Enkele kanttekeningen bij de Wiv 2017

De uitbreiding van bevoegdheden getoetst aan mensenrechten

Nico van Eijk en Quirine Eijkman*

Europese landen worstelen met het 'post Snowden'-tijdperk. Dit is zichtbaar in de nieuwe wetgeving die in veel landen recentelijk tot stand is gekomen. Grote thema's daarbij zijn onder meer hoe om te gaan met de hedendaagse informatiesamenleving, die oneindige hoeveelheden data produceert en die zich kenmerkt door snelle technologische ontwikkelingen. Hoe kan worden voorkomen dat zich een tweede 'Snowden'-onthulling gaat voordoen? Ook de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2017 is opnieuw een product van zijn tijd. Deze wet probeert de nieuwe dilemma's te ondervangen terwijl tegelijkertijd een werkbare situatie voor de bescherming van de rechtstaat via inlichtingen en veiligheidsdiensten wordt nagestreefd.

Wij presenteren in dit artikel een aantal kanttekeningen bij de Wiv 2017. Dit doen wij door een aantal relevante in Nederland (Eskens e.a. 2016; Loof e.a. 2016) en in de Europese Unie[1] verschenen overkoepelende studies over grondrechten te bespreken. Deze kanttekeningen zijn deels gebaseerd op normatieve uitgangspunten en aanbevelingen uit deze studies, deels ontleend aan nog lopend onderzoek. Gezien de aard en omvang van dit artikel is een selectie gemaakt en beperkt de analyse zich tot het schetsen van de belangrijkste dilemma's.

* Prof. dr. N.A.N.M. van Eijk is hoogleraar informatierecht verbonden aan het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam), www.ivir.nl/employee/eijk. Mr. dr. Quirine Eijkman is ondervoorzitter van het College voor de Rechten van de Mens en lector Toegang tot het Recht bij de Hogeschool Utrecht. Deze bijdrage is op persoonlijke titel geschreven.

1 Het Bureau voor de Grondrechten van de Europese Unie (Fundamental Rights Agency, FRA) publiceerde een tweede rapport met een inventarisatie van de laatste ontwikkelingen in Europe vergezeld van een lijst met aanbevelingen (FRA 2017). Dit is het vervolg op FRA 2015.

doi: 10.5553/JV/016758502018044001007

Achtergrond nieuwe regelgeving

De regelgeving op het gebied van de bevoegdheden van de inlichtingen- en veiligheidsdiensten zoals neergelegd in de nog geldende wetgeving dateert van 2002 en is een product van haar tijd. Dat deze wet in 2002 tot stand is gekomen, is niet zonder betekenis. De aanslag op de Twin Towers ('9/11') vond plaats in 2001. En de aanslagen in London en Madrid in 2004/2005 resulteerden in Europese regulering die telecomaanbieders verplichtte om grootschalig informatie te verzamelen over gebruikers: de Dataretentierichtlijn van 2006.[2] Alles bij elkaar genomen werd een zeer ruim raamwerk gecreëerd om digitale informatie te verzamelen. De Snowden-onthullingen in 2013, maar ook 'lekken' via andere bronnen, zoals Wikileaks, maakten zichtbaar wat inmiddels de gangbare praktijk was geworden. De bevoegdheden van inlichtingen- en veiligheidsdiensten om inlichtingen, te verzamelen bleken niet alleen zeer ruim te zijn, maar ook - dankzij nieuwe technologische ontwikkelingen - ongekende mogelijkheden te bieden tot 'massa surveillance' (Hobokoen e.a. 2012). Bovendien bleek dat verschillende diensten, zoals de Amerikaanse *National Security Agency* (NSA), niet alleen de grenzen van de regulering hadden verkend maar deze in voorkomende gevallen hadden overschreden. Het gaat dan vooral om de Amerikaanse diensten, over Europese diensten is met uitzondering van het Britse *Government Communications Headquarters* (GCSQ) relatief weinig bekend.
Buiten de maatschappelijke discussie die ontstond door de onthullingen – wie heeft niet de Oscar-winnende documentaire over Snowden, '*Citizenfour*', gezien – oordeelde ook de rechterlijke macht over de nieuwe reguleringskaders en de toepassing van digitale bevoegdheden door inlichtingendiensten. De bevindingen van de rechters waren ontluisterend. Het Europese Hof van Justitie, dat pas sinds 2009 kan toetsen aan het Handvest van de Grondrechten van de Europese Unie, haalde vernietigend uit en verklaarde in 2014 de Dataretentierichtlijn ongeldig.[3] Het is uitzonderlijk dat een richtlijn buiten werking wordt gesteld. Vervolgens is in de 'Schrems'-zaak hetzelfde gebeurd met de beschikking van de Europese Commissie over de uitwisseling van persoonsgegevens met de Verenigde Staten.[4] Daarin waren onvoldoende

