurisprudentie op dit punt vertoont, onbegrijpelijk en onjuist. Het kabinet kiest hier bewust voor een route die Nederland op termijn vrijwel zeker in botsing brengt met de EVRM-verdragseisen.

Het College beveelt aan de oordelen in het kader van het rechtmatigheidstoezicht door de CTIVD juridisch bindend te maken.

3.3 De positie van verschoningsgerechtigden

Ten aanzien van het gebruik van bijzondere bevoegdheden gericht op het achterhalen van de bron van een journalist voorziet het conceptwetvoorstel in voorafgaande toestemming

[27] EHRM 26 maart 1987, no. 9248/81 (*Leander t. Zweden*), § 82; EHRM 6 juni 2006, no. 62332/00 (*Segerstedt-Wiberg e.a. t. Zweden*), § 118-120.
[28] EHRM 26 april 2007, no. 71525/01 (*Dumitru Popescu t. Roemenië*); EHRM 10 februari 2009, no. 25198/02 (*Iordachi e.a. t. Moldavië*); EHRM 28 juni 2007, no. 62540/00 (*Association for European Integration and Human Rights en Ekimdzhiev t. Bulgarije*); EHRM 2 september 2010, no. 35623/05 (*Uzun t. Duitsland*); EHRM 8 maart 2011, no. 12739/05 (*Goranova-Karaeneva t. Bulgarije*); EHRM 27 november 2012, no. 7222/05 (*Savovi t. Bulgarije*); EHRM 15 januari 2015, no. 68955/11 (*Dragojević t. Kroatië*). Ook op andere terreinen heeft het reeds meermaals overwogen dat, gegeven de overlap tussen de procedurele waarborgen onder de artikelen 8 en 13, de waarborgen onder art. 8 moeten worden uitgelegd op een wijze die consistent is met de uitleg onder art 13 (zie o.m. EHRM 28 januari 2014, nos. 14876/12 en 63339/12 (*I.R. en G.T. t. VK*), § 62).

door de rechter. Het College beschouwt het als een gemis dat er naast de uitzondering voor journalisten in het conceptwetsvoorstel geen bijzondere bepalingen zijn opgenomen voor verschoningsgerechtigden zoals artsen en advocaten. Ook in de MvT wordt geen aandacht besteed aan de positie van deze personen met een beroepsgeheim.
Op 1 juli 2015 heeft de Rechtbank Den Haag in kort geding[29] bepaald dat binnen zes maanden voorzien moet worden in een toets door een onafhankelijk orgaan bij het gebruik van bijzondere bevoegdheden bij advocaten, waarbij het onafhankelijk toetsende orgaan de bevoegdheid moet hebben om de uitoefening van die bijzondere bevoegdheden tegen te gaan of te beëindigen. In een brief van 27 juli 2015 aan de Tweede Kamer heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties laten weten dat spoedappel tegen het vonnis is ingesteld.[30] Wel kondigt hij in de brief aan dat het kabinet voornemens is te voorzien in een vorm van onafhankelijke toetsing bij het tappen van advocaten. Het College wijst er op dat het hier gaat om het onderscheppen van communicatiegegevens van beroepsgroepen die te maken hebben met mensen in bijzondere, kwetsbare en afhankelijke situaties. Het gaat om mensen die een advocaat of een arts behoeven. Er zijn in deze situaties naast het recht op privacy een aantal andere mensenrechten in het geding: bij artsen het recht op toegankelijke gezondheidszorg en bij advocaten het recht op een eerlijk proces met daaruit voortvloeiend het recht op een effectieve verdediging en op vertrouwelijke communicatie met advocaten. Gelet op deze bijzondere omstandigheden dienen inbreuken op mensenrechten in deze situaties met extra waarborgen te worden omkleed. De in kort geding door de Haagse rechtbank geformuleerde voorwaarden zijn in de ogen van het College dan ook geheel in lijn met overwegingen zoals die in recente Europese jurisprudentie zijn geformuleerd.[31]

De noodzaak tot het treffen van waarborgen voor de positie van verschoningsgerechtigden versterkt de onder 3.1 reeds geformuleerde aanbeveling van het College om de inzet van communicatie-interceptie door de diensten afhankelijk te maken van toestemming door de rechter of een andere onafhankelijke instantie (zoals voor journalisten wel in het conceptwetsvoorstel is geregeld).

