CONCEPT-DAGVAARDING TEGEN DE WIV – MANAGEMENT SUMMARY – 30 maart 2017

Een coalitie van NGO's heeft fundamentele bezwaren tegen het wetsvoorstel voor de Wet op de Inlichtingen- en Veiligheidsdiensten ('Wiv') dat ter behandeling bij de Eerste Kamer voorligt (34588). De Grondwet schrijft voor dat de Wiv buiten toepassing moet blijven wanneer deze wet in strijd is met ieder verbindende verdragen, zoals het EVRM en het Handvest voor de Grondrechten. Tenminste zeven onderdelen van het wetsvoorstel voor de Wiv schenden die verdragen. Als de Wiv ongewijzigd door de Eerste Kamer wordt aangenomen, zal die wet een schending inhouden van het recht op privacy, het recht op vrijheid van meningsuiting en als onderdeel daarvan het recht om vertrouwelijk te communiceren, het recht op een eerlijk proces en het recht op effectieve rechtsbescherming.

De bezwaren tegen het wetsvoorstel zijn eerder uitvoerig ter kennis van het kabinet en de Tweede Kamer gebracht. Ook de Afdeling Advisering van de Raad van State, de Raad voor de Rechtspraak, het College voor de Rechten van de Mens, de Autoriteit Persoonsgegevens, de CTIVD en 29 vooraanstaande wetenschappers hebben forse kritiek geuit op het wetsvoorstel voor de Wiv. Tot nog toe tevergeefs. De fundamentele bezwaren lijken aan dovemansoren gericht. De Nederlandse wetgever lijkt koste wat kost een wettelijke regeling te willen invoeren om Nederland internationaal voorop te laten lopen bij het toekennen van bevoegdheden aan de inlichtingen- en veiligheidsdiensten.

De Wiv schendt fundamentele grondrechten door:

1) de bevoegdheid tot bulkinterceptie;
2) de regeling van bronbescherming;
3) de bevoegdheid tot het hacken van derden;
4) de bevoegdheid om derden te dwingen om aan ontsleuteling mee te werken;
5) de regeling van de notificatieplicht;
6) de regeling over samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten; en
7) de inrichting van het toezicht.

De bezwaren tegen deze onderdelen van het wetsvoorstel zijn verwoord in een concept-dagvaarding, om daarmee aan de Eerste Kamer zo helder en scherp mogelijk te laten zien welke juridische bezwaren er precies bestaan tegen deze onderdelen van het wetsvoorstel. Deze criteria volgen uit de rechtspraak van de hoogste Europese rechters, die de afgelopen jaren streng hebben geoordeeld over wetgeving over inlichtingen- en veiligheidsdiensten. Partijen hopen dat de Eerste Kamer het wetsvoorstel niet ongewijzigd aanneemt en dat het niet nodig zal zijn de Wiv aan de rechter voor te leggen.

Nederlandse Vereniging van Journalisten NVJ
Nederlandse Vereniging van Strafrechtadvocaten NVSA
Stichting Platform Bescherming Burgerrechten
Stichting Privacy First

DAGVAARDING

BODEMPROCEDURE TEGEN DE WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

CONCEPT 30 maart 2017

Heden, de _____ tweeduizendenzeventien, op verzoek van

1. de vereniging Nederlandse vereniging van Journalisten, gevestigd te (1071 DR) Amsterdam, aan de Johannes Vermeerstraat 22, hierna ook te noemen '**NVJ**';

2. de vereniging Nederlandse Vereniging van Strafrechtadvocaten, gevestigd te (5051 RB) Goirle, aan de Kloosterstraat 17-19, hierna ook te noemen '**NVSA**';

3. de stichting Stichting Platform Bescherming Burgerrechten, gevestigd te (1017 XJ) Amsterdam aan de Weteringschans 259, hierna ook te noemen '**Platform Bescherming Burgerrechten**'; en

4. de stichting Stichting Privacy First, gevestigd te (1091 GR) Amsterdam, aan de Wibautstraat 150, hierna ook te noemen '**Privacy First**';

voor deze zaak woonplaats kiezende te (1017 NA) Amsterdam aan de Leidsegracht 9, ten kantore van Boekx Advocaten, van welk kantoor mr. O.M.B.J. Volgenant en mr. F.F. Blokhuis tot advocaten worden gesteld en in deze zaak als zodanig zullen optreden, zulks met het recht van substitutie,

heb ik,

GEDAGVAARD

DE STAAT DER NEDERLANDEN (t.a.v. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Defensie, Ministerie van Algemene Zaken en Ministerie van Veiligheid en Justitie), wier zetel gevestigd is te Den Haag, mijn exploit doende ten parkette van de Procureur-Generaal bij de Hoge Raad der Nederlanden aan de Kazemestraat 52 (2514 CV) te Den Haag, aldaar aan genoemd adres mijn exploit doende door afschrift dezes te laten aan:

OM

op _____ (_____), des ____middags om _____ uur, niet in persoon, doch vertegenwoordigd door een advocaat te verschijnen voor de Rechtbank Den Haag, welke zitting dan zal worden gehouden in één van de zalen van het Gerechtsgebouw in het Paleis van Justitie aan de Prins Clauslaan 60 te (2595 AJ) Den Haag;

MET AANZEGGING DAT:

a. indien gedaagde niet op de voorgeschreven wijze in het geding verschijnt, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechter verstek tegen die gedaagde zal verlenen en de hierna omschreven vordering zal toewijzen, tenzij deze hem onrechtmatig of ongegrond voorkomt;

b. bij verschijning in het geding van gedaagde een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning;

c. de hoogte van de griffierechten is vermeld in de meest recente bijlage behorend bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website www.rechtspraak.nl en op de website van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders: www.kbvg.nl/griffierechtentabel;

d. van een persoon die onvermogend is, een bij of krachtens de Wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:

    a. een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand, dan wel:

    b. een verklaring van het bestuur van de raad voor de rechtsbijstand, bedoeld in artikel 7, derde lid, onderdeel 3 van de Wet op de rechtsbijstand, waaruit blijkt dat zijn inkomen niet meer bedraagt dan de inkomens, bedoeld in de algemene maatregel van bestuur krachtens artikel 35, tweede lid van die wet;

TENEINDE

alsdan namens de in de aanhef genoemde partijen als eisers te horen eis doen op de volgende gronden.

INHOUDSOPGAVE

1. INLEIDING EN ACHTERGROND

1.1 Eisers, hierna verder gezamenlijk te noemen 'Eisers', vorderen dat onderdelen van de Wet op de Inlichtingen- en Veiligheidsdiensten[1] (hierna: 'de Wiv') buiten toepassing worden verklaard.

1.2 De Grondwet bepaalt dat de bepalingen van een formele wet, zoals de Wiv, geen toepassing vinden indien deze toepassing niet verenigbaar is met ieder verbindende bepalingen van verdragen zoals het Europees Verdrag voor de Rechten van de Mens (hierna: 'EVRM'), het EU-Handvest voor de Grondrechten (hierna: 'Handvest') en het Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (hierna: 'IVBPR'). Daarin zijn onder meer het recht op privacy, het recht op vrijheid van meningsuiting en als onderdeel daarvan het recht om vertrouwelijk te communiceren, het recht op een eerlijk proces en het recht op effectieve rechtsbescherming vastgelegd. Bij toetsing van de Wiv aan die grondrechten blijkt dat de volgende onderdelen van de Wiv tot schending van die grondrechten leiden:

1) de bevoegdheid tot bulkinterceptie;
2) de regeling van bronbescherming;
3) de bevoegdheid tot het hacken van derden;
4) de bevoegdheid om derden te dwingen om aan ontsleuteling mee te werken;
5) de regeling van de notificatieplicht;
6) de regeling over samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten; en
7) de inrichting van het toezicht.

1.3 Een concept voor de Wiv is ter consultatie voorgelegd en leverde meer dan 1.000 kritische reacties op.[2] Het concept werd vervolgens niettemin vrijwel ongewijzigd aan de Tweede Kamer voorgelegd.

1.4 Eisers uitten scherpe kritiek op dat wetsvoorstel en stonden daar bepaald niet alleen in.

> Bijvoorbeeld ook de Raad van State, de Raad voor de Rechtspraak, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), de Autoriteit Persoonsgegevens, 29 vooraanstaande wetenschappers en de *OSCE Representative on Freedom of the Media* waren zeer kritisch op het wetsvoorstel. Een overzicht van een aantal van deze kritische reacties, inclusief de online vindplaatsen, is aan het eind van deze concept-dagvaarding opgenomen in bijlage A.

[1] Voluit: *Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..),* Kamerstukken nr. 34 588, online vindbaar op https://www.eerstekamer.nl/wetsvoorstel/34588_wet_op_de_inlichtingen_en

[2] https://www.internetconsultatie.nl/wiv/reacties

1.5 Met deze stortvloed van kritiek heeft de Nederlandse wetgever niets gedaan. De Wiv is op 14 februari 2017 ongewijzigd door de Tweede Kamer aangenomen.

1.6 De Wiv is op [*datum*] aangenomen door de Eerste Kamer. De Wiv treedt in werking op [*datum*].

1.7 De Wiv is onmiskenbaar in strijd is met grondrechten zoals vastgelegd in internationale verdragen en Europese regelgeving. Handhaving van onrechtmatige wetgeving is onrechtmatig. Door de Wiv wordt op massale schaal inbreuk gemaakt op de fundamentele grondrechten van burgers, geheimhouders en NGO's.

1.8 Nu ook de Eerste Kamer de Wiv heeft aangenomen, leggen Eisers de Wiv ter toetsing voor aan de rechter. De rechter heeft de afgelopen jaren regelmatig de wetgever teruggefloten wegens schending van grondrechten, met name ook waar privacy in het geding is. Zowel de Nederlandse rechter als de hoogste Europese rechters hebben de afgelopen jaren niet geaarzeld om té vergaande bevoegdheden bij het verzamelen, delen en bewaren van gegevens van burgers te verbieden. Dit wordt in deze dagvaarding nader uitgewerkt in Hoofdstuk 4. Het belang van nationale veiligheid wordt daarbij door de rechter erkend, maar inbreuken op grondrechten moeten wel noodzakelijk in een democratische samenleving zijn en voldoen aan eisen van kenbaarheid en voorzienaarheid, proportionaliteit en subsidiariteit, en voldoende waarborgen omvatten. Daarbij is voorafgaand onafhankelijk toezicht, bij voorkeur door een rechter, een cruciale factor.

1.9 Met de Wiv is de Nederlandse wetgever doorgeschoten. Met de Wiv loopt Nederland internationaal voorop bij het toekennen van nieuwe bevoegdheden aan inlichtingen- en veiligheidsdiensten. Maar de balans die nodig is bij het inperken van grondrechten is daarbij uit het oog verloren. In deze dagvaarding wordt uitgewerkt op welke onderdelen de Wiv té ver gaat, buiten de grenzen die volgen uit de grondrechten en buiten de grenzen die de hoogste Europese rechters in recente jurisprudentie hebben gesteld.

2. PARTIJEN

2.1 Eisers zijn onder te verdelen in twee groepen:

a. organisaties die zich sterk maken voor privacybelangen en/of mensenrechten; en
b. vertegenwoordigers van groepen die een recht op en plicht tot geheimhouding hebben, zoals advocaten en journalisten.

Beide groepen hebben er via hun eigen invalshoek belang bij dat onderdelen van de Wiv buiten toepassing worden verklaard.

Organisaties die de belangen van mensenrechten behartigen

2.2 De privacy-en burgerrechtenorganisaties ageren tegen de schending van de fundamentele privacy-grondrechten, zoals beschermd in artikelen 7 en 8 Handvest en 8 EVRM.

> **Stichting Platform Bescherming Burgerrechten** heeft ten doel 'de bescherming van het onvervreemdbare bezit van de klassieke burgerrechten, waaronder in het bijzonder begrepen het recht op de persoonlijke levenssfeer (..)' waaronder door middel van 'het voeren en/of steunen van proefprocessen, die met het vorenstaande in de ruimste zin verband houden of daartoe bevorderlijk zijn'. Haar belang strekt hiermee tot onder meer tot het optreden tegen inbreuk op het privéleven van de Nederlandse burgers door middel van (verruimde en verstrekkende) bevoegdheden van de overheid.
>
> **Privacy First** heeft ten doel: 'het behouden en bevorderen van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving, op welke wijze dan ook, onder meer door het in rechte optreden voor alle burgers in Nederland ter bescherming van dit algemene belang en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord.' In casu komt Privacy First op grond van artikel 3:305a BW op voor het algemeen belang bij handhaving van het recht op privacy van iedereen in Nederland die communiceert via telefoon of internet. Daarnaast heeft Privacy First een eigen belang om vertrouwelijk met bronnen te communiceren.

Verschoningsgerechtigden: journalisten en advocaten

2.3 Voor de geheimhouders, zoals advocaten en journalisten, geldt dat zij een verschoningsrecht hebben. Het opslaan en afgeven van de communicatiegegevens schendt dat recht. Het recht op journalistieke bronbescherming brengt met zich mee dat in ieder geval een rechterlijke toetsing plaats moet vinden voordat de overheid informatie opvraagt die kan leiden tot het identificeren van bronnen. De Staat is al driemaal door het EHRM veroordeeld[3] in zaken over journalistiek brongeheim wegens schending van artikelen 8 en 10 EVRM en al een aantal keren op de vingers

3 EHRM, *Voskuil v. Nederland*, 22 november 2007, nr. 64752/01, EHRM, Grote Kamer, *Sanoma v. Nederland*, 14 september 2010, nr. 38224/03: *First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. (…) It is clear, in the Court's view, that the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality.* Zie ooke EHRM, *Telegraaf v. Nederland*, 22 november 2012, nr. 39315/06: *Review post factum (…) cannot restore the confidentiality of journalistic sources once it is destroyed. The Court thus finds that the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. There has therefore been a violation of Articles 8 and 10 of the Convention.*

getikt wegens schending van de vertrouwelijkheid van de communicatie tussen advocaten en hun cliënten.[4]

> De **NVJ** stelt zich onder meer tot doel: 'nationaal en internationaal te waken en waar nodig te strijden voor de persvrijheid en het recht op informatie van de burgers, welke vrijheid en welk recht zij beschouwt als haar wezenlijke grondslagen'. De NJV tracht dat doel te realiseren via alle wettige middelen. Ook de NVJ was eerder ontvankelijk in een vergelijkbare procedure, 'aangezien de persvrijheid en het recht op informatie van burgers onderdeel zijn van het recht op bescherming van de vrijheid van meningsuiting en de NVJ met haar vorderingen op grond van dit grondrecht de bescherming van journalisten wier belangen zij behartigt, beoogt te bewerkstelligen'.[5] Omdat de Wiv de vertrouwelijkheid van communicatie en bronbescherming in gevaar brengt, heeft zij voorts ook een eigen belang om de Wiv middels deze procedure aan te vechten.
>
> De **NVSA** stelt zich onder meer ten doel '(…) al datgene, dat voor een goed functioneren van een verdediging in strafzaken dienstig is en zonodig daartoe in rechte op te treden.' Veel gespecialiseerde strafrechtadvocaten zijn lid van de NVSA. Advocaten kunnen aangeven welke telefoonlijnen onder geheimhoudersnummers vallen, zodat die gesprekken niet getapt kunnen worden door Justitie. Advocaten ontberen die mogelijkheid voor internetgegevens of metadata van telefonie. De bescherming van de vertrouwelijke communicatie tussen advocaat en cliënt is onder de Wiv niet voldoende gewaarborgd. Daarmee heeft de NVSA, naast een collectief belang, ook een eigen belang ex artikel 3:303 BW.

De Staat

2.4 De Nederlands Staat is gedaagde in deze procedure. Bij de Wiv zijn de volgende departementen betrokken: het Ministerie van Binnenlandse Zaken, het ministerie van Defensie, het ministerie van Algemene Zaken en het ministerie van Veiligheid en Justitie. De Wiv geeft bevoegdheden aan de inlichtingen- en veiligheidsdiensten Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). In deze dagvaarding zullen de AIVD en de MIVD gezamenlijk worden aangeduid als 'de diensten'.

3. ACHTERGROND EN FEITEN

De oude Wiv ('Wiv 2002')

3.1 De voorloper van de Wiv was de Wiv 2002. Die wet bood de diensten veel bevoegdheden om informatie te vergaren. Er is nooit aangetoond dat de diensten met de Wiv 2002 niet uit de voeten zouden kunnen. Het belangrijkste argument voor de nieuwe bevoegdheid om de internetkabel middels bulk-interceptie af te tappen is dat 90% van de communicatie via de

[4] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881 (*Afluisteren advocatenkantoor door AIVD*), bekrachtiging van Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436.
[5] Rb. Den Haag 23 juli 2014 ECLI:NL:RBDHA:2014:8966.

internetkabel loopt. Maar de diensten hadden onder de Wiv 2002 reeds de bevoegdheid om alle communicatie af te tappen, in het kader van gerichte onderzoeken. De mogelijkheid voor bulk-interceptie onder de Wiv 2002 betrof uitsluitend de communicatie via de ether. Nut en noodzaak van de uitbreiding met allerlei nieuwe bevoegdheden zijn nooit aangetoond.