2 Richtlijn 2006/24/EG d.d. 15 maart 2006.
3 ECLI:EU:C:2014:238.
4 ECLI:EU:C:2015:650.

doi: 10.5553/JV/016758502018044001007

waarborgen ingebouwd voor wat betreft het gebruik van de gegevens door inlichtingendiensten. In Straatsburg volgde het Hof voor de Rechten van de Mens in 2015 met de Zakharov-zaak.[5] Het Hof scherpt in deze uitspraak zijn eerdere jurisprudentie aan en geeft duidelijke grenzen voor (geheime) digitale surveillance. Overigens was Nederland al eerder door het Hof veroordeeld vanwege het ongeoorloofd aftappen van journalisten door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), die van de minister van Binnenlandse Zaken en Koninkrijksrelaties de opdracht had gekregen om een bron te achterhalen.[6] In Nederland is eveneens de nationale implementatie van de Dataretentierichtlijn buiten werking gesteld en zijn nieuwe grenzen gesteld aan het toezicht via een zaak over het afluisteren van advocaten.[7] Deze laatste zaak heeft geresulteerd in een tijdelijke noodmaatregel, waarbij een onafhankelijke toetsingscommissie is ingesteld die voorafgaand toestemming moet geven voor het inzetten van bevoegdheden jegens advocaten en journalisten.[8] Al deze jurisprudentie geeft in de eerste plaats het falen van de wetgever aan. Het Europese parlement, de Europese Raad, de Europese Commissie, de Nederlandse regering, de Tweede Kamer en de Eerste Kamer blijken te hebben ingestemd met regelgeving die in strijd is met de geldende fundamentele rechtenkaders.

Nieuwe bevoegdheden en technologieneutraliteit

Over het algemeen hebben inlichtingen- en veiligheidsdiensten al ruimere bevoegdheden dan gewone rechtshandhavers om informatie te verzamelen. Zo hoeft niet te worden voldaan aan dezelfde procedurele waarborgen als neergelegd in het Wetboek van Strafvordering en hebben de diensten de mogelijkheden tot het massaal verzamelen van communicatiedata. Bij reguliere rechtshandhaving is er meestal slechts de mogelijkheid om zeer gericht informatie te verzamelen, bijvoorbeeld alleen van een verdachte of personen uit zijn directe omge-

5 *Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015. In de slipstream ervan o.a.: *Szabó and Vssey v. Hungary* (Application nr. 37138/14), 12 januari 2016.
6 Telegraaf Media Nederland, Landelijke media b.v. and others v. The Netherlands (Application no. 39315/06), 22/11/2012.
7 ECLI:NL:RBDHA:2015:2498 en ECLI:NL:GHDHA:2015:2881.
8 Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten, *Stcrt.* 2015, 46477.

doi: 10.5553/JV/016758502018044001007

ving. Hierbij zij aangetekend dat ook bij klassieke handhaving het instrumentarium wordt uitgebreid en soms dicht komt bij wat de veiligheidsdiensten mogen. Zo laat de recente wetgeving de grootschalige automatische registratie van kentekenplaten toe (ANPR). Onlangs werd het aantal apparaten dat systematisch kentekens registreert uitgebreid met 200 waardoor het totaal komt op 330. Er wordt wel gesteld dat hiermee in feite een 'sleepnet' is gecreëerd om alle bewegingen van voertuigen (inclusief die van advocaten en journalisten) in kaart te kunnen brengen.[9]

Bij de inrichting van de bevoegdheden in de Wiv 2017 is gekozen voor een 'technologie neutrale' benadering. Dit is zichtbaar in een van de meest bediscussieerde onderdelen van de wet. De oude Wiv liet alleen toe dat draadloze informatie in bulk kon worden vergaard, de nieuwe breidt dit uit naar bulkvergaring van informatie die via vaste infrastructuur wordt verspreid (art. 48 e.v.). De wet richt zich daarbij niet alleen op traditionele telecommunicatie, diensten als Facebook, WhatsApp, enzovoort vallen ook onder de reikwijdte van de wet. Bij reguliere rechtshandhaving is veelal het uitgangspunt dat ieder in te zetten middel afdoende is omschreven om aldus rechtszekerheid te bieden en bevoegdheden af te grendelen. Door het nieuwe kabinet is gesteld dat van het willekeurig en massaal verzamelen van gegevens van burgers in Nederland of in het buitenland geen sprake kan, mag en zal zijn.[10] Dit neemt niet weg dat bevoegdheden in de wet breed zijn (Eijkman 2018).