4 Conclusie

Het College is van oordeel dat het conceptwetsvoorstel in de huidige vorm op diverse onderdelen ernstig tekort schiet. In de eerste plaats is de noodzaak van de uitbreiding van de interceptiebevoegdheden van de diensten nog onvoldoende overtuigend aangetoond. Daar komt bij dat de abstracte en technologie-onafhankelijke manier waarop de bijzondere bevoegdheden van de diensten in de concept-wettekst zijn geformuleerd - hoezeer daar op zich iets voor te zeggen valt - vanuit mensenrechtenperspectief tot problemen leidt. Vooral bij de interceptiebevoegdheden heeft die wijze van formuleren namelijk tot consequentie dat de omvang en privacy-impact van die bevoegdheden feitelijk niet te overzien is. De technische mogelijkheden voor gegevensuitwisseling ontwikkelen zich momenteel zo enorm snel, dat de wetgever nu nog niet kan weten welke vormen van gegevensoverdracht op basis van deze wettekst allemaal onderschept zouden kunnen worden. Dat doet vragen rijzen omtrent de voorzienbaarheid van de wettelijke bepalingen en maakt een noodzakelijkheids- en proportionaliteitstoets van de bevoegdheidstoekenning in wezen onmogelijk.

[29] ECLI:NL:RBDHA:2015:7436.
[30] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2015/07/27/kamerbrief-over-afluisteren-van-advocaten-door-inlichtingen-en-veiligheidsdiensten.html.
[31] Zie bijvoorbeeld de overwegingen van het HvJ EU in zaak C-293/12 (*Digital Rights Ireland*) m.b.t. specifieke proportionaliteitswaarborgen waarin bij verschoningsgerechtigden voorzien zou moeten zijn t.a.v. de bewaarplicht van telecomgegevens.

Belangrijk is tevens dat het ontbreken van toestemmingverlening door een rechter of andere onafhankelijke instantie voor de inzet van de bijzondere bevoegdheden door de diensten en het niet-bindende karakter van de rechtmatigheidsoordelen van de CTIVD haaks staan op de recente ontwikkelingen in de Europese jurisprudentie. Nederland loopt hierdoor het grote risico dat het EHRM in een toekomstige procedure tot de conclusie zal komen dat het Nederlandse toezichtstelsel op de diensten niet voldoet aan de EVRM-eisen. De analyse van de relevante jurisprudentie die in de MvT is opgenomen is op dit punt onvolledig en onjuist. Zij houdt geen rekening met de recente internationale en Europese (rechterlijke) oordeelsvorming die onder meer een reactie is op het feit dat in de afgelopen jaren aan het licht is gekomen op welk een massale wijze interceptie van telecommunicatie door inlichtingen- en veiligheidsdiensten heeft plaatsgevonden en hoezeer wettelijke grenzen daarbij zijn genegeerd en konden worden genegeerd vanwege tekortschietend onafhankelijk toezicht. Het valt het kabinet ernstig aan te rekenen dat het bij een voorstel tot het reguleren van bevoegdheden die in het geheim worden uitgeoefend en die diep ingrijpen in de privacy van burgers zo'n benepen houding aan de dag legt waar het gaat om het creëren van onafhankelijke controlemechanismen die een tegenwicht kunnen bieden aan deze 'secret surveillance'. Hiermee wordt geen bijdrage geleverd aan het creëren van publiek vertrouwen in het optreden van de inlichtingen- en veiligheidsdiensten. Integendeel, het reeds aanwezige wantrouwen zal daardoor eerder worden versterkt.