De Wiv

3.2 Het concept voor de Wiv dat ter consultatie werd voorgelegd heeft een record aantal reacties opgeleverd. Een overzicht van een aantal van deze kritische reacties, inclusief de online vindplaatsen, is aan het eind van deze concept-dagvaarding opgenomen in bijlage A.

3.3 Er zijn vele amendementen ingediend om het wetsvoorstel van de Wiv te wijzigen zodat deze geen grondrechten zou schenden. Daarvan is er niet één aangenomen.

3.4 In een toelichting van de regering op het ontraden van een motie[6] die beoogde 'te voorkomen dat de nieuwe bevoegdheden met betrekking tot bulkinterceptie leiden tot een situatie waarin onschuldige mensen stelselmatig en op grote schaal afgetapt worden' heeft de regering expliciet erkend dat er onder de Wiv stelselmatig en op grote schaal data zal worden vergaard en geanalyseerd:

> "De bevoegdheid tot onderzoeksopdrachtgerichte interceptie is onderworpen aan een toets aan de criteria van noodzakelijkheid, proportionaliteit en subsidiariteit. Deze begrenzen de praktijk op een wijze die is te toetsen door de TIB. **Daarbij zal wel degelijk stelselmatig en op een zekere (grote) schaal data worden vergaard en geanalyseerd**. Dit op voorhand uit te sluiten miskent de aard van de onderzoeksopdrachtgerichte interceptie."
> (dikgedrukt door advocaat. Toevoeging advocaat: 'TIB' is de afkorting van 'toetsingscommissie inzet bevoegdheden')

3.5 Met de invoering van de Wiv zijn de bevoegdheden voor de diensten ruimer dan in veel andere landen, terwijl de daaraan te koppelen versterking van onafhankelijk toezicht op de diensten ontbreekt.

4. GRONDRECHTEN EN JURISPRUDENTIE EHRM EN HvJEU

Om welke grondrechten gaat het?

4.1 Eisers beroepen zich op bescherming van het privéleven, de bescherming van de persoonlijke levenssfeer en bescherming van persoonsgegevens. De Wiv is in strijd met het recht op

[6] Kamerstuk 34 588, nr. 34 (D66/Verhoeven).

eerbiediging van privéleven en correspondentie zoals neergelegd in artikel 8 EVRM, artikel 7 en 8 Handvest en artikel 17 IVBPR. Eisers beroepen zich op vrijheid van meningsuiting, de communicatievrijheid en als onderdeel daarvan het recht op bronbescherming, zoals vastgelegd in artikel 10 EVRM, artikel 11 Handvest en artikel 19 IVBPR. Het feit dat gegevens van journalisten opgevraagd kunnen worden, brengt het risico met zich mee dat zij bepaalde onderwerpen gaan mijden of dat bronnen zich niet meer tot journalisten durven te wenden. Er is dus gevaar voor een '*chilling effect*'. Eisers beroepen zich op het recht op een '*effective remedy*' en het recht op een eerlijk proces, zoals vastgelegd in artikelen 6 en 13 EVRM, artikel 47 Handvest en artikel 14 IVBPR. Beperkingen van deze grondrechten, zoals opgenomen in de Wiv, moeten de wezenlijke inhoud van die grondrechten eerbiedigen, aldus artikel 52 Handvest. De tekst van deze artikelen luidt als volgt.

> **Artikel 8 EVRM - Recht op eerbiediging van privéleven, familie- en gezinsleven**
> 1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
> 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.
>
> **Artikel 7 Handvest – Eerbiediging van het privé-leven en het familie- en gezinsleven**
> Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.
>
> **Artikel 8 Handvest – Bescherming van persoonsgegevens**
> 1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
> 2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
> 3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.
>
> **Artikel 17 IVBPR**
> 1. Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam.
> 2. Eenieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting.
>
> **Artikel 10 EVRM – Vrijheid van meningsuiting**
> 1. Een ieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Dit artikel belet Staten niet radio-omroep-, en bioscoop- of televisieondernemingen te onderwerpen

aan een systeem van vergunningen.
2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.

Artikel 11 Handvest – Vrijheid van meningsuiting en van informatie
1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen.
2. De vrijheid en de pluriformiteit van de media worden geëerbiedigd.

Artikel 19 IVBPR
1. Eenieder heeft het recht zonder inmenging een mening te koesteren.
2. Eenieder heeft het recht op vrijheid van meningsuiting; dit recht omvat mede de vrijheid inlichtingen en denkbeelden van welke aard ook te garen, te ontvangen en door te geven, ongeacht grenzen, hetzij mondeling, hetzij in geschreven of gedrukte vorm, in de vorm van kunst, of met behulp van andere media naar zijn keuze. 3. Aan de uitoefening van de in het tweede lid van dit artikel bedoelde rechten zijn bijzondere plichten en verantwoordelijkheden verbonden. Deze kan derhalve aan bepaalde beperkingen worden gebonden, doch alleen beperkingen die bij de wet worden voorzien en nodig zijn: a. in het belang van de rechten of de goede naam van anderen; b. in het belang van de nationale veiligheid of ter bescherming van de openbare orde, de volksgezondheid of de goede zeden.

Artikel 6 EVRM – Recht op een eerlijk proces
1. Bij het vaststellen van zijn burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging heeft een ieder recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij de wet is ingesteld. De uitspraak moet in het openbaar worden gewezen maar de toegang tot de rechtszaal kan aan de pers en het publiek worden ontzegd, gedurende de gehele terechtzitting of een deel daarvan, in het belang van de goede zeden, van de openbare orde of nationale veiligheid in een democratische samenleving, wanneer de belangen van minderjarigen of de bescherming van het privé leven van procespartijen dit eisen of, in die mate als door de rechter onder bijzondere omstandigheden strikt noodzakelijk wordt geoordeeld, wanneer de openbaarheid de belangen van een behoorlijke rechtspleging zou schaden. (…)

Artikel 14 IVBPR
1. Allen zijn gelijk voor de rechter en de rechterlijke instanties. Bij het bepalen van de gegrondheid van een tegen hem ingestelde strafvervolging, of het vaststellen van zijn burgerlijke rechten en verplichtingen in een rechtsgeding, heeft eenieder recht op een eerlijke en openbare behandeling door een bevoegde, onafhankelijke en onpartijdige bij de wet ingestelde rechterlijke instantie. (…)

Artikel 13 EVRM – Recht op een daadwerkelijk rechtsmiddel
Een ieder wiens rechten en vrijheden die in dit Verdrag zijn vermeld, zijn geschonden, heeft recht op een daadwerkelijk rechtsmiddel voor een nationale instantie, ook indien deze

schending is begaan door personen in de uitoefening van hun ambtelijke functie.

Artikel 47 Handvest – Recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht
Eenieder wiens door het recht van de Unie gewaarborgde rechten en vrijheden zijn geschonden, heeft recht op een doeltreffende voorziening in rechte, met inachtneming van de in dit artikel gestelde voorwaarden. Eenieder heeft recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat vooraf bij wet is ingesteld. Eenieder heeft de mogelijkheid zich te laten adviseren, verdedigen en vertegenwoordigen. Rechtsbijstand wordt verleend aan diegenen die niet over toereikende financiële middelen beschikken, voorzover die bijstand noodzakelijk is om de daadwerkelijke toegang tot de rechter te waarborgen.

Artikel 52 Handvest – Reikwijdte van de gewaarborgde rechten
1. Beperkingen op de uitoefening van de in dit handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Met inachtneming van het evenredigheidsbeginsel kunnen alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.
2. De door dit handvest erkende rechten waaraan de communautaire verdragen of het Verdrag betreffende de Europese Unie ten grondslag liggen, worden uitgeoefend onder de voorwaarden en binnen de grenzen welke bij die verdragen zijn gesteld.
3. Voorzover dit handvest rechten bevat die corresponderen met rechten die zijn gegarandeerd door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zijn de inhoud en reikwijdte ervan dezelfde als die welke er door genoemd verdrag aan worden toegekend. Deze bepaling verhindert niet dat het recht van de Unie een ruimere bescherming biedt.

4.2 Al deze artikelen werken rechtstreeks door in de Nederlandse rechtsorde en maken onderdeel uit van het Nederlandse recht, op grond van de artikelen 93 en 94 van de Nederlandse Grondwet.

Artikel 93 Grondwet
Bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties, die naar haar inhoud een ieder kunnen verbinden, hebben verbindende kracht nadat zij zijn bekendgemaakt.

Artikel 94 Grondwet
Binnen het Koninkrijk geldende wettelijke voorschriften vinden geen toepassing, indien deze toepassing niet verenigbaar is met een ieder verbindende bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties.

Voorwaarden voor het beperken van grondrechten

4.3 Uit EVRM en Handvest vloeien vier voorwaarden voort waaraan beperkingen op grondrechten, zoals in de Wiv geformuleerd, moeten voldoen:[7] (a) de voorwaarde dat de noodzaak van de voorgestelde bevoegdheden afdoende moet worden onderbouwd, (b) de voorwaarde dat de voorgestelde bevoegdheden afdoende kenbaar en voorzienbaar moeten zijn voor burgers, (c) de voorwaarde dat de inzet van de voorgestelde bevoegdheden met afdoende waarborgen moet zijn omkleed ter bescherming van de rechten van burgers en (d) de voorwaarde dat sprake moet zijn van effectief en onafhankelijk toezicht op de diensten. Deze voorwaarden worden hieronder uitgewerkt.

A. Noodzakelijkheidseis

4.4 Een beperking of inbreuk op een grondrecht is alleen toegestaan indien sprake is van (a) een legitiem doel, (b) een dwingende maatschappelijke noodzaak voor de inbreuk ("*pressing social need*") en (c) de inbreuk proportioneel is aan het na te streven doel. De lidstaten hebben hierbij een eigen beoordelingsruimte ("*margin of appreciation*"), maar het EHRM houdt hierop wel toezicht.

> Ten aanzien van de inlichtingen- en veiligheidsdiensten heeft het EHRM geoordeeld dat inbreuken op de persoonlijke levenssfeer ter bescherming van de nationale veiligheid kunnen gelden als een legitiem doel in een democratische samenleving.[8] Deze inbreuken moeten dan uiteraard daadwerkelijk noodzakelijk zijn ter bescherming van dit legitieme doel. Er zal dan ook steeds een afweging moeten worden gemaakt of activiteiten van de diensten daadwerkelijk noodzakelijk zijn.
>
> De noodzakelijkheidseis ziet niet alleen op de concrete inzet van bevoegdheden van de diensten, maar ook de introductie van nieuwe bevoegdheden moet *an sich* noodzakelijk zijn in een democratische samenleving. Uit de jurisprudentie van het EHRM en het HvJEU volgt dat reeds het enkele bestaan van wetgeving op grond waarvan persoonsgegevens kunnen worden onderschept, geldt als een inbreuk op de bescherming van de persoonlijke levenssfeer.[9]

[7] Zie artikel 52 Handvest, waar een koppeling met het EVRM is gemaakt.
[8] Zie o.a. EHRM 6 september 1978, 5029/71, *Klass e.a. t. Duitsland*, par. 48-50.
[9] EHRM (Grote Kamer) 4 december 2015, 47143/06, *Roman Zakharov t. Rusland*, par. 168-171; EHRM 6 september 1978, 5029/71, *Klass e.a. t. Duitsland*, par. 41. HvJEU (Grote Kamer) 8 april 2014 (C-293/12) ECLI:EU:C:2014:238 (*Digital Rights Ireland*) en HvJEU (Grote Kamer) 21 december 2016, C-698 9 (*Tele2 Sverige/ Post- och telestyrelsen*). Zie tevens: Sarah Eskens, Ot van Daalen en Nico van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Institute for Information Law (IViR, University of Amsterdam), 2015, p. 14.

4.5 De Nederlandse wetgever heeft de noodzaak van de introductie van nieuwe bevoegdheden zoals bulk-interceptie van communicatie via de kabel, het hacken van onschuldige derden en de verplichting mee te werken aan ontsleuteling niet voldoende onderbouwd.[10]

> Bovendien zijn de bestreden onderdelen van de Wiv niet 'noodzakelijk in een democratische samenleving'. Er moet sprake zijn van een '*pressing social need*' en de inbreuk op de privacy moet proportioneel zijn ten opzichte van het te bereiken doel. De Staat heeft op dit punt slechts een beperkte beoordelingsmarge omdat de bescherming van persoonsgegevens van groot belang is voor het recht op bescherming van het privéleven, terwijl de maatregelen een ernstige inbreuk maken op dit recht,[11] zowel wat betreft de opslag van als de toegang tot de gegevens.

4.6 Toegang tot de gegevens en het gebruik van de gegevens door de nationale autoriteiten moet strikt noodzakelijk zijn ten opzichte van het te bereiken doel.[12] Daarbij moeten adequate garanties bestaan tegen onrechtmatig gebruik. Een voorafgaande rechterlijke toets vormt een belangrijke waarborg bij zware inbreuken op het recht op privéleven.[13] De Wiv bevat niet zo'n rechterlijke toets, zodat deze regeling in strijd is met artikel 8 EVRM.

B. Kenbaarheid en voorzienbaarheid

4.7 Uit het EVRM en de jurisprudentie van het EHRM vloeit voort dat inbreuken op de persoonlijke levenssfeer bij wet moeten zijn voorzien. Deze wettelijke basis moet aan bepaalde kwaliteitseisen voldoen.[14] Volgens het EHRM moet te allen tijde worden voorzien in regels die kenbaar en voorzienbaar zijn voor burgers.[15]

4.8 Binnen de context van geheime interceptiebevoegdheden is het volgens het EHRM nodig dat burgers onder meer kennis kunnen nemen van de doelen waarvoor interceptiebevoegdheden

[10] De Autoriteit Persoonsgegevens wijst er in haar kritische advies op dat de wetgever de mogelijke negatieve effecten van de voorgestelde nieuwe bevoegdheden niet in onderlinge samenhang heeft beschouwd, dat de wetgever niet inhoudelijk is ingegaan op onderzoeken waaruit blijkt dat de effectiviteit van grootschalige data-interceptie niet vaststaat en dat evenmin duidelijk is gemaakt welke alternatieven zijn overwogen. De Autoriteit Persoonsgegevens concludeert dat niet is voldaan aan de noodzakelijkheidstoets en dat er dus niet kan worden beoordeeld of er in een democratische samenleving als Nederland plaats is voor de uitbreiding van de bevoegdheden van de diensten, zoals voorgesteld in de Wiv.

[11] Arrest, r.o. 48; EHRM (GK) *S en Marper t. VK*, 4 december 2008, appl.nrs. 30562/04 en 30566/04, par. 102; EHRM *M.K. t. Frankrijk*, 18 april 2013, appl.nr. 19522/09, par. 31.

[12] EHRM *M.K. t. Frankrijk*, 18 april 2013, appl.nr. 19522/09.

[13] EHRM *Huvig t. Frankrijk*, 24 april 1990, 11105/84, par. 33; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 71-72; EHRM *Rotaru t. Roemenië*, 4 mei 2000, appl.nr. 28341/95, par. 59.

[14] EHRM 24 april 1990, 11801/85, *Kruslin t. Frankrijk*, par. 30-36.

[15] EHRM, 2 augustus 1984, 8691/79, *Malone t. Verenigd Koninkrijk*, par. 67.

kunnen worden ingezet, de categorieën van personen jegens wie deze bevoegdheden mogen worden ingezet, de periode waarbinnen deze bevoegdheden mogen worden ingezet en de procedure die moet worden gevolgd voor het onderzoeken, gebruiken en bewaren van onderschepte gegevens.[16] Juist omdat de inlichtingen- en veiligheidsdiensten in de praktijk heimelijk opereren, moet in de wet duidelijk worden aangegeven wanneer bepaalde bevoegdheden mogen worden ingezet tegen burgers.

> De Autoriteit Persoonsgegevens concludeert dat in ieder geval twee nieuwe bevoegdheden die de Wiv biedt niet voldoen aan dit vereiste van kenbaarheid en voorzienbaarheid. De inzet van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie (artikel 48 Wiv) is niet afdoende kenbaar en voorzienbaar voor burgers. Dit komt door de gebruikte terminologie, het gebrek aan uitgewerkte voorbeelden, het driefasenmodel, de onduidelijkheid over de precieze doelen en door de bewaartermijnen van de bulkinterceptie. Ook de reikwijdte van de in artikel 45 Wiv opgenomen bevoegdheid om zowel individuele burgers als bedrijven (providers) te hacken is onvoldoende kenbaar en voorzienbaar, aldus de Autoriteit Persoonsgegevens.