Als er al voor technologieneutraliteit wordt gekozen, zou bij voorkeur een onderscheid moeten worden gemaakt tussen de introductie van nieuwe methoden en de concrete toepassing ervan. Omdat niet voorspelbaar is hoe de technologie zich gaat ontwikkelen is niet bij voorbaat vast te stellen of er sprake is van een toepassing daarvan die mogelijk als te vergaand wordt gezien of alleen onder bepaalde voorwaarden mag worden ingezet. Een veelgebruikt voorbeeld is de lichamelijke integriteit. Ontwikkelingen in de medische wetenschap maken het mogelijk om bijvoorbeeld een pacemaker vanaf buitenaf te herprogrammeren. Is daarmee het hacken van dergelijke pacemakers aanvaardbaar om data te verkrijgen over de gezondheidstoestand van een (buitenlandse) bewindspersoon en via de daartoe benodigde hack vervolgens deze pacemaker te manipuleren (waardoor de betreffende

9 www.ad.nl/binnenland/kentekenregistratie-nu-ook-langs-binnenwegen~a99302d8.
10 *Kamerstukken II* 2017/18, 34 588, nr. 69.

doi: 10.5553/JV/016758502018044001007

persoon meer vermoeid raakt en in politieke onderhandelingen verzwakt)? Alleen op het laatste moment – tijdens het afsluitende debat in de Eerste Kamer – zegde de minister van Binnenlandse Zaken en Koningsrijkrelaties toe dat zich in dit verband mogelijk een situatie zou kunnen voordoen waarin hij eerst het gesprek wil aangaan met de Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD, ook wel commissie-'Stiekem' genoemd) van de Tweede Kamer.[11]

Algemene versus bijzondere bevoegdheden

De nieuwe wet kent een klassiek onderscheid tussen algemene en bijzondere bevoegdheden. Onder de algemene bevoegdheden vallen met name het stelselmatig verzamelen van gegevens omtrent personen uit open bronnen (art. 38) en het raadplegen van informanten (art. 39). Bij de bijzondere bevoegdheden gaat het om activiteiten als het observeren en volgen (art. 40), de inzet van agenten (art. 41), onderzoek van besloten plaatsen, van gesloten voorwerpen en DNA-onderzoek (art. 42/43), het openen van brieven (art. 44), het binnendringen in geautomatiseerde werken (hacken) (art. 45) en het onderzoek van communicatie inclusief bulkverzameling van data via zogenaamde 'onderzoeksopdrachtgerichte interceptie'[12] (artikelen 46 t/m 57) en toegang tot plaatsen (art. 58). Een paar uitzonderingen daargelaten, zijn alle bijzondere bevoegdheden onderhevig aan *ex ante*, voorafgaand, toezicht door de rechter of de speciaal daartoe opgerichte Toetsingscommissie Inzet Bevoegdheden (TIB).
Bij het toepassen van algemene bevoegdheden is er geen voorafgaand onafhankelijk toezicht, maar volstaat veelal de instemming van de Minister van Binnenlandse Zaken en Koninkrijksrelaties of Defensie (of is sprake van een gedelegeerde bevoegdheid). Een belangrijke reden voor dit onderscheid is de indringendheid en impact van bijzondere bevoegdheden. Het is de vraag of de wet op dit punt voldoende toekomstbestendig is. Een dergelijke onderscheiding in de rechtsbescherming past minder goed bij een technologieneutrale benadering en bij de jurisprudentie die in beginsel een dergelijk onderscheid niet kent maar met name ziet op de mate van inbreuk die gemaakt wordt op fundamentele vrijheden. Het grootschalig verzame-

11 *Handelingen I*, 11 juli 2017, 35-8-1.
12 Zie meer hierover in de andere bijdragen.

doi: 10.5553/JV/016758502018044001007

len van gegevens uit openbare bronnen kan eenzelfde of grotere impact hebben dan het in bulk verzamelen van data(Eijkman & Weggemans 2012). Daar komt bij dat het begrip 'uit openbare bron' zich leent voor een extensieve interpretatie zoals het (al dan niet tegen betaling) verkrijgen van illegaal verworven bestanden op het '*darknet*' of vrijwillig via personen die in een ziekenhuis die gegevens vergaren uit systemen waar zij vertrouwelijk toegang toe hebben (denk aan artsen in ziekenhuizen en andere vertrouwenspersonen). Het onderscheid met de bijzondere bevoegdheid tot het binnendringen in een geautomatiseerd werk of het verzamelen van bulk data kan dan vervagen. Voorafgaande onafhankelijke toetsing bij een dergelijke overlap of de keuze tussen een algemene en bijzondere bevoegdheid zou dan op zijn plaats zijn, zeker wanneer er sprake is van een grote(re) impact op mensenrechten. Een andere benadering had kunnen zijn om sowieso meer aan te sluiten bij de jurisprudentie en het onderscheid tussen algemene en bijzondere bevoegdheden geheel of zoveel mogelijk te laten vervallen.