C. Met waarborgen omkleed

4.9 Om te beoordelen of deze inbreuken in overeenstemming met de wet zijn ('*in accordance with the law*' zoals vereist door artikel 8 lid 2 EVRM), is niet alleen het bestaan van toepasselijke wetgeving maar ook de kwaliteit daarvan relevant: de wet moet voldoende waarborgen tegen misbruik en willekeur bevatten en moet voldoende duidelijk en precies zijn om individuen een adequate indicatie te geven van de omstandigheden en voorwaarden waaronder de autoriteiten de maatregelen mogen inzetten.[17] Het resultaat van die beoordeling hangt onder meer af van *'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.'*[18] Het EHRM vereist daarbij gedetailleerde regels: *'the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity'*.[19]

[16] EHRM 29 juni 2006, 54934/00, *Weber en Saravia t. Duitsland*, par. 95.
[17] EHRM *Khan t. VK*, 12 mei 2000, appl.nr. 35394/97, par. 26; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 63; EHRM *Weber en Saravia* (n-o), 29 juni 2006, 54934/00, par. 93; EHRM *Liberty and others t. VK*, 1 juli 2008, appl.nr. 58243/00, par. 62-63.
[18] EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 63; EHRM *Weber en Saravia (n-o)*, 29 juni 2006, 54934/00, par. 106.
[19] EHRM *Weber en Saravia (n-o)*, 29 juni 2006, 54934/00, par. 94; EHRM *Liberty and others t. VK*, 1 juli 2008, appl.nr. 58243/00, par. 62-63.

4.10 Het HvJEU legt de jurisprudentie van het EHRM aldus uit dat er minimumregels moeten bestaan om te zorgen *'dat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens'*, met name wanneer de gegevens automatisch worden verwerkt en het risico dat ze op onrechtmatige wijze worden geraadpleegd aanzienlijk is.[20]

4.11 Onder het EVRM vormt het bestaan van een rechterlijke toets een belangrijke waarborg bij zware inbreuken op het recht op privéleven.[21] Het gebrek aan een dergelijke toets in de Nederlandse wetgeving omtrent toegang tot de gegevens heeft tot gevolg dat die wetgeving niet aan het vereiste '*in accordance with the law*' voldoet.

D. Effectief en onafhankelijk toezicht

4.12 Het EHRM benadrukt steeds het belang van adequaat toezicht op de inzet en uitoefening van de bevoegdheden van inlichtingen- en veiligheidsdiensten, een vereiste dat voortvloeit uit artikel 13 EVRM. Een adequate invulling van het toezicht op de werkzaamheden van de inlichtingendiensten moet compensatie bieden voor het feit dat degenen die onderzocht worden hiervan veelal geen weet zullen hebben. Dit betekent dat betrokkenen vaak zelf geen mogelijkheden hebben om een beroep te doen op de rechter of andere instanties indien zij menen dat er ten onrechte een inbreuk wordt gemaakt op hun rechten. Om die reden is van belang dat een onafhankelijke instantie controleert of de diensten opereren binnen hun bevoegdheden, op grond van de juiste procedures en met inachtneming van eisen van proportionaliteit en subsidiariteit. Dit toezicht dient zich uit te strekken tot de verschillende fasen van het onderzoek, moet onafhankelijk en - zoals artikel 13 EVRM uitdrukkelijk stelt - effectief zijn.

4.13 Voordat de diensten bevoegdheden wensen in te zetten jegens journalisten en advocaten, is een voorafgaande bindende toets door een rechterlijke instantie vereist.

4.14 Effectief toezicht vereist ook dat alle fasen in de werkzaamheden van de diensten afdoende gecontroleerd kunnen worden. Zo moet er niet alleen toezicht zijn op de besluitvorming over de

[20] HvJEU 8 april 2014 (Grote Kamer), gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland en Seitlinger ea*, par. 54.
[21] EHRM *Huvig t. Frankrijk*, 24 april 1990, 11105/84, par. 33; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 71-72.

inzet van met name de bijzondere bevoegdheden (de toestemming), maar ook op de feitelijke uitvoering.

> In het rapport '*Ten standards for oversight and transparency of national intelligence services*' van het Instituut voor Informatierecht (IViR) van de Universiteit van Amsterdam is een grondige analyse opgenomen van de jurisprudentie van het EHRM en het HvJEU over veiligheidsdiensten en de opslag en het gebruik van data van burgers. Eisers verwijzen naar dat rapport[22] (zie ook bijlage A).

Recente rechterlijke uitspraken

Relevante uitspraken Nederlandse rechter

4.15 De Nederlandse rechter heeft een aantal malen geoordeeld over de handelswijze van de AIVD, onder meer bij het toepassen van dwangmiddelen tegen journalisten (nader uitgewerkt in Hoofdstuk 5.II) en bij het afluisteren van advocaten. Daarbij werd geoordeeld dat de toen bestaande wettelijke regeling, de Wiv 2002, op essentiële onderdelen tekortschoot en dat de Nederlandse Staat daardoor in strijd handelde met artikelen 6 en 8 EVRM.[23]

Relevante uitspraken HvJEU

4.16 Het HvJEU, de hoogste rechter van de Europese Unie, heeft de laatste jaren in een bestendige lijn van jurisprudentie invulling gegeven aan bescherming van fundamentele rechten die samenhangen met gebruik van moderne technieken. Het HvJEU heeft onderwerpen als dataretentie en massasurveillance naar zich toe getrokken. En daar heeft het ook alle reden toe. Privacy en gegevensbescherming zijn onderdeel van het Handvest en ingevuld met een stelsel van privacyrichtlijnen[24] en direct vatbaar voor toetsing en uitleg door het HvJEU.

> De bevoegdheid van het HvJEU om te oordelen over massasurveillance en afluisterbevoegdheden blijkt (onder meer) uit Richtlijn 2002/57. Uitgangspunt is het recht op vertrouwelijkheid van communicatie, vastgelegd in artikel 5: *'De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via*

[22] https://www.ivir.nl/publicaties/download/1591.pdf
[23] Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881 (*Afluisteren advocatenkantoor door AIVD*), bekrachtiging van Rb. Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436.
[24] 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie ('Richtlijn 2002/58' of 'e-privacyrichtlijn') en de Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ('Richtlijn 95/46' of 'privacyrichtlijn').

openbare elektronische communicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1.'

Artikel 15 geeft invulling aan de uitzondering die lidstaten mogen toepassen, bijvoorbeeld in het kader van de nationale veiligheid: *'De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale [veiligheid], d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, (...). Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.'*

Recent, op 21 december 2016, heeft de Grote Kamer van het HvJEU het voor de beoordeling van deze kwestie belangrijke *Tele2*-arrest gewezen.[25] Daarin overweegt het HvJEU onder meer: *"De in artikel 5, lid 1, van richtlijn 2002/58 gewaarborgde bescherming van het vertrouwelijke karakter van de communicatie en van de daarmee verband houdende verkeersgegevens, geldt immers voor de door alle andere personen dan de gebruikers getroffen maatregelen, ongeacht of het daarbij gaat om particuliere personen of entiteiten dan wel om overheidsentiteiten. Zoals in overweging 21 van die richtlijn wordt gezegd, beoogt deze richtlijn „elke" onbevoegde „toegang" tot de communicatie, daaronder begrepen de toegang tot de „gegevens over die communicatie", te verhinderen teneinde het vertrouwelijke karakter van de elektronische communicaties te beschermen. (…) Bovendien wordt in artikel 15, lid 1, derde zin, van richtlijn 2002/58 bepaald dat „[a]lle in dit [artikel 15, lid 1,] bedoelde maatregelen in overeenstemming [dienen] te zijn met de algemene beginselen van het [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, [EU]", waaronder de algemene beginselen en de grondrechten die thans worden gewaarborgd door het Handvest.* ***Artikel 15, lid 1, van richtlijn 2002/58 moet aldus tegen de achtergrond van de door het Handvest gewaarborgde grondrechten worden uitgelegd*** *[..]"*[26] (dikgedrukt door advocaat)

4.17 Het HvJEU heeft geoordeeld dat beperkingen die lidstaten mogen aanbrengen op het recht van burgers om vertrouwelijk te communiceren, bijvoorbeeld doordat de diensten in het kader van nationale veiligheid toegang tot communicatie(gegevens) krijgen, tegen de achtergrond van de door het Handvest gewaarborgde grondrechten moeten worden uitgelegd.

4.18 Kortom, de Wiv dient aan het Handvest getoetst te worden.

---

[25] HvJE 21 december 2016 (Grote Kamer), gevoegde zaken (C-203/15) (*Tele2 Sverige AB v. Post- och telestyrelsen)* en (C-698/15) (*Secretary of State for the Home Department v. Tom Watson, Peter Brice en Geoffrey Lewis).*

[26] HvJ EU (Grote Kamer) 21 december 2016, C-698 9 (*Tele2 Sverige/ Post- och telestyrelsen*) resp. par. 77 en 91.

> De beoogde opvolger van de Richtlijn 2002/58, verordening 2017/0003 (COD) (de 'e-privacy verordening'), voorlopig nog in concept, is ook toepasselijk op de bevoegdheden van de veiligheidsdiensten en spreekt in overweging 26 van '*de wettelijk toegestane interceptie (...) die noodzakelijk en evenredig is ter bescherming van de bovengenoemde openbare belangen,* ***in overeenstemming met het Handvest van de grondrechten van de Europese Unie en het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals uitgelegd door het Hof van Justitie en het Europees Hof voor de rechten van de mens'***. (dikgedrukt door advocaat)

4.19 De hierna te noemen vier uitspraken uit 2014, 2015 en 2016 zijn gedaan door de Grote Kamer van het HvJEU, waarmee aan deze uitspraken extra gewicht toekomt.

> In 2014 heeft de Grote Kamer van het HvJEU in de zaak *Digital Rights Ireland* de Dataretentierichtlijn, die bepaalde dat telecomaanbieders moeten worden verplicht om met het oog op de opsporing van zware criminaliteit verkeersgegevens op te slaan, ongeldig verklaard27 omdat deze 'een zeer ruime en bijzonder zware inmenging' inhield van het recht op bescherming van de persoonlijke levenssfeer en de bescherming van persoonsgegevens als bedoeld in artikel 7 en 8 Handvest. Dat oordeel was gebaseerd op het in de richtlijn ontbreken van belangrijke waarborgen, niet alleen met betrekking tot het verzamelen, maar ook met betrekking tot het gebruik (bewaren en raadplegen) van de bewaarde gegevens. In dat verband wees het HvJEU er op dat de richtlijn van toepassing was op alle personen, alle elektronische communicatiemiddelen en alle verkeersgegevens, zonder enige relatie met het doel van de gegevensverzameling en zonder dat er enige aanwijzing bestond dat het gedrag van degenen wier gegevens geregistreerd worden enig verband vertoonde met zware criminaliteit. De opslag van de betreffende verkeers- en locatiegegevens en de toegang die de nationale autoriteiten tot die gegevens hebben vormen beide zelfstandige inbreuken op het recht op bescherming van de persoonlijke levenssfeer. De opslag vormt ook een inbreuk indien slechts een beperkt deel van de opgeslagen informatie daadwerkelijk wordt gebruikt. Retentie van de grote hoeveelheid data over onschuldige personen vormt een zware inbreuk op artikel 8 EVRM en artikel 7 en 8 Handvest. Het HvJEU heeft er in het *Dataretentie*-arrest op gewezen dat uit de betreffende gegevens 'zeer precieze conclusies kunnen worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.' De omstandigheid dat de gegevens worden bewaard en later worden gebruikt zonder dat de betrokkenen worden ingelicht, 'kan bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden', aldus het HvJEU.
>
> In het arrest *Google Spain/Costéja*[28] heeft de Grote Kamer van het HvJEU geoordeeld dat privacyrechten 'in de regel' voorrang hebben op het belang van internetgebruikers op toegang tot informatie.

[27] HvJEU (Grote Kamer) 8 april 2014 (C-293/12) ECLI:EU:C:2014:238 (*Digital Rights Ireland*).
[28] HvJEU 13 mei 2014 (Grote Kamer), ECLI:EU:C:2014:317, C-131/12 (*Google Spain/Costéja*).

> In 2015 heeft het HvJEU in het *Schrems*-arrest[29] (wederom als Grote Kamer) geoordeeld dat een regeling die 'algemeen toestaat dat alle persoonsgegevens van alle personen van wie de gegevens vanuit de Unie naar de Verenigde Staten worden doorgegeven, worden bewaard, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het nagestreefde doel en zonder dat wordt voorzien in een objectief criterium ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan voor specifieke doeleinden, die strikt beperkt zijn en als rechtvaardiging kunnen dienen voor de inmenging als gevolg van zowel de toegang tot als het gebruik van deze gegevens' niet proportioneel is. Het toegang kunnen krijgen tot de inhoud van elektronische communicatie tast de wezenlijke inhoud van het recht op privacy aan. Dat de betrokkene niet de mogelijkheid heeft om inzage, rectificatie of verwijdering van gegevens van persoonsgegevens te eisen is bovendien in strijd met het wezen van het recht op een effectieve voorziening in rechte.
>
> Bij de verzameling van persoonsgegevens moeten de systemen zo worden ingericht dat het aantal verzamelde persoonsgegevens tot het strikt noodzakelijke moet worden beperkt. Met betrekking tot de in *Tele2* voorgelegde bewaarplicht van telecommunicatiegegevens, vergelijkbaar met wat door de Wiv wordt bereikt door het invoeren van een bevoegdheid tot bulk-interceptie, oordeelt het HvJEU dat dit een 'bijzonder ernstige' inbreuk vormt op het privéleven van een persoon. Volgens het HvJEU kan een ongedifferentieerde en algemene bewaring van persoonsgegevens, zelfs met het oog op de bestrijding van (zeer) ernstige criminaliteit, nooit gerechtvaardigd worden.

Relevante uitspraken EHRM

4.20 In het arrest *Zakharov v. Rusland*[30] van 4 december 2015 overwoog de Grote Kamer van het EHRM dat, in de context van interceptie van communicatie, de eis van een wettelijke basis zowel inhoudt dat er een basis moet zijn in het nationale recht als dat de maatregel voldoet aan eisen van rechtsstatelijkheid. Het recht moet derhalve voldoen aan kwaliteitseisen.

> Het EHRM overwoog dat in zaken waarin er een geschil is over wetgeving die geheime aftapmaatregelen toestaat, de wettelijke basis van de inbreuk nauw samenhangt met de vraag of de maatregel noodzakelijk is in de democratische samenleving. Om die reden onderzocht het EHRM tegelijk de eis van de wettelijke basis en de noodzakelijkheidseis. De eis van kwaliteit van het recht impliceert niet alleen dat het nationale recht toegankelijk moet zijn en voorzienbaar in zijn toepassing, maar ook dat de geheime aftapmaatregelen alleen worden toegepast wanneer zij noodzakelijk zijn in de democratische samenleving, in het bijzonder door het bieden van adequate en effectieve waarborgen en garanties tegen misbruik. Het EHRM oordeelde dat het Russische wettelijke systeem inzake interceptie van telefoonverkeer geen adequate en effectieve waarborgen en garanties bood tegen misbruik. In het bijzonder stelde het EHRM tekortkomingen vast op de volgende gebieden: de omstandigheden waarin de publieke autoriteiten bevoegd waren om geheime aftapmaatregelen te nemen, de duur van de geheime aftapmaatregelen, de procedures voor het vernietigen en opslaan van onderschepte data, de procedures voor het autoriseren van de autoriteiten om aftapmaatregelen te nemen, het toezicht op de interceptie en de

[29] HvJEU 6 oktober 2015 (Grote Kamer), ECLI:EU:C:201 5:650, C362/14 (*Maximillian Schrems tegen Data Protection Commissioner*).
[30] EHRM (Grote Kamer) 4 december 2015 nr. 47143/06 (*Zakharov t. Rusland).*

notificatie van de interceptie en de effectiviteit van de beschikbare rechtsmiddelen. Het EHRM concludeerde dat het Russische recht niet voldeed aan de eis van kwaliteit van het recht en niet in staat was om de interceptie van telefoonverkeer te beperken tot wat noodzakelijk was in de democratische samenleving. Gelet hierop oordeelde het EHRM unaniem dat artikel 8 EVRM was geschonden.

4.21 Kort daarna heeft het EHRM deze uitgangspunten bevestigd in het arrest *Szabó en Vissy v. Hongarije* [31] waarin geoordeeld werd dat de Hongaarse tegenhanger van de Nederlandse Wiv een schending van de grondrechten opleverde.

4.22 Bij het EHRM lopen momenteel verschillende zaken waarin nationale wetgeving op het gebied van inlichtingendiensten is voorgelegd, onder meer tegen het Verenigd Koninkrijk en Frankrijk.[32]

Tussenconclusie

4.23 De tussenconclusie is dat de rechter niet schroomt om wetgevers terug te fluiten die hun inlichtingen- en veiligheidsdiensten te ruime bevoegdheden geven in wetgeving die niet voldoet aan de eisen van noodzakelijkheid, kenbaarheid en voorzienbaarheid, voldoende waarborgen en effectief toezicht. De Wiv zal langs die lat worden gelegd. Op zeven onderdelen schiet de Wiv, zoals door de Eerste Kamer aangenomen, tekort.

---

[31] EHRM 12 januari 2016 nr. 37138/14 (*Szabó and Vissy v. Hungary*): *In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse. (…) For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen (…), especially when automated and systemic data collection is technically possible and becomes widespread. In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. (…) Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives.*

[32] *Big Brother Watch v. UK*, nr. 58170/13, gecommuniceerd op 9 januari 2014, *Bureau of Investigative Journalism and Alice Ross v. UK*, nr. 62322/14, gecommuniceerd op 5 januari 2015, en *10 Human Rights Organisations v. UK*, nr. 24960/15, gecommuniceerd op 24 november 2015, gaan over de wetgeving m.b.t. de Britse inlichtingen- en veiligheidsdiensten. Tegen de in mei 2015 aangenomen Franse wet op de inlichtingen- en veiligheidsdiensten lopen al 13 klachten bij het EHRM. En tegen andere nationale wetten die de bevoegdheden van de inlichtingen- en veiligheidsdiensten verruimen zijn rechtszaken in voorbereiden.

5. ONDERDELEN VAN DE WIV DIE BUITEN TOEPASSING MOETEN WORDEN VERKLAARD

5.1 Zolang de Wiv niet is ingetrokken of aangepast worden de privacyrechten van burgers massaal geschonden. Voor geheimhouders zijn er onvoldoende waarborgen dat hun communicatie vertrouwelijk blijft. Door de Wiv niet buiten werking te stellen, handelt de Staat onrechtmatig jegens Eisers (artikel 6:162 BW). De volgende onderdelen van de Wiv zijn in strijd met de door Eisers ingeroepen grondrechten.

I. Bulkinterceptie

5.2 De in artikel 48 lid 1 Wiv omschreven bevoegdheid tot bulkinterceptie legaliseert het op ongekende schaal verwerven, voorbewerken en verder verwerken van communicatiegegevens. Het legitimeert daarmee willekeurige en ongerichte inzet van technologische interceptiebevoegdheden, oftewel massa-surveillance. Uit de toelichting van de regering blijkt ook dat dit de intentie is van dit onderdeel van de Wiv. Deze bevoegdheid voldoet echter niet aan de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving.

> De CTIVD adviseerde om vijf waarborgen in de Wiv op te nemen die ervoor zorgen dat de opslag, analyse en het gebruik van de gegevens die in bulk zijn verzameld zo doelgericht mogelijk plaatsvinden en duidelijkheid geven wanneer welke gegevens vernietigd moeten worden. De CTIVD adviseerde dat:
> *"1. de opslag van gegevens wordt beperkt tot gegevens die gerelateerd zijn aan een onderzoeksopdracht;*
> *2. een doorlopende vernietigingsplicht geldt wanneer bij de verwerking wordt geconstateerd dat opgeslagen gegevens toch niet gerelateerd zijn aan een onderzoeksopdracht;*
> *3. onderscheid wordt gemaakt in de bewaartermijn voor metadata en voor inhoud;*
> *4. selectie doelgerichter plaatsvindt door daaraan de voorwaarde te verbinden dat een selectiecriterium ofwel moet worden gemotiveerd specifiek voor een persoon of organisatie ofwel moet zijn verkregen door search gericht op selectie;*
> *5. geselecteerde gegevens inhoudelijk op relevantie worden beoordeeld en worden vernietigd als zij niet relevant zijn."*
> Geen van deze waarborgen is vervolgens opgenomen in de Wiv.

5.3 Artikel 48 lid 1 Wiv geeft de nieuwe bevoegdheid om 'onderzoeksopdrachtgericht' communicatie en gegevensoverdracht te intercepteren, in bulk, ook van de internetkabel. Hoewel het woord 'onderzoeksopdrachtgericht' suggereert dat de reikwijdte van deze bevoegdheid beperkt zou zijn, maakt deze bevoegdheid massa-surveillance mogelijk. Aanbieders van communicatiediensten zijn op grond van artikel 52 lid 3 en artikel 53 lid 5 Wiv verplicht mee te werken met de diensten om bulkinterceptie mogelijk te maken.

Noodzaak voor bulkinterceptie kabel niet aangetoond

5.4 De noodzaak voor deze nieuwe bevoegdheid is niet aangetoond. In de Memorie van Toelichting is gesteld dat tegenwoordig 90% van de communicatie over de kabel verloopt en dat de diensten geen toegang hebben tot die communicatie. Dat is onjuist. De diensten hadden voor inwerkingtreding van de Wiv al toegang tot kabelgebonden communicatie. Ze konden onder meer *gericht* de kabel aftappen van personen, groepen of organisaties die zij in het vizier hadden, ze konden ook vorderingen tot aanbieders van communicatie richten, geautomatiseerde werken hacken, onderzoek doen op sociale media; dit alles ook als die informatie via de kabel verzonden wordt.

> In de Memorie van Toelichting is gesteld dat de informatiepositie van de diensten risico loopt, maar dit is niet onderbouwd. De diensten hadden ook voor inwerkingtreding van de Wiv tal van bevoegdheden tot hun beschikking om informatie te verzamelen. Nergens blijkt dat die bevoegdheden onvoldoende effectief zijn om de informatiepositie op peil te houden.
>
> Dat het technisch mogelijk is kabelgebonden communicatie te onderscheppen, geeft nog geen noodzaak om dat vervolgens ook daadwerkelijk te doen, aldus ook de CTIVD.[33] '*Uitgangspunt zou moeten zijn dat eerst de noodzaak voor nieuwe bevoegdheden, ingegeven door tekortschietende effecten van de huidige bevoegdheden, overtuigend moet worden aangetoond voordat sprake kan zijn van een wettelijke uitbreiding.*', aldus de CTIVD.

5.5 Of de uitbreiding van de bevoegdheden van de diensten effectief is valt te betwijfelen. Internationaal en nationaal is niet aangetoond dat niet-gerichte interceptiebevoegdheden daadwerkelijk effectief zijn. Het is maar de vraag in hoeverre er doelgericht kan worden gezocht wanneer de hoeveelheid informatie en persoonsgegevens die wordt verzameld steeds groter wordt.

Bulkinterceptie voldoet niet aan eisen proportionaliteit en subsidiariteit

5.6 De regering heeft niet aangetoond dat de bevoegdheid tot het in bulk onderscheppen van communicatie van burgers proportioneel is. Ook de subsidiariteit van deze bevoegdheid is niet aangetoond. De regering heeft niet onderbouwd dat de bestaande bevoegdheden die de diensten hadden onvoldoende effectief waren. De regering heeft geen onderzoek gedaan naar andere bevoegdheden, waarmee met een geringere inbreuk op de grondrechten van burgers een zelfde resultaat kan worden bereikt.

[33] Jaarverslag CTIVD 2014-2015, p. 28.

5.7 In plaats van de data-hooiberg te vergroten en daardoor het zoeken naar de spreekwoordelijke speld te bemoeilijken, zouden de diensten beter meer mankracht en technische middelen kunnen inzetten om heel gericht hun werk te doen. Bijvoorbeeld door alle communicatie van specifieke personen waarvoor concrete aanwijzingen zijn dat zij een gevaar voor de nationale veiligheid vormen af te tappen. Met bulkinterceptie zal – naar de aard van de methode – heel veel data van onschuldige burgers worden vastgelegd. Daaronder zal ook vertrouwelijke communicatie zijn met geheimhouders, zoals communicatie tussen advocaten en hun cliënten. Die communicatie mag vervolgens drie jaar worden bewaard, te rekenen vanaf het moment van ontsleuteling.

5.8 De interceptie van data en de opslag daarvan levert op zichzelf een grote inbreuk op de privacy van burgers. Die inbreuk ontstaat door het opvangen en opslaan van communicatie, los van wat er daarna met de data gebeurt.[34]

Veel te lange bewaartermijn en onvoldoende vernietiging

5.9 Uit de jurisprudentie van het EHRM en het HvJEU volgt dat gegevens die niet relevant zijn voor het doel waarvoor ze zijn verkregen, onmiddellijk moeten worden vernietigd.[35] De Wiv biedt echter de ruimte om grote hoeveelheden data die niet relevant zijn voor het onderzoek waarvoor zij zijn verzameld te bewaren en ook om grote hoeveelheden gegevens die niet op relevantie zijn onderzocht te bewaren. Door het ontbreken van strikte regels omtrent de vernietiging van niet-relevante en niet-onderzochte gegevens, bestaat het risico dat de vernietiging van deze gegevens in de praktijk eerder uitzondering dan regel zal zijn.

> De Autoriteit Persoonsgegevens adviseerde om het principe van "*select while you collect*" expliciet in de wet vast te leggen, om te voldoen aan de eisen van artikel 8 EVRM. Gegevens die niet relevant zijn voor het doel waarvoor zij zijn verzameld, zouden volgens de Autoriteit Persoonsgegevens terstond moeten worden vernietigd, terwijl gegevens waarvan de relatie met de onderzoeksopdracht niet is onderzocht binnen een kortere termijn dan drie jaar zouden moeten worden vernietigd.

[34] Working Party Article 29, *Opinion 04/2014 on electronic communications for intelligence and national security purposes: 'Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles. Limitations to fundamental rights have to be interpreted restrictively, following case law from the European Court of Human Rights (ECtHR)7 and the Court of Justice of the European Union (ECJ)8.'*

[35] EHRM 4 december 2015, 47143/06, *Roman Zakharov t. Rusland*, par. 255.

> Dit principe van "*select while you collect*" werd ook geadviseerd in de Privacy Impact Assessment, en de Raad van State nam dit in haar advies over. De Raad van State acht het niet uitgesloten dat er grote hoeveelheden gegevens die niet op relevantie zijn onderzocht, voor langere tijd opgeslagen blijven en derhalve geen recht wordt gedaan aan dit "*select while you collect*" principe.

5.10 De bewaartermijn van drie jaar van artikel 48 lid 5 Wiv is niet proportioneel en is in strijd met artikel 8 EVRM en artikelen 7 en 8 Handvest. Het HvJEU verklaarde in het *Dataretentie-arrest* de Dataretentierichtlijn ongeldig, onder meer omdat de bewaartermijn van tussen de zes maanden en twee jaar 'een zeer ruime en bijzonder zware inmenging in de fundamentele rechten' was die niet met voldoende waarborgen was omgeven. De bewaartermijn van de Wiv is een stuk langer en evenmin met waarborgen omgeven. In de memorie van toelichting stelt de regering dat een bewaartermijn van drie jaar noodzakelijk is om beter inzicht te verkrijgen in nog onbekende dreigingen, maar - zoals de Raad voor de Rechtspraak terecht heeft opgemerkt[36] - bewaartermijnen kunnen niet worden gebaseerd op het criterium "mogelijk nuttig". De Raad voor de Rechtspraak heeft geoordeeld dat deze bewaartermijn van drie jaar van artikel 48 lid 5 Wiv *'vanuit privacy-oogpunt onwenselijk is'*.

> De Autoriteit Persoonsgegevens heeft erop gewezen dat de Wiv de mogelijkheid schept om gedurende de bewaartermijn van drie jaar de (bulk)gegevens te verstrekken aan buitenlandse diensten, waaronder ook niet-geëvalueerde gegevens, en adviseerde de bewaartermijn ten aanzien van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie te beperken. De Raad van State achtte 'de kans klein dat het EHRM in het kader van artikel 8, tweede lid, EVRM een termijn van drie jaar voor het bewaren van niet onderzochte 'bulkgegevens' aanvaardbaar acht' en adviseerde 'een substantiële verkorting'. Niettemin heeft de wetgever de wettelijke bewaartermijn van artikel 48 lid 5 Wiv op drie jaar bepaald. Die termijn van drie jaar gaat lopen op het moment van verwerving of pas op het moment van ontsleuteling, waardoor een nog veel langere en in theorie onbeperkte bewaartermijn is ontstaan.

<u>Toezicht op bulkinterceptie is onvoldoende</u>

5.11 Artikel 48 lid 2 Wiv bepaalt dat de bevoegdheid tot bulkinterceptie door de betrokken minister kan worden toegestaan. De toestemming wordt verleend voor een periode van ten hoogste een jaar en kan telkens op een daartoe strekkend verzoek worden verlengd voor eenzelfde periode. Er is dus géén voorafgaand onafhankelijk toezicht op bulkinterceptie.

[36] Raad voor de Rechtspraak, "Advies Wet op de inlichtingen- en veiligheidsdiensten 20..", 15 november 2016, p. 6.

Tussenconclusie bulkinterceptie

5.12 De bevoegdheid tot bulkinterceptie van artikel 48 Wiv is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

II. Journalistieke bronbescherming en de rol van NGO's

5.13 De communicatie tussen en bronnen en journalisten of NGO's mag zich helaas vaak in de bijzondere aandacht van de diensten verheugen. Juist in de gevallen dat een bron via een journalist of een NGO een misstand naar buiten wil brengen, heeft die bron er groot belang bij hebben dat die communicatie vertrouwelijk is en dat zijn identiteit niet bekend wordt.

5.14 Journalisten en NGO's moeten kritisch kunnen berichten over misstanden. Zonder bescherming voor bronnen zal informatie over misstanden opdrogen. Uitbreiding van bevoegdheden van inlichtingen- en veiligheidsdiensten om informatie te vergaren zonder dat voorafgaande rechterlijke toetsing heeft plaatsgevonden, staat haaks op het maatschappelijke belang van bronbescherming.

5.15 De praktijk heeft de afgelopen jaren geleerd dat de AIVD een aantal malen aantoonbaar te ver is gegaan met het inzetten van bevoegdheden jegens journalisten. De constatering achteraf dat hiermee de regels rond bronbescherming werden overtreden biedt geen bescherming aan bronnen. Wanneer de identiteit van een bron eenmaal bekend is kan die kennis niet meer ongedaan gemaakt worden. De waarborgen dienen er op gericht te zijn dat er altijd voorafgaande rechterlijke toetsing plaatsvindt vóórdat de inlichtingendiensten informatie verkrijgen waarmee bronnen geïdentificeerd kunnen worden. En wanneer er zonder voorafgaande rechterlijke toestemming niettemin dergelijke informatie is vergaard, dient deze direct vernietigd te worden.

> Het EHRM heeft keer op keer het belang van journalistieke bronbescherming benadrukt en daarbij het principe van een *ex ante* beoordeling door een rechter of onafhankelijke instantie erkend als cruciale procedurele waarborg. Uit de rechtspraak van het EHRM blijkt dat artikel 10 EVRM zich ook uitstrekt tot inlichtingen- en veiligheidsdiensten.[37] Het EHRM heeft de Nederlandse Staat al drie keer veroordeeld wegens schending van artikel 10 EVRM in verband met onvoldoende regeling van de journalistieke bronbescherming.

[37] EHRM 22 november 2012, no. 39315/06, *De Telegraaf / Nederland*, EHRM 25 juni 2014, no. 48135/06, *Youth Initiative for Human Rights v. Servië*, EHRM 8 januari 2013, no. 40238/02, *Bucur en Toma v. Roemenië*, EHRM 4 december 2015, no. 47143/06, *Zakharov t. Rusland.*

> Helaas heeft de AIVD waar het gaat om de bescherming van de speciale positie van journalisten en hun bronnen geen goed *track record*. De AIVD is de afgelopen jaren een aantal keren in de fout gegaan toen zij de bronnen van journalisten die over de AIVD berichtten wilde achterhalen. Toen De Telegraaf in 2006 publiceerde over 'AIVD-geheimen bij de drugsmaffia' ging de AIVD direct de betrokken journalisten afluisteren, volgen en hun telecomgegevens opvragen. Deze kwestie leidde tot een veroordeling van Nederland door het EHRM in 2012. En toen De Telegraaf in 2009 publiceerde hoe de 'AIVD faalde rond Irak' ging de AIVD wederom direct de journalisten afluisteren om hun bron te achterhalen. De CTIVD oordeelde achteraf dat dit niet proportioneel was, maar toen had de AIVD al voldoende informatie vergaard. Deze kwestie is aan het EHRM voorgelegd. In die kwestie vond ook huiszoeking plaats bij een journaliste van De Telegraaf en werden computers van journalisten in beslag genomen. De Nederlandse regering heeft expliciet erkend dat hiermee inbreuk werd gemaakt op artikel 10 EVRM: *"[T]he Government hereby wishes to express – by way of unilateral declaration – its acknowledgement that the requirements of Article 10 of the Convention were violated in respect of the applicants*".[38]

5.16 Onder de Wiv zullen de diensten middels bulk-interceptie op basis van artikel 48 Wiv grote hoeveelheden gegevens verzamelen. Daaronder zullen ook 'gegevens inzake de bron' zijn. De diensten zullen dan toegang hebben tot gegevens over bronnen van journalisten, zónder dat daaraan voorafgaand rechterlijke toetsing ex artikel 30 Wiv heeft plaatsgevonden. Het recht op bronbescherming zal een wassen neus zijn als deze bronbescherming beperkt zou worden tot het vragen van rechterlijke toetsing in een fase dat een overheidsdienst de informatie al lang in huis heeft. Dit is in strijd met de rechtspraak van het EHRM.[39]

> Dunja Mijatović, *Representative on Freedom of the Media* van de *OSCE*, wees Minister Plasterk hier in haar brief van 1 december 2016 op.[40] Het EHRM verwoordt het als volgt: '*Review post factum cannot restore the confidentiality of journalistic sources once it is destroyed.*' De Staat heeft dit erkend.[41] De Wiv geeft niettemin onvoldoende waarborgen om journalistieke bronbescherming te waarborgen en te voorkomen dat de diensten al gegevens hebben verzameld waarmee een bron kenbaar is, zonder dat daar voorafgaandelijke rechterlijke toestemming voor is gegeven.