Rechtmatigheids- en doelmatigheidstoetsing

Bij (digitale) informatievergaring dient de inzet van de middelen proportioneel te zijn. De proportionaliteitstoetsing is een standaardelement in de toetsing door de rechter en met name sterk ontwikkeld binnen de jurisprudentie van het Europese Hof voor de Rechten van de Mens. Beperkingen op mensenrechten zijn alleen mogelijk als deze 'noodzakelijk zijn in een democratische samenleving'. Er worden ook wel vergelijkbare/complementaire termen gehanteerd zoals 'nut en noodzaak' of 'subsidiariteit'. De vraag is evenwel hoe aan dergelijke vereisten invulling te geven. In de jurisprudentie van het Hof in Straatsburg wordt aangegeven dat het inzetten van massasurveillance als zeer ingrijpend moet worden gezien omdat primair gegevens worden verzameld van onschuldige burgers.[13]
Naar verwachting zal de Europese jurisprudentie op dit punt zich in de komende jaren verder ontwikkelen. In het wetsvoorstel voor de

13 O.a. *Kennedy v. United Kingdom* (Application nr. 58243/05), 18 mei 2010; *Big Brother and Others v. United Kingdom* (Application nr. 58170/13), 7 januari 2014; *Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015: *Szabó en Vssey v. Hungary* (Application nr. 37138/14), 12 januari 2016. Zie ook Loof e.a. 2016.

doi: 10.5553/JV/016758502018044001007

nieuwe Wiv staat een afzonderlijke bepaling over noodzakelijkheid, proportionaliteit en subsidiariteit. Deze kunnen door de toezichthouders worden getoetst, die aldus niet alleen de rechtmatigheid maar ook de doelmatigheid kunnen beoordelen. Dit is belangrijk omdat bijvoorbeeld uit de Zakharov-zaak[14] blijkt dat '*rubber stamping*' in zaken omtrent geheime surveillance niet voldoende is. Bij toetsing kan niet worden volstaan met te beoordelen of aan alle formaliteiten is voldaan. In andere woorden: of het juridisch raamwerk in orde is. Dat een brede, mede op de doelmatigheid gerichte toetsing - als deze al niet uit de wet zelf volgt[15] - als een paraplu boven de toepassing van de wet hangt, is nog eens expliciet bevestigd via een motie van de Tweede Kamer. Daarin wordt gesteld dat 'de wettelijke eisen van noodzakelijkheid, proportionaliteit en subsidiariteit ook geïnterpreteerd worden en in de praktijk gebruikt worden als eisen die zullen leiden tot een zo gericht mogelijke inzet van bevoegdheden'.[16] Het kabinet heeft verklaard de motie te zullen uitvoeren en zich tijdens de parlementaire behandeling kritisch opgesteld ten aanzien van '*rubber stamping*'.[17]

Onafhankelijk toezicht

Deugdelijk toezicht is een van de belangrijkste waarborgen bij het inzetten van digitale inlichtingenverzameling door veiligheidsdiensten en draagt tegelijkertijd bij aan de legitimatie van deze inzet. De noodzaak van goed en onafhankelijk toezicht wordt benadrukt in het rapport van de Commissie-Dessens (waarin de Wiv werd geëvalueerd), die stelt dat het geven van meer bevoegdheden hand in hand moet gaan met een versterkt stelsel van *checks and balances* (Dessens 2013, p. 10-11). Diverse anderen benaderen dit ook in combinatie met het belang van effectief toezicht.[18] In een afzonderlijke bijdrage wordt uit-

14 Het ging volgens de klager, hoofdredacteur van een uitgeverij in St. Petersburg, om het in het geheim afluisteren en onderscheppen van mobiele telefoonverkeer in Rusland. Dit maakte inbreuk op de bescherming van het privéleven, zoals beschermd door art. 8 van het Europees Verdrag voor de Rechten van de Mens, omdat er geen adequate en effectieve waarborgen waren tegen misbruik (*Roman Zakharov v. Russia* (Application nr. 47143/06), 4 december 2015).

15 Zie o.a. art. 24 (zorgplicht) en 26 (subsidiariteit/proportionaliteit).

16 *Kamerstukken II* 2016/17,34 588, nr. 66.