5.17 In artikel 27 lid 2 Wiv is een specifieke bepaling opgenomen ter zake van gegevens die door de diensten zijn verzameld en betrekking hebben op de vertrouwelijke communicatie tussen een

---

[38] EHRM 22 september 2016, nr. 33847/11, *Telegraaf en Jolande van der Graaf v. Nederland.*
[39] EHRM 22 november 2012, no. 39315/06, *De Telegraaf / Nederland*, eist '*prior review by an independent body with the power to prevent or terminate it. Review post factum (…) cannot restore the confidentiality of journalistic sources once it is destroyed.'*
[40] Brief Dunja Mijatović, 1 december 2016: '*On the other hand, the same draft law foresees the possibility of bulk interception and storage of communication data (…) These safeguards are welcome, but they do not address the question how communication of journalists with their sources would be exempt from this indiscriminate interception.'*
[41] Vzr. Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436, *Advocaten / De Staat*, r.o. 4.9: '*Volgens de Staat kan als een journalistieke bron eenmaal bekend is, dit niet meer ongedaan gemaakt worden.'*

advocaat en diens cliënt. Het gaat hierbij om communicatie die als bijvangst is verkregen. Uitgangspunt daarbij is dat dergelijke gegevens terstond dienen te worden vernietigd. Een vergelijkbare regeling ontbreekt voor communicatie tussen journalisten en bronnen, of communicatie tussen journalisten onderling.

> Dit onderscheid vond ook de CTIVD onjuist.[42] De CTIVD adviseerde artikel 27 lid 2 aan te passen zodat het als volgt komt te luiden: "*Gegevens die betrekking hebben op de vertrouwelijke communicatie tussen een advocaat en diens cliënt* ***dan wel gegevens die betrekking hebben op de identiteit van een bron van een journalist*** *en verkregen zijn door de uitoefening van een bijzondere bevoegdheid als bedoeld in paragraaf 3.2.5 in andere gevallen als bedoeld in artikel 30, tweede of derde lid, worden terstond vernietigd [...].*" (dikgedrukt door advocaat)

> Dunja Mijatović adviseerde Minister Plasterk dit gelijk te trekken.[43] In een ingezonden opinie in *De Volkskrant* van 17 november 2016 werd namens journalisten en hoofdredacteuren op ditzelfde punt gewezen.[44] Dit punt wordt in de samenleving breed gedragen. Vanuit de Tweede Kamer is een amendement voorgesteld, om er voor te zorgen dat de plicht tot vernietiging van gegevens die zijn verzameld zonder rechterlijke toestemming, zoals dat voor advocaten is geregeld in artikel 27 lid 2, ook zou gelden voor gegevens over journalisten en hun bronnen die zonder rechterlijke toestemming zijn verzameld.[45] De Wiv is echter niet aangepast op dit punt.

5.18 De Studiecommissie Journalistieke Bronbescherming heeft een aantal adviezen geformuleerd om het recht op journalistieke bronbescherming in de Wiv te waarborgen, maar geen van deze aanbevelingen is overgenomen in de Wiv.

---

[42] Zienswijze CTIVD op wetsvoorstel Wiv 20.., 7 november 2016, https://www.ctivd.nl/documenten/publicaties/2016/11/09/bijlage-ii

[43] Brief Dunja Mijatović, *Representative on Freedom of the Media* van de OSCE, 1 december 2016: '*The draft WIV law seems to offer a stronger protection to the confidentiality of the communication of lawyers with their clients. Article 27.2 demands that information regarding this communication be destroyed without delay and exceptions will only be possible following a judicial decision. The draft law does not introduce a similar provision on the destruction without delay of the communication between journalists and their sources. I would suggest that explicit safeguards are needed in this respect, bringing the text of the draft Law on the Intelligence and Security Services in line with the draft law on the protection of sources, in order to avoid a negative impact on the freedom of the media. Without these safeguards, whistle blowers and others may refrain from contacting the media with sensitive information. Self-censorship could be an unwelcome consequence of the new legislation, contrary to the public interest. The Netherlands has always been a model country in its respect of fundamental freedoms. The new law may, for that reason, have an impact beyond its borders.*'

[44] *Nieuw wetsvoorstel brengt bronbescherming ernstig in gevaar*, http://www.volkskrant.nl/opinie/nieuw-wetsvoorstel-brengt-bronbescherming-ernstig-in-gevaar~a4416611/

[45] TK 34 588, nr. 10, Amendement van het lid Verhoeven, 21 december 2016.

> De Studiecommissie adviseerde het volgende:
> *Het verdient aanbeveling om het rechterlijk toezicht te beleggen bij een meervoudige kamer van de rechtbank Den Haag, zodat drie rechters gezamenlijk beslissen over het opzij zetten van de journalistieke bronbescherming. Het Wetsvoorstel wijst wel de rechtbank Den Haag aan, maar specificeert niet dat de toetsing door een meervoudige kamer dient te geschieden.*
> *Het delen van gegevens met andere partijen, waaronder buitenlandse inlichtingendiensten, is met onvoldoende waarborgen omgeven. Uit 'ongeëvalueerde gegevens' zullen bronnen van journalisten kunnen worden gedestilleerd. De wet dient voldoende waarborgen te bevatten om te voorkomen dat derden onderzoek kunnen doen waar de diensten zelf niet toe gerechtigd zijn. Die waarborgen ontbreken nu.*
> *Bronbescherming strekt zich in het aanhangige wetsvoorstel tot wijziging van het Wetboek van Strafvordering[46] ook uit tot de 'publicist', maar in het voorliggende Wetsvoorstel is dat niet overgenomen. De Studiecommissie is overtuigd van het nut van de uitbreiding van bronbescherming tot de publicist. De regering licht niet toe waarom de publicist wél recht heeft op bronbescherming waar het gaat om een strafrechtelijk onderzoek, maar níet waar het gaat om onderzoek door de veiligheidsdiensten. Bronbescherming voor de publicist dient ook in het voorliggende Wetsvoorstel te worden opgenomen.*
> *De verplichting om mee te werken aan ontsleuteling van gegevens en aan het onderzoek van geautomatiseerde systemen kan een groot chilling effect hebben wanneer de diensten zich richten op systemen die juist functioneren dankzij het vertrouwen van de gebruiker in de veiligheid en versleuteling. Denk aan het Nederlandse klokkenluidersplatform Publeaks. De Studiecommissie is niet gerustgesteld door de 'terughoudendheid' die in de Memorie van Toelichting wordt toegezegd. Beveiligde journalistieke omgevingen zouden niet gedwongen moeten kunnen worden om mee te werken aan ontsleuteling.*

5.19 Maatschappelijke waakhonden zoals NGO's stellen ook misstanden aan de kaak op basis van informatie van bronnen en klokkenluiders. Regelmatig komen NGO's zelf daarmee in de belangstelling van inlichtingen- en veiligheidsdiensten.[47]

> In de rechtspraak worden NGO's als 'maatschappelijke waakhonden' aangemerkt die op dezelfde rechtsbescherming als journalisten kunnen rekenen.[48] Dunja Mijatović wees hier ook op.[49]

---

[46] TK 34032, Wetsvoorstel Bronbescherming in strafzaken.

[47] Greenpeace werd bijvoorbeeld afgeluisterd in India en Zuid-Korea, en Amnesty International in het Verenigd Koninkrijk.

[48] EHRM 28 november 2013 nr. 39534/07 (*Österreichische Vereinigung zur Erhaltung v. Austria*): *NGO's "may be characterized as social "watchdogs" enjoying similar protection to that afforded to the press"* (par. 34).

[49] Dunja Mijatović, *Representative on Freedom of the Media* van de OSCE, brief van 1 december 2016 aan Minister Plasterk: '*Finally, the draft Law on Intelligence and Security Services refers to 'journalists', in the articles on investigations regarding citizens performing journalistic activities. The use of the term 'journalists' may lead to the application of this protection to a smaller group of media professionals than those targeted by the draft law on the protection of sources, where your Government plans to extend this right to "journalists and publicists." I commend this as it clearly refers to a broader group of writers, editors, bloggers and commentators, taking into account the fast changing media landscape. The draft law on Intelligence and Security Services may benefit from a harmonization of the terms used.'*

5.20 De consequentie van de Wiv is dat bronnen en klokkenluiders die zich met informatie over een misstand tot een journalist of een NGO wenden, er niet op kunnen vertrouwen dat hun identiteit en de inhoud van hun communicatie beschermd is. Deze informatie kan eenvoudig als 'bijvangst' bij de diensten terecht zijn gekomen. Met name wanneer de diensten gebruik maken van de bevoegdheid tot bulk-interceptie is de kans levensgroot dat daar ook dergelijke gegevens bij zitten, zonder dat er vooraf rechterlijke toetsing heeft plaatsgevonden. En wanneer de diensten zonder voorafgaande toestemming van de Rechtbank Den Haag gegevens hebben verkregen inzake de bron van een journalist, hoeven die gegevens op grond van de Wiv niet terstond vernietigd te worden – zoals dat wel het geval is bij onterecht vastgelegde communicatie tussen een advocaat en zijn cliënt (o.g.v. artikel 27 lid 2 Wiv).

Tussenconclusie bronbescherming

5.21 Bronbescherming is onvoldoende gewaarborgd in de Wiv. De regeling van artikel 27 lid 2 Wiv en artikel 30 Wiv in strijd is met de rechten waarop Eisers zich in deze procedure beroepen.

III. De bevoegdheid derden te hacken

5.22 Het hacken van computers en smartphones is een extreem verregaande vorm van surveillance. Computers spelen een grote rol in het privéleven van personen. Via het hacken van een computer kan inzicht worden verkregen in het gehele leven van een individu. Niet alleen communicatie die op dat moment plaatsvindt kan worden onderschept, ook het communicatieverleden wordt inzichtelijk. Bovendien geeft hacken toegang tot zaken, zoals foto's of documenten, die nooit eerder met anderen zijn gedeeld, kan met terugwerkende kracht de locatie worden getraceerd en hacken geeft de mogelijkheid om heimelijk de bezitter van de computer te filmen en geluid op te nemen.

> De VN-rapporteur over vrijheid van meningsuiting verklaarde hierover: *'Vanuit een mensenrechtenperspectief is het gebruik van zulke technologie zeer zorgwekkend.'*[50]

5.23 De diensten beschikten onder de Wiv 2002 al over de bevoegdheid om binnen te dringen in 'geautomatiseerde werken', oftewel een hackbevoegdheid. Artikel 45 Wiv heeft deze bevoegdheid uitgebreid naar het 'hacken van derden'.

[50] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue*, VN Algemene Vergadering, 17 april 2013, A/HRC/23/40, §62.

> Deze derden zullen in de praktijk veelal "technisch gerelateerde" partijen zijn, zoals providers, tussenleveranciers of dienstverleners. In de praktijk kan het hierdoor gaan om bedrijven die beschikken over persoonsgegevens van grote hoeveelheden burgers. Het kan echter ook gebeuren dat de diensten zich toegang zullen verschaffen tot geautomatiseerde werken van individuele burgers, die verder geen doelwit van de diensten zijn, of van NGO's, om zicht te krijgen op de communicatie met bijvoorbeeld bronnen in conflictgebieden of communicatie met klokkenluiders die NGO's informeren over misstanden.

5.24 De diensten mogen *malware* op apparatuur van burgers en organisaties plaatsen om op die manier hun eigenlijke doelwit te bereiken. Wanneer de diensten zich toegang verschaffen tot een geautomatiseerd werk van een derde, kunnen zij bovendien gegevens overnemen (artikel 45 lid 2 sub d Wiv).

5.25 Deze uitbreiding van de hackbevoegdheid leidt tot een grote inbreuk op mensenrechten van derden, zonder dat zij aanleiding hebben gegeven om in het vizier van de inlichtingen- en veiligheidsdiensten terecht te komen. Het is voor derden niet te voorzien dat ze gehackt kunnen worden door de geheime diensten. Bovendien behoeven gegevens van deze derde niet te worden vernietigd als deze relevant zijn voor een ander lopend onderzoek. Daarmee wordt de gehackte computer een zelfstandige bron van informatie zonder dat de daarvoor gestelde waarborgen in acht zijn genomen.

5.26 De diensten zijn niet verplicht om een derde te notificeren dat diens computer gehackt is geweest (artikel 59 Wiv). Dit terwijl er een risico bestaat dat de technische hulpmiddelen, zoals malware, die zijn gebruikt om het hacken mogelijk te maken niet altijd verwijderd kunnen worden (artikel 45, lid 7 Wiv). De gehackte derde partij beschikt dan vervolgens over een onveiligere computer zonder daarvan af te weten en is daarmee kwetsbaarder geworden voor digitale dreigingen.

5.27 Nut en noodzaak van deze nieuwe bevoegdheid is niet aangetoond. Extern voorafgaand toezicht op het uitoefenen van deze bevoegdheid ontbreekt. Toestemming van de minister volstaat. Deze inbreuk op onder andere het recht op privacy van derden is niet noodzakelijk en niet proportioneel.

> De Autoriteit Persoonsgegevens concludeerde dat deze hackbevoegdheid in de praktijk een (toenemend) belangrijke rol kan gaan spelen in de taakuitoefening van de diensten, aangezien het onderscheppen van communicatie door toenemende versleuteling minder effectief kan worden. Voor burgers moet – in overeenstemming met artikel 8 EVRM – afdoende kenbaar en voorzienbaar zijn wanneer en hoe de diensten deze bevoegdheid kunnen inzetten. Ook de Raad van State was zeer kritisch op deze nieuwe bevoegdheid,

zoals vastgelegd in artikel 45 Wiv. Met deze kritiek heeft de regering niets gedaan. De nieuwe hackbevoegdheid is ongewijzigd aangenomen.

Tussenconclusie hacken van derden

5.28 De bevoegdheid om onverdachte en onschuldige derden te hacken, zoals vastgelegd in artikel 45 Wiv, is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

IV. De verplichting mee te werken aan ontsleuteling

5.29 Anoniem en vertrouwelijk communiceren op internet raakt aan de kern van de vrijheid van meningsuiting en privacy.[51] De mogelijkheid gegevens te versleutelen (encryptie) is daar een belangrijke waarborg voor. Dit is van belang voor binnenlandse en buitenlandse activisten, dissidenten en klokkenluiders, maar ook voor anderen die zich (terecht) zorgen maken over het vastleggen van online gedrag omdat die gegevens in de toekomst tegen hun wensen en belangen kunnen opduiken in andere contexten. Versleuteling is vooralsnog de enige manier om digitale communicatie te beschermen tegen inbreuken als cybercriminaliteit, identiteitsdiefstal of onrechtmatige interceptie door overheden.

5.30 De Wiv wet verbiedt encryptie niet, maar stelt wel een medewerkingsplicht in voor ontsleuteling via artikel 57 en artikel 45 lid 9 Wiv. Niet meewerken is een strafbaar feit waarop twee jaar gevangenisstraf staat (artikel 143 Wiv).

5.31 Via deze ontsleutelplicht kunnen de diensten iemand die vermoedelijk kennis heeft van de wijze van versleuteling verplichten mee te werken, door die kennis te delen of de versleuteling ongedaan te maken. NGO's zullen vanwege de aard van hun missie en daaruit volgende werkzaamheden soms contact onderhouden met personen die zich ook in het vizier van de diensten bevinden. Op basis van de Wiv kunnen medewerkers van NGO's verplicht worden mee te werken aan ontsleuteling.

5.32 Voor zover de ontsleutelplicht zich richt tot verdachten, is dit in strijd met het *nemo tenetur*-beginsel.[52] Nu de ontsleutelplicht zich richt tot 'degene van wie redelijkerwijs vermoed wordt

[51] Aldus ook de *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, VN Mensenrechtenraad, in zijn rapport van 22 mei 2015, A/HRC/29/32.
[52] Advies W03.14.0055/II van de Raad van State over wetsvoorstel Computercriminaliteit III, Kamerstukken II 2015/2016, 34 372. Uit dat wetsvoorstel is het decryptiebevel geschrapt, mede naar aanleiding van de kritiek van de Raad van State.

dat hij kennis draagt van de wijze van versleuteling van de desbetreffende gesprekken, telecommunicatie of gegevensoverdracht' is niet uitgesloten dat degene die op straffe van een gevangenisstraf van twee jaar verplicht moet meewerken aan ontsleuteling, hiermee gedwongen wordt mee te werken aan zijn eigen veroordeling. Dat is in strijd met – onder meer – artikel 6 EVRM.

5.33 Ook voor deze nieuwe bevoegdheid geldt dat nut en noodzaak niet zijn aangetoond. Deze inbreuk op de privacy is niet noodzakelijk en niet proportioneel. Extern voorafgaand toezicht op het uitoefenen van deze bevoegdheid ontbreekt. Toestemming van de minister volstaat.

Tussenconclusie ontsleutelplicht

5.34 De bevoegdheid om derden te dwingen om aan ontsleuteling mee te werken, zoals vastgelegd in artikel 45 lid 9 en artikel 57 Wiv, is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

V. De notificatieplicht schiet tekort

5.35 Een van de waarborgen tegen misbruik van bevoegdheden door de diensten is dat degene die onderworpen is aan surveillance genoegdoening kan krijgen. Om misbruik aan de orde te kunnen stellen, moet een individu ervan op de hoogte zijn dat hij of zij het doelwit was van een surveillanceoperatie.

> Het EHRM heeft meerdere malen gesteld dat de notificatieplicht de mogelijkheid waarborgt om de rechtmatigheid van de inzet van bevoegdheden achteraf te betwisten en daarmee beschermt tegen misbruik van bevoegdheden.[53]

5.36 Artikel 59 Wiv regelt een notificatieplicht. Vijf jaar nadat een surveillanceonderzoek beëindigd is moeten de diensten onderzoeken of de betreffende persoon daarover geïnformeerd kan worden. Maar deze plicht geldt slechts voor enkele bijzondere bevoegdheden, namelijk voor het doorbreken van het briefgeheim, het gericht afluisteren van personen of organisaties en in gevallen waarin is binnengetreden in een woning zonder toestemming van de bewoner. Eisers menen dat de notificatieplicht een sterkere waarborg tegen misbruik van bevoegdheden biedt als deze geldt voor de inzet van álle bijzondere bevoegdheden, dus ook voor bijvoorbeeld het binnendringen in geautomatiseerde werken (hacken). Voorts dient in het verslag dat wordt

[53] EHRM 6 september 1978, nr. 5029/71, *Klass e.a./Duitsland*, §39, 56-57, EHRM 28 juni 2007, nr. 62540/00, *Association for European Integration and Human rights en Ekimdzhiev v. Bulgarije*, § 101.

uitgebracht aan de onderzochte persoon te staan op basis van welke juridische grond de bevoegdheid is uitgevoerd, welke gegevens zijn verzameld en op welke rechtsmiddelen de onderzochte persoon een beroep kan doen.

5.37 Volgens artikel 59 Wiv mag de notificatieplicht worden uitgesteld of vervallen als het legitieme doel van een surveillanceoperatie door notificatie in gevaar komt. Eisers vrezen dat de ministers deze uitzondering in de praktijk te ruim zullen interpreteren, waardoor de notificatieplicht een lege huls wordt. In het verleden constateerde de CTIVD dat dit inderdaad het geval was.[54] Zonder nadere waarborgen, die ontbreken, voldoet de vereiste notificatieplicht niet aan de daaraan te stellen eisen.

Tussenconclusie notificatieplicht

5.38 Het recht op notificatie is onvoldoende gewaarborgd in de Wiv. De regeling van artikel 59 Wiv is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

VI. Samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten

5.39 De Wiv biedt de diensten ruime mogelijkheden om eenmaal onderschepte gegevens uit te wisselen met andere partijen. Zo kunnen onder meer niet-geëvalueerde gegevens worden verstrekt aan buitenlandse inlichtingen- en veiligheidsdiensten, waarbij van tevoren niet duidelijk is welke informatie van Nederlandse burgers en organisaties precies wordt verstrekt.

5.40 Artikel 62 Wiv verleent de diensten de bevoegdheid om gegevens te verstrekken aan inlichtingen- en veiligheidsdiensten van andere landen waarmee een samenwerkingsrelatie als bedoeld in artikel 88, eerste lid, wordt onderhouden, alsmede andere daarvoor in aanmerking komende internationale beveiligings-, verbindingsinlichtingen- en inlichtingenorganen.

5.41 Artikel 88 Wiv geeft de criteria die gelden voor het aangaan van een samenwerkingsrelatie met een buitenlandse dienst, waaronder een democratische inbedding van de dienst, eerbiediging van de mensenrechten in het desbetreffende land, de professionaliteit en betrouwbaarheid van de desbetreffende dienst, de wettelijke bevoegdheden en mogelijkheden van de dienst in het desbetreffende land en het door de desbetreffende dienst geboden niveau van gegevensbescherming. Op zo'n samenwerkingsrelatie is geen voorafgaande rechterlijke toetsing

[54] CTIVD, *Toezichtsrapport Inzake de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD*, nr. 24 (2010).

en ook geen rechtmatigheidstoetsing door de Toetsingscommissie Inzet Bevoegdheden (hierna 'TIB'). Toestemming van de minister volstaat. De minister kan dit mandateren aan het hoofd van de dienst (artikel 88 lid 4 Wiv).

5.42 Artikel 64 Wiv verruimt die bevoegdheid zodanig dat die zich ook uitstrekt tot het verstrekken van geëvalueerde of ongeëvalueerde gegevens aan een inlichtingen- of veiligheidsdienst van een ander land waarmee géén samenwerkingsrelatie bestaat als bedoeld in artikel 88, eerste lid. Daarmee is een wettelijke basis gegeven voor het samenwerken met buitenlandse inlichtingen- en veiligheidsdiensten *buiten* een wettelijk kader dat voldoet aan mensenrechtenverplichtingen. Het werk en leven van onder andere individuele activisten, journalisten en oppositieleden kan zodoende door het handelen van de Nederlandse diensten in gevaar komen.

5.43 Artikel 89 Wiv bepaalt dat de toestemming voor het verstrekken van ongeëvalueerde gegevens direct voor meerdere opeenvolgende verstrekkingen van vergelijkbare aard kan worden verleend, voor een periode van maar liefst twaalf maanden, die met nog eens twaalf maanden kan worden verlengd.

> De Raad van State heeft geadviseerd dat de Wiv expliciet zou moeten bepalen dat overdracht aan landen die niet voldoen aan de genoemde criteria alleen in uitzonderlijke gevallen kan plaatsvinden.[55] De regering heeft dat advies niet overgenomen.

5.44 Onder de met buitenlandse diensten uit te wisselen gegevens vallen ook de gegevens afkomstig uit bulkinterceptie, zoals bedoeld in artikel 48 Wiv. Gedurende de bewaarperiode van drie jaar kunnen onderschepte gegevens worden uitgewisseld met buitenlandse diensten. Lang niet alle buitenlandse diensten zijn gebonden aan een maximale bewaartermijn.

> De Autoriteit Persoonsgegevens en de Raad van State hebben er op gewezen dat het verstrekken van gegevens aan buitenlandse diensten – en dan met name niet-geëvalueerde gegevens – in de praktijk bijzondere risico's met zich meebrengt voor individuele burgers en organisaties.[56] Zo kan het gebeuren dat bijzondere persoonsgegevens, zoals gegevens over de seksuele geaardheid of gegevens over politieke of religieuze overtuigingen, worden verstrekt aan autoriteiten in landen waar mensenrechten niet (ten volle) worden gerespecteerd. Dit kan negatieve gevolgen hebben voor Nederlandse burgers wanneer zij

[55] Advies afdeling advisering Raad van State, p. 33.

[56] Reactie Autoriteit Persoonsgegevens op het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20.." , p. 11, en Advies afdeling advisering Raad van State, p. 33, waar o.a. wordt gewezen op het feit dat bewaartermijnen in andere landen sterk kunnen afwijken van de Nederlandse bewaartermijnen. (Kamerstukken II, 2016-2017, 34588 nr. 4).

deze landen bezoeken. Omdat met bulkinterceptie ook gegevens van niet-Nederlanders worden onderschept, kan het verstrekken van gegevens bovendien ingrijpende gevolgen hebben voor burgers die wonen in de landen waaraan deze gegevens worden verstrekt. Deze risico's zijn bij de verstrekking van niet-geëvalueerde gegevens nog groter; op voorhand staat immers niet vast welke informatie besloten ligt in de verstrekte gegevens.

De CTIVD heeft erop gewezen dat door de overgangsbepaling van artikel 166 Wiv een toezichtshiaat ontstaat voor wat betreft het toezicht op de samenwerking met buitenlandse diensten.[57] Gedurende twee jaar na de inwerkingtreding van de Wiv zal toezicht op bestaande samenwerkingsrelaties van de Nederlandse diensten met buitenlandse diensten buiten toepassing blijven. In de woorden van de CTIVD: [Dit] '*levert een groot hiaat op in de rechtsbescherming tegen ongeoorloofde inbreuken op onze grondrechten.*' De CTIVD adviseerde artikel 166 Wiv te schrappen uit het wetsvoorstel. Artikel 166 Wiv is niettemin ongewijzigd aangenomen.

Tussenconclusie samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten

5.45 De samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten is onvoldoende gewaarborgd in de Wiv. De regeling van artikelen 62, 64, 88 en 89 Wiv jo. artikel 166 Wiv is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

VII. Onafhankelijk bindend toezicht op alle fases is onvoldoende gewaarborgd

5.46 Effectief en onafhankelijk toezicht op de diensten is van bijzonder belang. Omdat de diensten heimelijk opereren, hebben burgers doorgaans immers geen kennis van het feit dat hun persoonsgegevens zijn onderschept. Dit betekent dat burgers, wanneer sprake is van een onrechtmatige inbreuk op de persoonlijke levenssfeer, veelal niet zelf aanspraak kunnen maken op een effectief rechtsmiddel tegen deze onrechtmatige inbreuk. Effectief en onafhankelijk toezicht dient in het geval van de diensten dan ook als een belangrijke aanvulling op het recht op een *effective remedy*, zoals neergelegd in artikel 13 EVRM. Wanneer de burger vanwege de heimelijke aard van de operaties van de diensten zelf niet in staat is te controleren of zijn persoonlijke levenssfeer op onrechtmatige wijze wordt aangetast, moet dit gebrek worden gecompenseerd door het bestaan van een effectief en onafhankelijk systeem van toezicht. Effectief en onafhankelijk toezicht is *"an essential component of the protection of individuals with regard to the protection of personal data"*.[58]

[57] Zienswijze van de CTIVD Bijlage I p. 35-36.

[58] Artikel 29 Werkgroep, *Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)*

> Uit de jurisprudentie van het EHRM volgt een dat onafhankelijke (rechterlijke) toets voorafgaand aan het inzetten van bijzondere bevoegdheden sterk de voorkeur heeft.[59] Toch is dat niet in de Wiv opgenomen. Rechterlijke toetsing vooraf is de uitzondering op de regel. Alleen voor het inzetten van bijzondere bevoegdheden jegens journalisten en advocaten is voorafgaande rechterlijke toestemming nodig (artikel 30 lid 2 en 3 Wiv). Ook voor andere verschoningsgerechtigden zou dit moeten gelden.[60]

5.47 Alleen voorafgaande autorisatie door een onafhankelijke instantie is niet genoeg, er moet ook *ex post* rechtmatigheidstoezicht zijn op de uitvoering van de operatie. Door middel van *ex post* toezicht kan immers worden gecontroleerd of de operatie binnen de grenzen van de verleende toestemming is uitgevoerd en of de (uitvoering van de) operatie de grenzen van het EVRM, met name wat betreft de noodzaak, proportionaliteit en subsidiariteit, niet heeft overschreden.[61]

5.48 De artikelen 32 tot en met 37 Wiv regelen de instelling van en toetsing door een nieuwe commissie, de TIB. De TIB oefent bindend voorafgaand toezicht uit op de inzet van bijzondere bevoegdheden.

5.49 De toetsing door de TIB is met minder waarborgen omkleed dan een gang naar de rechter. Die wordt immers voor het leven benoemt én maakt geen onderdeel uit van de uitvoerende macht. De onafhankelijkheid van de rechter wordt doorgaans ook niet betwist. Daarnaast is de rechter het beste in staat om juridische concepten als proportionaliteit, subsidiariteit en noodzakelijkheid te beoordelen en eigenstandig tot een oordeel te komen over het verzoek van de diensten om bepaalde bevoegdheden in te zetten, waarbij toegang mogelijk moet zijn tot alle relevante informatie bij de diensten. De TIB daarentegen toetst enkel de toestemming van de minister. De rechter kan externe deskundigen raadplegen waar nodig. In elk geval zou het beginsel van hoor en wederhoor toegepast moeten worden. Er is geen reden om voorafgaande toetsing door een onafhankelijke rechter te beperken tot uitsluitend die gevallen waarin brieven worden geopend (artikel 44 Wiv), de communicatie tussen advocaten en hun cliënten wordt afgeluisterd (artikel 30, lid 3 Wiv) of om de bronnen van journalisten te achterhalen (artikel 30, lid 2 Wiv).

---

[59] EHRM 6 september 1978, 5029/71, *Klass e.a. t. Duitsland*, par. 56; EHRM 18 mei 2010, 26839/05, *Kennedy t. Verenigd Koninkrijk*, par. 167.

[60] Aldus adviseerde het College voor de Rechten van de Mens, *Advies Conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..,* p. 14.

[61] J.P. Loof e.a., *"Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten"* (Onderzoek in opdracht van het CTIVD, Universiteit Leiden, augustus 2015)

> Er is fundamentele kritiek geuit op het beleggen van het toezicht bij de TIB. De Raad van State[62], de Raad voor de Rechtspraak[63] en de Autoriteit Persoonsgegevens[64] waren unaniem in hun kritiek dat de toetsing van de TIB in de praktijk waarschijnlijk beperkt zal zijn, aangezien de TIB beperkt van omvang is en geen eigen onderzoeksbevoegdheden heeft. Daarmee in samenhang valt te vrezen dat de TIB – gezien haar beperkte omvang en bevoegdheden – niet afdoende kennis en inzicht kan vergaren om een inschatting te kunnen maken van de effectiviteit en effecten van het optreden van de diensten. Het beschikken over deze kennis en inzichten is echter onmisbaar om een weloverwogen oordeel over de noodzaak, proportionaliteit en subsidiariteit van de inzet van bijzondere bevoegdheden te vellen. De Raad van State heeft gewaarschuwd dat moet worden voorkomen dat de toets door de TIB in de praktijk nagenoeg altijd positief zal uitvallen, omdat de TIB enerzijds niet afdoende inzicht heeft in de noodzaak van de inzet van deze bevoegdheden maar anderzijds wel rekening dient te houden met de ingrijpende gevolgen van het weigeren van toestemming. De Raad van State adviseerde de TIB uit de Wiv te schrappen.
>
> De Autoriteit Persoonsgegevens heeft gewaarschuwd dat moet worden voorkomen dat de TIB niet meer dan een "stempelmachine" zal zijn. Deze rechtmatigheidstoets *ex ante* kwalificeert de Autoriteit Persoonsgegevens als 'marginaal', waarbij volgens haar geldt dat de TIB hoogstwaarschijnlijk niet beschikt over afdoende middelen en bevoegdheden om deze toets effectief uit te voeren.

5.50 Naast de TIB oefent de CTIVD toezicht uit op de diensten (artikelen 97 – 124 Wiv). De CTIVD beschikt in dit kader over zelfstandige onderzoeksbevoegdheden en is bevoegd rechtmatigheidsoordelen te geven over het concrete optreden van de diensten. De oordelen van de CTIVD zijn echter niet bindend. De minister kan dit naast zich neerleggen. Dit is problematisch omdat toezicht eigenlijk in de plaats komt van het rechtsmiddel dat iemand die onderworpen is aan surveillance kan inroepen, omdat deze persoon niet afweet van de inbreuk op diens recht op privacy. De CTIVD zou het gebruik van een bevoegdheid onrechtmatig moeten kunnen verklaren én herstelmaatregelen moeten kunnen bevelen, zoals het vernietigen van reeds verzamelde gegevens. De Wiv geeft deze bevoegdheid echter niet aan de CTIVD. Het College voor de Rechten van de Mens adviseerde het rechtmatigheidstoezicht door de CTIVD juridisch bindend te maken.[65]

---

[62] De Raad van State spreekt van "*een zeer marginale en abstracte rechtmatigheidsbeoordeling ex ante*". Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 16.

[63] Raad voor de Rechtspraak, "Advies Wet op de inlichtingen- en veiligheidsdiensten 20..", 15 november 2016, p. 4-5. Over de TIB: *'Het komt de Raad voor dat hiermee op twee punten een effectieve vorm van toezicht onmogelijk wordt gemaakt (…).'*

[64] Reactie Autoriteit Persoonsgegevens op het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20.."

[65] College voor de Rechten van de Mens, Advies Conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..., p. 13.

Volgens de Autoriteit Persoonsgegevens is het ten zeerste de vraag of de Wiv voorziet in een stelsel van toezicht dat – in totaliteit bezien – daadwerkelijk effectief is en alle facetten van de activiteiten van de diensten omvat, zoals bedoeld in artikel 8 EVRM. Eisers zijn van oordeel dat het stelsel van toezicht van de Wiv op cruciale onderdelen tekortschiet.

Het College voor de Rechten van de Mens is snoeihard over de inrichting van toezicht in het wetsvoorstel: '*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.*'
Het College voor de Rechten van de Mens beoordeelt de door de Tweede Kamer aangenomen versie van de Wiv als '*niet voldoende*'.[66]

De CTIVD spreekt naar aanleiding van de reikwijdte van het toezicht door de CTIVD ten opzichte van autorisatie door de TIB van '*een toezichtshiaat*'.[67] Ook de overgangsbepaling van artikel 166 Wiv levert volgens de CTIVD een hiaat in het toezicht op.