17 O.a. *Handelingen I* 11 juli 2017, 35-8-3.

18 Raad van State, Advies over het wetsvoorstel de wet op de inlichtingen- en veiligheidsdiensten Wiv 20XX en de verandering van anderen wetten, *Kamerstukken* 2016/17, 34 588, nr. 2, 21 september 2016; CTIVD 2012.

doi: 10.5553/JV/016758502018044001007

gebreider ingegaan op het toezicht. Wij beperken ons hier tot aanvullende observaties inzake de taakverdeling tussen de Rechtbank Den Haag en de TIB (zie ook de artikelen van Dielemans en Hagens in dit nummer).

De jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM)is helder waar het betreft het toezicht.[19] Toezicht dient zowel *ex ante*, ervoor, als *ex post*, erna, geregeld te zijn. Het dient in de eerste plaats onafhankelijk te zijn en kan daarom het best bij een rechterlijke instantie worden ondergebracht. Er is in de regel geen twijfel over de onafhankelijkheid van de rechter. Het is mogelijk dat het toezicht bij een andere instantie wordt gelegd, maar die zal over dezelfde onafhankelijkheid en waarborgen moeten beschikken. Onder de oude Wiv bestond er alleen voorafgaand toezicht door de rechter op het openen van brieven (een onvermijdelijk gevolg van art. 13 Grondwet), in alle andere gevallen was de verantwoordelijke minister exclusief bevoegd. Er ligt een voorstel om artikel 13 Grondwet te wijzigen.[20] In het voorstel blijft weliswaar de rechterlijke last voor het briefgeheim ongewijzigd, maar wordt voor de inzet van digitale middelen in het kader van de nationale veiligheid een uitzondering gemaakt. Het wetsvoorstel is in eerste lezing aanvaard. Het parlement zal zich er opnieuw in tweede lezing over moeten buigen en daarbij moeten ingaan op de vraag of de wijziging voldoende waarborgen biedt in het licht van de Straatsburgse jurisprudentie. De Rechtbank Den Haag oordeelde in ieder geval dat onafhankelijk voorafgaand toezicht een vereiste is bij de relatie tussen een advocaat en zijn cliënt.[21]

In de nieuwe wet is een gecompliceerd stelsel van toezicht opgenomen. Voor het inzetten van bijzondere bevoegdheden tegen advocaten en journalisten dient in beginsel vooraf toestemming te worden verkregen van de Rechtbank Den Haag, bij de meeste andere bijzondere bevoegdheden is voorafgaande toestemming vereist van de TIB, waarin voornamelijk personen zitting hebben die voldoen aan de vereisten om te worden benoemd in de rechterlijke macht.[22] In de discussie rond de totstandkoming van de wet is wel aan de orde geweest waarom er onderscheid zou moeten zijn in de bescherming van advocaten en juristen enerzijds en 'gewone burgers' anderzijds. In hoeverre

19 Kamerstukken II, 2017-2018, 34588, nr. 69.
20 Kamerstukken II, 2013/14, nr. 33.989
21 Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten, Stcrt. 2015, 46477.
22 Zie de voordracht: *Kamerstukken II*, 2017/18, 34 862, nr. 1.

doi: 10.5553/JV/016758502018044001007

kan eigenlijk betoogd worden dat de geregelde bescherming via de rechtbank beter is dan via de TIB? Daarnaast is onvoldoende besproken geweest of ook andere verschoningsgerechtigden, zoals artsen of ngo's, aanspraak zouden moeten kunnen maken op een bijzondere positie. Zo genieten in veel landen politieke ambtsdragers extra bescherming. Dat is ook in Nederland het geval wanneer bijvoorbeeld parlementsleden uitspraken doen in het parlement. Een en ander staat in schril contrast met de huidige wettelijke regeling: ook op het afluisteren en gegevens verzamelen van parlementsleden, leden van de regering of de rechterlijke macht zijn de reguliere procedures van toepassing.