Het Instituut voor Informatierecht van de Universiteit van Amsterdam heeft in 2016 een rapport over toezicht op en transparantie rond veiligheids- en inlichtingendiensten gepubliceerd. Het rapport, *Ten standards for oversight and transparency of national intelligence services*, bevat een analyse van jurisprudentie van het Europees Hof voor de Rechten van de Mens en het Hof van Justitie van de Europese Unie over dit onderwerp en benoemt vervolgens tien standaarden waaraan toezicht op de diensten moet voldoen.[68] De auteurs concludeerden dat het concept-wetsvoorstel voor de Wiv niet aan deze standaarden voldeed. Eisers stellen zich op het standpunt dat de Wiv aan ieder van deze standaarden dient te voldoen en dat de huidige Wiv daarin tekortschiet. Ondanks al deze fundamentele kritiek is het stelsel van toezicht zoals voorgesteld door de regering aanvaard door de Tweede Kamer en vervolgens door de Eerste Kamer.

---

[66] Brief van het College voor de Rechten van de Mens van 3 februari 2017 aan de Tweede Kamer: '*Er dient een evenwicht te worden gevonden tussen enerzijds de bevoegdheden van de diensten ten behoeve van de nationale veiligheid en anderszijds de waarborgen die bescherming bieden tegen ongerechtvaardigde inbreuken op mensenrechten. De in de Nota van wijziging opgenomen aanpassingen van het wetsvoorstel zijn nog niet voldoende om deze balans te bereiken.'*
[67] Standpunt CTIVD Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze, februari 2017.
[68] https://www.ivir.nl/publicaties/download/1591.pdf

Tussenconclusie toezicht

5.51 Het stelsel van toezicht in de Wiv voldoet volgens Eisers niet aan de daaraan te stellen eisen, zoals hierboven samengevat. De inrichting van het toezicht op de uitoefening door de diensten van de bevoegdheden die de Wiv hen geeft is in strijd met de rechten waarop Eisers zich in deze procedure beroepen.

Tussenconclusie over de onderdelen van de Wiv die buiten toepassing dienen te worden verklaard

5.52 De Wiv kan niet in stand blijven wegens strijd met de grondrechten. Eisers hebben in deze dagvaarding zeven onderdelen genoemd waarop de Wiv in ieder geval een schending van grondrechten met zich meebrengt. De Wiv is op al die punten in strijd met hogere regelgeving.

> In het *Van Gelder Papier*-arrest heeft de Hoge Raad vastgesteld dat sprake is van onrechtmatig handelen van de Staat wanneer de Staat een met een hogere regeling strijdig en mitsdien onverbindend voorschrift handhaaft. Artikel 94 Grondwet staat de rechter toe de Wiv, als formele wet, te toetsen aan de artikelen 7, 8 en 11 Handvest, artikel 15 e-privacyrichtlijn, aan de artikelen 8 en 10 EVRM en aan de artikelen 14, 17 en 19 IVBPR. Die toetsing leidt tot het oordeel dat de in deze procedure bestreden onderdelen van de Wiv wegens strijd met ieder verbindende verdragsbepalingen buiten toepassing moeten blijven.

5.53 Het onverkort handhaven van de Wiv is onrechtmatig (6:162 BW) jegens alle Eisers en jegens eenieder wier belangen zij vertegenwoordigen, waaronder alle in Nederland internettende burgers, geheimhouders zoals advocaten en journalisten en de achterban waarmee Eisers contact houden, waaronder buitenlandse bronnen, klokkenluiders en politieke tegenstanders van buitenlandse regimes.

6. MOGELIJKE VERWEREN

6.1 Eisers zijn niet bekend met een verweer van de Staat.

6.2 Voor zover de Staat zou betogen dat de rechter niet bevoegd is om onderdelen van een formele wet buiten toepassing te verklaren, wijzen Eisers erop dat uit de jurisprudentie[69] volgt dat de rechter hiertoe bevoegd is als de regelgeving in strijd is met een ieder verbindende verdragsbepalingen.

[69] HR 1 juli 1983, NJ 1984, 360 (*LSV*), HR 16 mei 1986, NJ 1987, 251 (*Landbouwvliegers*) en HR 16 mei 1986, NJ 1987, 252 (*Van Gelder*).

Het komt regelmatig voor dat een wet wegens strijd met grondrechten buiten werking wordt gesteld. In 2012 gebood Uw Rechtbank in kort geding de Staat een wet buiten werking te stellen.[70] Op 28 januari 2014 oordeelde Hof Den Haag dat de Staat een richtlijn niet goed had geïmplementeerd.[71] Op 29 januari 2014 werd een artikel uit de Telecommunicatiewet onverbindend verklaard door Rechtbank Den Haag.[72] In mei 2014 stelde Uw Rechtbank de Wet Verbod Pelshouderij buiten werking wegens strijd met hogere regelgeving.[73] En op 11 maart 2015 stelde Uw Rechtbank in kort geding de Wet Bewaarplicht Telecommunicatie buiten werking.[74]

Voor zover de Staat zou betogen dat Eisers niet ontvankelijk zijn omdat er een andere rechtsgang open zou staan wijzen Eisers op het volgende. Burgers hebben geen mogelijkheid zich te verzetten tegen de Wiv en ook voor de geheimhouders is er geen andere rechtsgang. Op basis van vaste jurisprudentie van de Hoge Raad kan van justitiabelen niet gevergd worden dat zij een wet overtreden om uit te lokken dat zij een strafrechtelijke sanctie krijgen of dat zij bestuursdwang opgelegd te krijgen, waartegen zij vervolgens tegen zouden kunnen ageren.[75]

7. TOELICHTING VORDERINGEN

7.1 De vorderingen nopen tot toetsing door Uw Rechtbank van de Wiv aan een ieder verbindende verdragsbepalingen.[76]

7.2 Uw Rechtbank staat voor de vraag of de Wiv in strijd is met de in deze dagvaarding genoemde grondrechten. Strijd met een ieder verbindende verdragsbepalingen heeft tot gevolg dat de desbetreffende voorschriften buiten toepassing moeten blijven (artikel 94 Grondwet). Bij deze toetsing dient Uw Rechtbank de rechtspraak van internationale gerechten, zoals het EHRM en het HvJEU in acht te nemen. Uw Rechtbank kan op de voet van artikel 94 Grondwet oordelen dat formele wetgeving zoals de Wiv buiten toepassing moet worden gelaten.[77] Deze buiten toepassing verklaring – wegens de onverbindendheid van de Wiv gelet op de strijdigheid met

[70] Rb. Den Haag 3 januari 2012, ECLI:NL:RBSGR:2012:BU9921 (*FNV Kiem- De Staat*), inhoudelijk bekrachtigd door Hof Den Haag 5 juni 2012.
[71] Hof Den Haag 28 januari 2014, ECLI:NL:GHDHA:2014:72, aansprakelijkheid Staat voor niet juist invoeren Richtlijn 2003/88/EG m.b.t. recht op vakantie tijdens ziekte.
[72] Rb. Den Haag 29 januari 2014, ECLI:NL:RBDHA:2014:1004.
[73] Rb. Den Haag 21 mei 2014, JB 2014/164, ECLI:NL:RBDHA:2014:6161.
[74] Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498.
[75] HR 11 oktober 1996 (*Leenders/Ubbergen*), LJN: ZC2169, NJ 1997/165, m.nt. Van der Scheltema, AB 1997/1, m.nt. Van der Drupsteen, JB 1996/241, m.nt. EvdL.
[76] Het toetsingsverbod van artikel 120 Grondwet ziet op de toetsing van wetgeving in formele zin aan de Grondwet. Dat verbod heeft geen betrekking op de toetsing aan ieder verbindende voorschriften als bedoeld in art. 94 Grondwet. Zie HR 18 september 2015, ECLI:NL:HR 2015:2722 (*Vakantiedagen*).
[77] HR 1 juli 1983, NJ 1984, 360 (*LSV*) en HR 16 mei 1986, NJ 1987, 251 (*Landbouwvliegers*).

hogere regelgeving – is dan van kracht totdat is voldaan aan een in een toepassingsverbod op te nemen voorwaarde, zoals aanpassing van de Wiv waardoor de schending van de grondrechten wordt opgeheven.

7.3 Buiten toepassing verklaring houdt een absoluut toepassingsverbod in ten aanzien van alle ambten die behoren tot de veroordeelde overheidsrechtspersoon. In het onderhavige geval hebben de diensten, de AIVD en de MIVD, zich hier dus aan te houden.[78]

7.4 De privacy van burgers moet voldoende gewaarborgd zijn. En de geheimhouders dienen de garantie te krijgen dat de Staat hun rechten respecteert. Eisers vorderen dat die onderdelen van de Wiv buiten toepassing worden gesteld die – naar oordeel van Uw Rechtbank – in strijd zijn met de toepasselijke grondrechten.

7.5 Toepasselijkheid van het Unierecht brengt mee dat de nationale rechter, via artikel 267 WVEU, al in eerste aanleg prejudiciële vragen kan stellen aan het HvJEU over de toetsing van nationale wetten aan het Handvest. Indien Uw Rechtbank derhalve vragen heeft over de wijze waarop het Handvest dient te worden uitgelegd in verband met de Wiv, kan Uw Rechtbank daarover een prejudiciële vraag stellen aan het HvJEU.

7.6 Eisers vertrouwen erop dat de Staat het vonnis van Uw Rechtbank zal opvolgen. Daarom wordt geen dwangsom gevorderd.

8. BEWIJSAANBOD

8.1 Eisers bieden uitdrukkelijk bewijs aan van hun stellingen, voor zover zij krachtens art. 150 Rv daartoe zouden zijn gehouden. Eisers behouden zich het recht voor dit bewijsaanbod in deze procedure te preciseren.

9. ONTVANKELIJKHEID EISERS

9.1 Eisers komen op grond van artikel 3:305a BW op voor een collectief belang, welk belangen zij ieder afzonderlijk volgens hun statuten behartigen. Het merendeel van de eisers was eerder

[78] Zie HR 21 maart 2003, ECLI:NL:HR:2003:AE8462 (*Waterpakt/Staat*) en voor provinciale verordeningen HR 1 oktober 2004, ECLI:NL:HR:2004:AO8913 (*Faunabescherming/ Provincie Fryslan*).

ontvankelijk in een of meer procedures tegen de Staat.[79]

9.2 Aan de eisen van artikel 3:305a BW is voldaan. Eisers hebben getracht door overleg het in deze procedure gevorderde te bereiken. Eisers zijn allen een vereniging of stichting en zij behartigen de belangen die hier in het geding zijn, op basis van toereikende statutaire doelomschrijvingen (3:305a lid 1 BW). Zij ontplooien allen activiteiten op het gebied van bescherming van privacy, bronbescherming of geheimhouding. De belangen zijn gelijksoortig en lenen zich bij uitstek voor bundeling. Zij hebben de betrokken ministers op [*datum*] 2017 verzocht te overleggen. De poging van Eisers om via overleg het in deze procedure gevorderde te bereiken heeft geen resultaat gehad.

9.3 Eisers komen op voor verschillende algemene belangen, met name het belang van het respecteren van grondrechten, het belang van de bescherming van privacy, het belang van bronbescherming en het belang van vertrouwelijke communicatie van verschoningsgerechtigden en geheimhouders. De belangen die Eisers behartigen overstijgen de gebundelde belangen van individuele belanghebbenden. Daarnaast heeft ieder van de Eisers een eigen belang om vertrouwelijk met de eigen achterban te kunnen communiceren en juist ook met (buitenlandse) bronnen, klokkenluiders, slachtoffers van buitenlandse regimes, dissidenten, leden van de oppositie en andere organisaties en personen die in de belangstelling staan van binnenlandse en buitenlandse inlichtingen- en veiligheidsdiensten te communiceren.

10. BEVOEGDHEID

10.1 Uw Rechtbank is bevoegd kennis te nemen van dit geschil op grond van artikel 99 Rv.

MITSDIEN het de Rechtbank te 's-Gravenhage moge behagen bij vonnis, zoveel als mogelijk uitvoerbaar bij voorraad, met veroordeling van de Staat in de kosten van deze procedure, inclusief de nakosten:

[79] Zie Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966 (*Burgers tegen Plasterk*), waarin de NVSA, de NVJ en Privacy First ontvankelijk waren, bekrachtigd door Hof Den Haag 14 maart 2017, ECLI:NL:GHDHA:2017:535, Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498 (*Wet Bewaarplicht Telecommunicatie*), waarin Privacy First, de NVJ en de NVSA ontvankelijk waren en Rb. Den Haag 9 november 2016, ECLI:NL:RBDHA:2016:13313 (*Drones*), waarin de NVJ ontvankelijk was.

I. voor recht te verklaren dat

a. de bevoegdheid tot bulkinterceptie, zoals vastgelegd in artikel 48 Wiv; en/of
b. de regeling van bronbescherming, zoals vastgelegd in artikel 27 lid 2 Wiv en artikel 30 Wiv; en/of
c. de bevoegdheid tot het hacken van derden, zoals vastgelegd in artikel 45 Wiv jl. artikel 59 Wiv; en/of
d. bevoegdheid om derden te dwingen om aan ontsleuteling mee te werken, zoals vastgelegd in artikel 45 lid 9 en artikel 57 Wiv jo. artikel 143 Wiv; en/of
e. de regeling van de notificatieplicht, zoals vastgelegd in artikel 59 Wiv; en/of
f. de regeling over samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, zoals vastgelegd in artikelen 62, 64, 88 en 89 Wiv jo. artikel 166 Wiv; en/of
g. de inrichting van het toezicht op de uitoefening door de diensten van de bevoegdheden die de Wiv hen geeft;

niet voldoen aan de daaraan te stellen eisen op grond van

- de artikelen 7, 8, 11 en 52 van EU-Handvest van de Grondrechten gelezen in samenhang met artikel 15 van de e-privacyrichtlijn; en/of
- de artikelen 6, 8, 10 en 13 van het EVRM; en/of
- de artikelen 14, 17 en 19 van het IVBPR;

en daarbij voor recht te verklaren dat deze bevoegdheden en/of regelingen, of onderdelen daarvan

- niet noodzakelijk zijn in een democratische samenleving; en/of
- niet voldoen aan de eisen van proportionaliteit en subsidiariteit; en/of
- niet voldoen aan het vereiste van kenbaarheid en voorzienbaarheid; en/of
- niet met voldoende waarborgen zijn omkleed; en/of
- niet onderworpen zijn aan voldoende effectief onafhankelijk toezicht;

en daarmee onrechtmatig zijn jegens Eisers; en

II. de Wiv buiten toepassing te verklaren voor wat betreft de hierboven sub I genoemde artikelen of delen daarvan, althans voor wat betreft de onderdelen van de Wiv die Uw Rechtbank in goede justitie in strijd oordeelt met door Eisers ingeroepen bepalingen.

Deze zaak wordt behandeld door Boekx Advocaten
mr. O.M.B.J. Volgenant en mr. F.F. Blokhuis
Leidsegracht 9 (1017 NA) Amsterdam
T: 020 – 528 9532 | F: 020 – 528 9537
E: blokhuis@boekx.com | volgenant@boekx.com
www.boekx.com

BIJLAGE A: OVERZICHT KRITISCHE REACTIES OP WETSVOORSTEL WIV MET ONLINE VINDPLAATSEN

- **Artikel 29 Werkgroep**, 10 april 2014, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes', 819/14/EN WP 215 (*Algemeen advies*).
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

  "From its analysis, the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society."

- **Ten standards for oversight and transparency of national intelligence services**
  https://www.ivir.nl/publicaties/download/1591.pdf
  Sarah Eskens, Ot van Daalen en Nico van Eijk
  Institute for Information Law (IViR, University of Amsterdam), 2015

- **De Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek ("TNO")**, 12 februari 2016, 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX'.
  https://pure.uvt.nl/portal/en/publications/privacy-impact-assessment-wet-op-de-inlichtingen-en-veiligheidsdiensten-20xx(c07127ed-3d00-4664-b737-2e63aaad3b95).html

  "In enkele gevallen argumenteren we dat de wetgever er verstandig aan doet om een voorgestelde bepaling te heroverwegen, omdat de noodzaak ervan niet is aangetoond en onzes inziens ook moeilijk aannemelijk is te maken, ook niet als er zwaardere waarborgen zouden worden voorgesteld."

- **Raad van State,** 21 september 2016, Kamerstukken II 2016/2017, 34 588, nr. 4.
  https://www.raadvanstate.nl/adviezen/advies.html?id=12331

  [De] Afdeling [heeft] ernstige twijfels over de daadwerkelijke effectiviteit van het voorgestelde stelsel van toezicht. Het gaat er niet uitsluitend om dat een toezichtsstelsel formeel - op papier - voldoet aan de criteria die het EHRM stelt, opdat het in 'Straatsburg' EVRM-proof is. Het gaat er vooral om, dat het stelsel van toezicht is toegesneden op de specifieke inrichting van het nationale systeem en daarbinnen, in samenhang bezien, daadwerkelijk effectieve bescherming biedt. Het wetsvoorstel schiet op dit punt tekort. [..] Daarnaast is de Afdeling er met betrekking tot de proportionaliteit van met name de grootschalige gegevensverzameling (Big Data) niet van overtuigd dat het voorstel en de motivering in de memorie van toelichting op alle punten daadwerkelijk voldoen aan de vereisten die voortvloeien uit het EVRM."

- **Raad voor de Rechtspraak,** 15 november 2016, 'Advies Wet op de inlichtingen- en veiligheidsdiensten 20..'
  https://www.rijksoverheid.nl/documenten/brieven/2016/11/15/advies-raad-voor-de-rechtspraak-over-de-wiv-20
  "De Raad is echter enkel formeel gevraagd te adviseren op de werklastgevolgen van het Wetsvoorstel en pas na de advisering door de Afdeling. De Raad benadrukt dat dit een zeer ongebruikelijke gang van zaken is. Hij ziet zich daarom genoodzaakt om door middel van deze brief op eigen initiatief inhoudelijk advies uit te brengen. [..] Bij een dergelijk grote inbreuk op de rechten en vrijheden van burgers zoals in dit Wetsvoorstel beoogd, is een stevige onafhankelijke toezichthouder vereist die op een effectieve wijze zijn taak kan vervullen."

- **Amnesty International,** december 2016, 'Wetsvoorstel van Wet op de inlichtingen- en veiligheidsdiensten 20xx'
  https://www.amnesty.nl/wat-we-doen/themas/veiligheid-en-mensenrechten/nederlands-wetsvoorstel-geeft-geheime-diensten-te-veel-ruimte
  "Amnesty International is zeer bezorgd over de impact van de wet op de samenleving, het recht op eerbiediging van de persoonlijke levenssfeer en andere mensenrechten van individuen en groepen mensen in binnen- en buitenland indien deze wordt vastgesteld zoals nu is voorgesteld."

- **Studiecommissie Journalistieke Bronbescherming,** 9 december 2016, 'Reactie op wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20.. Aanbevelingen Studiecommissie Journalistieke Bronbescherming'
  https://www.villamedia.nl/images/uploads/bronbescherming.pdf
  "De Studiecommissie constateert dat het recht op bronbescherming onvoldoende gewaarborgd is wanneer het Wetsvoorstel ongewijzigd zou worden aangenomen."

- **29 vooraanstaande wetenschappers**
  12 december 2016, 'Position paper t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016'
  https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2016A04612

  "In het wetsvoorstel ontbreken afdoende waarborgen ten aanzien van informatievoorziening over de activiteiten. Daarbij gaat het om de informatieverstrekking door de overheid, de mate waarin informatie door burgers kan worden opgevraagd en de wijze waarop door betrokken organisaties kan worden gerapporteerd over hun betrokkenheid bij de inzet van surveillance. Er is maximale transparantie gewenst in het geheel van voorafgaande toestemming, niet zozeer met betrekking tot concrete gevallen, maar wel waar het informatie zoals het aantal goed- en afgekeurde verzoeken of methodes betreft."

- **Raad voor de Rechtspraak,** 12 december 2016, 'Position paper Raad voor de Rechtspraak t.b.v. t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016'
  https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2016A04612

  "De Raad benadrukt dat een randvoorwaarde voor effectief toezicht door de TIB is dat deze beschikt over voldoende eigenstandige bevoegdheden en informatie. De Raad plaatst echter vraagtekens bij de wijze waarop hierin in het huidig wetsvoorstel is voorzien."

  Autoriteit Persoonsgegevens, 12 december 2016,' Position paper AP t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016'
  https://www.tweedekamer.nl/kamerstukken/detail?id=2016D49115&did=2016D49115

  "De AP baseert haar reactie op het EVRM, dat direct van toepassing is op de inlichtingen- en veiligheidsdiensten. Uit het EVRM vloeien vier voorwaarden voort waaraan het wetsvoorstel moet voldoen. De AP is van mening dat belangrijke onderdelen van het wetsvoorstel nog niet aan deze vier voorwaarden voldoen:
  a. de noodzaak van de voorgestelde bevoegdheden is nog onvoldoende onderbouwd;
  b. de voorgestelde nieuwe bevoegdheden zijn onvoldoende kenbaar en voorzienbaar voor mensen;
  c. de inzet van de voorgestelde nieuwe bevoegdheden is met onvoldoende waarborgen ter bescherming van de rechten van mensen omkleed;
  d. er is nog geen sprake van daadwerkelijk effectief en onafhankelijk toezicht op de diensten."

  "De (nieuwe) bevoegdheden van de diensten zullen onmiskenbaar gevolgen hebben voor Nederlandse burgers, en in het bijzonder voor het recht op bescherming van de persoonlijke levenssfeer. Er bestaat een reële kans dat de introductie van deze bevoegdheden fundamentele vrijheden die ten grondslag liggen aan de Nederlandse rechtsstaat, negatief beïnvloedt."

- **Microsoft**, 14 december 2016, 'Position paper Microsoft t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016'
  https://www.tweedekamer.nl/kamerstukken/detail?id=2016D49050&did=2016D49050

  "Microsoft is tegen grootschalige, ongerichte verzameling van gegevens. Wij vinden dat afluisteren alleen mogelijk mag zijn als die gericht is op specifieke, bekende verdachten. Grootschalige en ongerichte verzameling van gegevens is disproportioneel en schaadt de privacy van gebruikers en het vertrouwen in onze technologie. We maken ons daarbij in het bijzonder zorgen over die elementen van het wetsvoorstel die het mogelijk maken om verzamelde metadata te delen met andere veiligheidsdiensten (Artikel 64), waarvoor bovendien alleen akkoord van de Minister vereist is. Eveneens vinden wij het zorgelijk dat het wetsvoorstel het mogelijk maakt voor de diensten om gegevens te verzamelen wanneer daartoe verzocht door een buitenlandse dienst."

- **Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten ("CTIVD"),** februari 2017, 'Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze'
  https://www.ctivd.nl/documenten/publicaties/2016/11/09/bijlage-ii

  "[..] Dat neemt niet weg dat het wetsvoorstel op belangrijke onderdelen nog steeds geen heldere, toetsbare normen en beperkingen geeft voor de inzet van een aantal bevoegdheden"

SELECTIE UIT DE KRITISCHE REACTIES T.B.V. DE INTERNETCONSULTATIE OVER HET WETSVOORSTEL VOOR DE WIV

- ***Amnesty International** (E. Nazarski)*
  https://www.internetconsultatie.nl/wiv/reactie/991cef42-c446-40de-a663-621a13665007

  "In een democratische rechtsstaat zoals Nederland kan het nooit noodzakelijk zijn om de gehele bevolking onder communicatie-surveillance te plaatsen. Het wetsvoorstel breekt met een wereldwijde trend om meer waarborgen op te nemen in de bevoegdheden van inlichtingen- en veiligheidsdiensten om niet-noodzakelijke en disproportionele inbreuken op mensenrechten te voorkomen of te compenseren. Ook is het maar de vraag of het stelsel van waarborgen zoals voorgesteld in de Wiv 20XX aan mensenrechtenstandaarden voldoet, zoals bijvoorbeeld in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden is vastgelegd."

- ***BCPA** (BT, Colt, Verizon) (N.C. van Veen)*
  https://www.internetconsultatie.nl/wiv/reactie/2bebef40-57b6-4c8b-8497-00b793cc529b

  "De bevoegdheid om verkeer in 'bulk' te onderscheppen is bijzonder ruim omschreven. Hetzelfde geldt voor de corresponderende medewerkingsverplichting. Noch in de wet noch in de Memorie van Toelichting is omschreven wat de medewerkingsplicht voor aanbieders precies behelst. De bevoegdheid wordt op geen enkele wijze begrensd."

- ***Bits of Freedom** (A.G.M. Siedsma)*
  https://www.internetconsultatie.nl/wiv/reactie/ce6aef81-5bc8-480d-adae-5b5abea9689b

  "Het wetsvoorstel beoogt een nieuwe balans te vinden tussen nieuwe bevoegdheden en versterkte waarborgen. Bits of Freedom is van mening dat voor zowel het geheel van de wet als voor een aantal specifieke bevoegdheden die balans wordt gemist."

- ***College voor de Rechten van de Mens** (J.P. Loof)*
  https://www.internetconsultatie.nl/wiv/reactie/368cc884-358d-492a-bc17-91289bf52512

  "Het College is van oordeel dat het conceptwetsvoorstel in de huidige vorm op diverse onderdelen ernstig tekort schiet."

- ***Free Press Unlimited*** *(L. Willems)*
  https://www.internetconsultatie.nl/wiv/reactie/763eb481-eff2-4027-a286-9c9b38e4930a

  "Free Press Unlimited is van mening dat er punten van aandacht zijn [..] die naar onze stellige overtuiging een grote inbreuk maken op kernwaarden van de Nederlandse samenleving"

- ***Google*** *(R. Klimbie)*
  https://www.internetconsultatie.nl/wiv/reactie/0841bb5e-09c8-446a-be7d-ba4273abd5df

  "The measures proposed are extremely intrusive and detrimental to the fundamental rights of civilians and companies worldwide (privacy, confidentiality of correspondence, freedom of expression, freedom of information, freedom to conduct a business, integrity of property). Clear boundaries, procedural safeguards and strong, independent oversight are essential."

- ***Instituut voor Informatierecht*** *(Universiteit van Amsterdam) (Mr O.L. van Daalen)*
  https://www.internetconsultatie.nl/wiv/reactie/211f94f9-2c58-44ff-b462-23c6986f4840

  "[..] Het huidige wetsvoorstel voldoet in ieder geval niet aan een aantal belangrijke [..] standaarden. Deze standaarden zijn niet vrijblijvend: het zijn aanbevelingen gebaseerd op grondrechtelijke verplichtingen."

- ***Internet Society Nederland*** *(B. Goslings)*
  https://www.internetconsultatie.nl/wiv/reactie/e5dbdd08-0364-40ec-ab34-6804432eb3e8

  "De uitgangspositie van het kabinet is in de kern niet onderbouwd en ongemotiveerd."

- ***KPN*** *(P.C. Knol en G.J.C Wabeke)*
  https://www.internetconsultatie.nl/wiv/reactie/847cb5be-31b5-461f-9b4a-4c121271abb9

  "Onvoldoende is gemotiveerd waarom rechterlijke toetsing op de uitoefening van bevoegdheden die inbreuk maken op het communicatiegeheim niet nodig of mogelijk zou zijn"

- ***Microsoft*** *(J.K.A. de Groot)*
  https://www.internetconsultatie.nl/wiv/reactie/697b2577-72f3-482a-ae58-7d960689360e

  "Met een dergelijke wet kan een aanzienlijke hoeveelheid informatie, die door gebruikers via technologiebedrijven wordt opgeslagen of verstuurd, worden ingezien door de Nederlandse inlichtingen- en veiligheidsdiensten, met wantrouwen van die gebruikers in deze bedrijven tot gevolg"

- ***Nederland ICT*** *(L. de Bruijn)*
  https://www.internetconsultatie.nl/wiv/reactie/828d2159-cf3c-4003-83d6-09be63bedf11

  "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*."*

- ***Nederlandse orde van advocaten*** *(N. van Dam)*
  https://www.internetconsultatie.nl/wiv/reactie/e8c49ce8-83f2-45a5-b133-bf987cb08065

  "De minster [staat] met dit wetsvoorstel nog te ver [af] van de realisatie van zijn voornemen te komen tot een wettelijk kader dat in lijn is met grondwettelijke waarborgen en andere belangrijke (rechtsstatelijke) uitgangspunten."

- ***NJCM*** *(M. van Noorloos)*
  https://www.internetconsultatie.nl/wiv/reactie/ee7c913d-d231-4937-b167-c04780cfc90a

  "Het voorstel strekt ertoe de diensten de mogelijkheid te bieden bulk te intercepteren in het kabelbebonden domein [..] door middel van een geautomatiseerd werk met betrekking tot niet specifieke personen, organisaties en nummers [..] 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 [..]. 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."

- ***Privacy International*** *(C. Wilson Palow)*
  https://www.internetconsultatie.nl/wiv/reactie/19fc8742-6f2c-4a03-988a-5992b66a61d8

  "[..] In particular the provisions relating to bulk interception, the lack of judicial authorisation, the breaking of encryption, and the hacking of computers and devices raise serious concerns when considering he law's compliance with internationally-agreed human rights norms."

- ***Radboud Universiteit Nijmegen*** *(M.E. Koning)*
  https://www.internetconsultatie.nl/wiv/reactie/0e73b0d3-71d1-4591-9f50-d0e5b5a25884

  "Without effective and complete oversight safeguards have little meaning. The proposal grants the minister — member of the executive branch of the government — powers to override the judgment of the better-equipped oversight committee on the lawfulness of the interception. When the minister disregards the opinion of the oversight committee the Parliament is asked to decide on the legitimacy of the interception. This needlessly politicises the oversight on human rights infringements. In a democracy under the Rule of Law an independent oversight committee or judge should assess the legitimacy of restricting measure"

- ***Stichting DINL*** *(M.J.A Steltman)*
  https://www.internetconsultatie.nl/wiv/reactie/4c660078-e1b1-4a5b-8ac9-e55f1540e858

  "[..] Het wetsvoorstel laat echter een heel ander verhaal zien. Het voorziet in een zeer omvangrijke uitbreiding van de bevoegdheden van de diensten, die veel verder gaan dan het adresseren van de genoemde rol van technologie. De nieuwe bevoegdheden doen sterk denken aan hetgeen naar buiten kwam tijdens de onthullingen over het afluistergedrag van de NSA. Ook Nederland lijkt ten prooi gevallen aan de ongebreidelde verzamel- en afluisterwoede van de geheime diensten en de

veronderstelling dat die verzameldrift ons veiligheid brengt."

- ***Stichting Privacy First*** *(V.A. Böhre)*
  https://www.internetconsultatie.nl/wiv/reactie/60cd87ec-2b8b-4620-8763-f79aa0635479
  "Het huidige concept-wetsvoorstel komt, in de woorden van het Europees Hof voor de Rechten van de Mens, neer op "destroying democracy on the ground of defending it".

- ***Studiecommissie Journalistieke Bronbescherming*** *(O.M.B.J. Volgenant)*
  https://www.internetconsultatie.nl/wiv/reactie/050ef52a-4dfd-4839-b09e-35ee6398c07e
  "Nederland is de afgelopen jaren al drie keer veroordeeld wegens schending van het grondrecht van artikel 10 EVRM, in 2007 (Voskuil), 2010 (Sanoma) en 2012 (De Telegraaf). Bij brief van 7 december 201215 heeft de Minister van Binnenlandse Zaken de Tweede Kamer toegezegd de Wiv 2002 te wijzigen om journalistieke bronbescherming een wettelijke basis te geven [..] Uit het optreden van de Staat spreekt geen urgentie om consequenties te verbinden aan de drie veroordelingen door het EHRM. Dat is een onwenselijk signaal. De Staat zou veroordelingen door het EHRM serieuzer moeten nemen."

- ***Tele2 Nederland B.****V. (R. van der Berg)*
  https://www.internetconsultatie.nl/wiv/reactie/2b072dce-5a22-4132-b2be-4a6aad59b58f
  "Tele2 zal niet vrijwillig meewerken aan een dergelijk overleg om elke schijn van belangenverstrengeling en onwenselijkheid van de voorgestelde wetgeving te onderstrepen."

- ***T-Mobile Netherlands B.V.*** *(J. van der Linden)*
  https://www.internetconsultatie.nl/wiv/reactie/a451fe55-4ffc-4748-ab7d-2251ca21b869
  "T-Mobile is [..] van mening dat de basis ten aanzien van de onderbouwing, afbakening en motivatie voor dit wetsvoorstel nog onvoldoende is. Het wetsvoorstel en de bijbehorende Memorie van Toelichting roepen vele vragen op. Bij een aantal belangrijke onderdelen zijn er grote juridische en operationele vraagtekens te zetten voor wat betreft de haalbaarheid van het voorstel."

- ***VNO-NCW / MKB-Nederland*** *(N.C.J.M. Mallens)*
  https://www.internetconsultatie.nl/wiv/reactie/0bfede7e-a32a-474f-a545-bf8c422f379a
  "De in dit wetsvoorstel voorziene uitbreiding van de bijzondere bevoegdheid van de diensten om `in bulk' het kabelgebonden verkeer af te tappen is verregaand. De enkele constatering dat tegenwoordig verreweg het grootste deel van de communicatie via kabelnetwerken verloopt, vormt naar onze mening hiervoor onvoldoende rechtvaardiging. De huidige, gerichte internettap biedt ons inziens voldoende mogelijkheden voor de diensten om hun taken te kunnen uitvoeren. Wij vragen de minister dan ook om een onderbouwing van nut, noodzaak én effectiviteit van deze vergaande aanpassingen"

- ***Vodafone Nederland*** *(M.A. Prinsen Geerligs*)
  https://www.internetconsultatie.nl/wiv/reactie/a8781d87-8f38-4b6c-86fd-de68277e78b2
  "Doordat bevoegdheden en medewerkingsplichten met de concept WIV20xx vrijwel onbeperkt worden uitgebreid, zonder daarbij transparantie en toezicht te versterken, beweegt Nederland precies in omgekeerde richting van bijvoorbeeld de Verenigde Staten."