Een contentieuze procedure en de raadpleging van deskundigen

Het kunnen bieden van tegenspraak is een van de fundamentele waarborgen in het recht. In de context van de activiteiten van inlichtingen- en veiligheidsdiensten (evenals bij reguliere rechtshandhaving) zijn er vanzelfsprekende belemmeringen om in alle fasen tegenspraak mogelijk te maken. Zo kan een verdachte/target om vanzelfsprekende redenen niet vooraf geïnformeerd worden over het feit dat hij gaat worden afgeluisterd of dat gegevens zullen worden verzameld. Dit ligt nog ingewikkelder wanneer massaal data van burgers worden ingezameld. Dat in de Wiv de Rechtbank Den Haag en de TIB alleen op basis van verzoeken en overgelegde of gevraagde informatie van de inlichtingendiensten moeten afwegen of een middel kan worden ingezet, is derhalve niet optimaal. Er is voor gepleit om een afzonderlijke '*public advocate*' in te stellen die kan opkomen voor de belangen van de betrokkenen burgers. Ook is gepleit voor de mogelijkheid dat de rechtbank en de TIB zich kunnen laten bijstaan door deskundigen. Het Amerikaanse hof dat toeziet op de handhaving van de Amerikaanse veiligheidswetgeving , de '*FISA court*', heeft bij de herziening van de wetgeving – mede op eigen verzoek – een expliciete bevoegdheid gekregen om zich door deskundigen ('*amici*') te laten adviseren.[23] De Rechtbank Den Haag kan externe deskundigen raadplegen op de voor een rechtbank gebruikelijke wijze.[24] De samenstelling van de TIB voorziet erin dat één van de leden een materiedeskundige is. Daarnaast

23 www.fisc.uscourts.gov/amici-curiae.
24 Art. 194 Rv. Zie over dit onderwerp o.a.: Groot & Elbers 2008.

doi: 10.5553/JV/016758502018044001007

wordt de TIB ondersteund door een bureau waarvan deskundigen deel kunnen uitmaken. In beide gevallen gaat het dus om interne deskundigheid en niet om het aantrekken van externe deskundigheid. Evenwel, de Wiv verbiedt niet dat de TIB op eigen titel externe deskundigen raadpleegt. Bij zowel de rechtbank als de TIB zal het dan moeten gaan om deskundigen die over de noodzakelijke kwalificaties beschikken om kennis te kunnen nemen van vertrouwelijke of geheime informatie, maar het is eveneens voorstelbaar dat vragen op een dusdanig aggregatieniveau worden gesteld dat een en ander niet aan de orde is.

Bindende klachtenprocedure en klokkenluidersregeling

De Wiv kent – zeker in vergelijking met andere landen – een versterkte regeling met betrekking tot klachten van betrokken personen (art. 114 t/m 124) en een geheel nieuwe regeling van klokkenluiders (art. 125 t/m 131). Een nieuwe afdeling klachtenbehandeling binnen de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)[25] is belast met de uitvoering van beide regelingen. Ten aanzien van het klachtenrecht betekent dit dat de Nationale ombudsman niet langer bevoegd is, de wet sluit zelfs in artikel 114, lid 1 elke betrokkenheid van de ombudsman uit: de klachtenprocedure die voorheen bij de Ombudsman lag, is verhuisd naar een nieuwe afdeling binnen de CTIVD (zie ook de artikelen van Dielemans en Hagens in dit nummer).
De afdeling klachtenbehandeling, die zelfstandig opereert binnen de CTIVD, heeft verstrekkende bevoegdheden wanneer sprake is van onrechtmatige of niet behoorlijke gedragingen (art. 124). Zij kan bepalen dat a) een lopend onderzoek dient te worden gestaakt b) de uitoefening van een bevoegdheid dient te worden beëindigd of c) door de diensten verwerkte gegevens dienen te worden verwijderd en vernietigd. De betrokken minister is gehouden om het oordeel van de afdeling klachtenbehandeling uit te voeren, hoewel het natuurlijk wel de vraag blijft hoe een betrokken persoon vermoedt of zelfs weet dat hij of zij onderwerp van interesse is. Daarnaast is de procedure gemakkelijk te begrijpen en toegankelijk voor (potentiële) klagers, inclusief

25 De CTIVD houdt toezicht op de diensten, kan daarover rapporteren en bericht hierover aan onder meer het parlement (art. 97 en verder).

doi: 10.5553/JV/016758502018044001007

degenen die zichzelf vertegenwoordigen.[26] De wet laat veel open voor wat betreft de werkwijze van de afdeling zelf. Om een aantal vraagstukken te benoemen:
- Hoe gaat de commissie anonieme (of geanonimiseerde) klachten en klachten van organisaties behandelen?
- Gaat de afdeling '*in abstracto*' klachten accepteren?
- Hoe streng houdt de afdeling vast aan de vereiste dat de verantwoordelijke minister door de klager vooraf wordt geïnformeerd?
- Voorziet de afdeling in een spoedprocedure ten einde te kunnen oordelen over '*ex nunc*' situaties die actueel zijn?
- Worden klagers daadwerkelijk gehoord of wordt het een 'papieren' procedure?

De klokkenluidersregeling, die zich beperkt tot hen die betrokken zijn of zijn geweest bij de uitvoering van de Wiv of de Wet veiligheidsonderzoeken, sluit in belangrijke mate aan bij de regeling zoals voorzien in de Wet huis voor klokkenluiders. Dit betekent dat er de nodige procedurele vereisten zijn om een beroep te kunnen doen op de regeling. Zo dient in beginsel de mistoestand eerst intern aan de orde te zijn gesteld, voordat naar de CTIVD, afdeling klachtenbehandeling kan worden gestapt. Het blijft bij dit soort regelingen niet eenvoudig om regelingen laagdrempelige te houden en tegelijkertijd misbruik te voorkomen. Wanneer de procedures ertoe leiden dat klagers geen of onvoldoende bescherming krijgen en daarmee 'vogelvrij' worden, wordt het paard achter de wagen gespannen. Het is belangrijk om snel duidelijkheid te krijgen over de werkbaarheid en effectiviteit van de klokkenluidersregelingen, zowel voor wat betreft de algemene regeling in de Wet Huis voor klokkenluiders als voor de bijzondere regeling in de Wiv. De eerste ervaringen met het huis voor klokkenluiders geven aan dat dit een ingewikkeld vraagstuk is in de praktijk.[27]

Bezwaar en beroep

Waar het in het algemene recht gebruikelijk is om procedures van bezwaar en beroep te hebben, is dit in de Wiv onduidelijk. Diverse beslissingen zijn de eerste en laatste, dus in principe finaal. Zij kennen

26 Eijkman 2018; PIA 2016.
27 *Kamerstukken II* 2017/18, 33 258, nr. 34 (+ bijlage).

doi: 10.5553/JV/016758502018044001007

geen in de wet geregeld bezwaar of beroep. Dat geldt voor alle besluiten (of weigeringen om besluiten te nemen) van de uitvoerders en de diverse toezichthouders. Bijvoorbeeld, de TIB- en de CTIVD-klachtenprocedure vallen buiten de Algemene wet bestuursrecht (art. 148 Awb). Als gevolg daarvan kan er geen bewaar worden gemaakt op basis van het algemeen geldende bestuursrecht door bijvoorbeeld de betrokken minister in het geval van de TIB. Ten aanzien van de CTIVD-klachtenafdeling is dit ook het geval. Denk, onder andere, aan een rechtsgeschil tussen de klager en de verantwoordelijk minister, dat in de loop van een klachtenprocedure opkomt. In de context van de WIV kan geen beroep worden ingesteld. Echter, aangezien de CTIVD en de TIB geen rechtscolleges zijn op basis van de Wet op de rechterlijke organisatie, blijft een (beroeps)gang naar de gewone rechter een mogelijkheid. De vraag blijft natuurlijk wat die rechter zal oordelen. Uiteraard is het voor de hand liggend dat dit de Rechtbank Den Haag zal zijn aangezien de betrokken instituties in Den Haag zijn gevestigd.

Uitwisseling met buitenlandse diensten

Internationale informatie-uitwisseling tussen diensten is essentieel bij cyberspionage en grensoverschrijdend terrorisme. Het intensiveren van deze uitwisseling en het verhogen van de hoeveelheid uitgewisselde informatie wordt gezien als een van de grotere uitdagingen voor de komende tijd. De wet scherpt de oude kaders aan. Uitwisseling met andere landen dient in beginsel vooraf te worden gegaan door een toets van het 'democratische en mensenrechtengehalte' van het betreffende land en de professionaliteit van de betrokken veiligheidsdienst, hetgeen wordt neergelegd in een zogenoemde wegingsnotitie (art. 88 t/m 90). Op deze vrij generieke procedure zijn echter uitzonderingen. Op grond van dringende en gewichtige redenen kunnen ook gegevens worden verstrekt aan landen waarmee geen samenwerkingsrelatie bestaat. In dat geval moet de minister wel terstond de CTIVD op de hoogte stellen (art. 64). Bij het uitwisselen van gegevens kan het gaan om zowel geëvalueerde als ongeëvalueerde gegevens. Met name aan deze laatste categorie kunnen risico's zijn verbonden, bijvoorbeeld wanneer het zou kunnen gaan om gegevens die betrekking hebben op verschoningsgerechtigden. De beslissing om gegevens aan derde partijen ter beschikking te stellen zou niet alleen altijd gebon-

doi: 10.5553/JV/016758502018044001007

den moeten zijn aan ministeriële instemming, maar ook aan voorafgaand toezicht. Daar is niet voor gekozen, ondanks het feit dat het kan gaan om zeer impactvolle informatie en met het uit handen geven van deze informatie de controle erover verdwijnt.

Slot

Het behoeft geen betoog dat de Wiv 2017 op meerdere onderdelen beter had gekund. Evenmin is uitgesloten dat bij rechterlijke toetsing in binnen- en buitenland zal blijken dat er gaten in de wet zitten voor wat betreft de conformiteit met de onderliggende mensenrechten. In dit verband zijn enkele van de belangrijkste dilemma's onder de loep genomen. De geconstateerde problemen rondom de algemene en de bijzondere bevoegdheden, de rechtmatigheid en de doelmatigheid, het toezicht, de klachten- en klokkenluidersprocedures, de bezwaar- en beroepsprocedure en uitwisseling met buitenlandse diensten: deze zullen – hoe problematisch ook – mede in de toepassing van de wet zichtbaarder worden. Er ligt hier een grote en zware taak bij het vernieuwde toezicht inclusief de klachtenprocedure. Hopelijk wordt er niet alleen gefocust op rechtmatigheid maar is er ook voldoende aandacht voor doelmatigheid, zoals de Straatsburgse jurisprudentie vraagt. De tijd voor de nieuwe wet om zich te bewijzen is relatief kort. Niet later dan twee jaar na de inwerkingtreding dient met de evaluatie van de WIV 2017 te zijn begonnen.[28] Dat is misschien maar goed ook. Dan zijn er mogelijkheden om in te gaan op de besproken dilemma's en waar nodig een en ander te herzien.

28 *Kamerstukken II* 2016/17, 34 588, nr. 69.

doi: 10.5553/JV/016758502018044001007

Literatuur

Commissie-Dessens 2013
Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, Naar een nieuwe balans tussen bevoegdheden en waarborgen (rapport van de Commissie evaluatie Wiv 2002) (Commissie-Dessens) 2013.

Eijkman, 2018
Q. Eijkman, 'Access to justice for communications surveillance and interception: scrutinising intelligence gathering reform legislation', *Utrecht Law Review* 2018 (geaccepteerd voor publicatie).

Eijkman e.a. 2018 (te verschijnen)
Eijkman, Van Eijk & Van Schaik, *Dutch National Security reform under reviews: Sufficient checks and balances in the Intelligence and Security Services Act 2017*?, Utrecht/Amsterdam: Kenniscentrum voor Sociale Innovatie (KSI) / Instituut voor Informatierecht (IViR) 2018 (te verschijnen)

Eijkman & Weggemans 2012
Q. Eijkman & D. Weggemans, 'Open source intelligence and privacy dilemma's: it is time to reassess state accountability?', *Security and Human Rights* 2016, afl. 4, p. 285-296.

Eskens e.a. 2016
S. Eskens, O. van Daalen en N.A.N.M. van Eijk, '10 standards for oversight and transparency for surveillance by intelligence services', *Journal of National Security Law & Policy*, (8) 2016, afl. 3, p. 553-594, http://jnslp.com/2016/07/25/10-standards-oversight-transparency-national-intelligence-services.

FRA 2015
European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services – Volume I: Member states' legal frameworks* 2015.

FRA 2017
European Union Agency for Fundamental Rights (FRA), *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU – Volume II: Field perspectives and legal update* 2017, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf.

doi: 10.5553/JV/016758502018044001007

De Groot & Elbers 2008
G. de Groot & N.A. Elbers, *Inschakeling van deskundigen in de rechtspraak*, Raad voor de Rechtspraak, Research Memoranda nr. 3, jrg. 4 2008, www.rechtspraak.nl/SiteCollectionDocuments/Inschakeling-van-deskundigen-in-de-rechtspraak.pdf.

Van Hoboken e.a. 2012
J.V.J van Hoboken, A.M. Arnbak & N.A.N.M. van Eijk, *Cloud computing in higher education and research institutions and the USA Patriot Act*, Amsterdam: Institute for Information Law 2012, www.ivir.nl/publicaties/download/684.

Loof e.a. 2015
J.P. Loof, J. Uzman, T. Barkhuysen, A. Buyse, J.H. Gerards & R. Lawson, *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Leiden: Universiteit Leiden 2015, https://dspace.library.uu.nl/handle/1874/323665.

PIA, 2016
Privacy Impact Assessment (PIA), *Privacy impact assessment op de Wet op Inlichtingen- en Veiligheidsdiensten*, Privacy & Identity Lab / Universiteit Tilburg 2016, www.rijksoverheid.nl/documenten/rapporten/2016/02/12/privacy-impact-assessment-wet-op-de-inlichtingen-en-veiligheidsdiensten-20xx

doi: 10.5553/JV/016758502018044001007