BETERE WAARBORGEN VOOR DE WERKWIJZE VAN INLICHTINGENDIENSTEN

Nico van Eijk*

Inlichtingendiensten spelen een belangrijke rol bij het waarborgen van de rechtsstaat. Zij zorgen er mede voor dat fundamentele rechten worden gehandhaafd. Tegelijkertijd beschikken deze diensten over bijzondere bevoegdheden waartegenover bijzondere waarborgen moeten staan. In de groeiende informatiesamenleving wordt meer en meer digitale informatie gegenereerd. Informatie waar inlichtingendiensten meer en meer geïnteresseerd in zijn. Dit creëert nieuwe dilemma's.

In Nederland wordt door twee inlichtingdiensten, de AIVD (Algemene Inlichtingen- en Veiligheidsdienst) en de MIVD (Militaire Inlichtingen- en Veiligheidsdienst) digitale – en andere – informatie vergaard. Zij doen dit in opdracht en onder verantwoordelijkheid van respectievelijk de minister van Binnenlandse Zaken en de minister van Defensie. Op de diensten wordt 'ex post' toezicht uitgeoefend door de Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD). Zo staat het geregeld in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). De Wiv dateert van 2002 en wordt momenteel herzien. Daartoe ligt een wetsvoorstel voor advies bij de Raad van State.

De rechterlijke macht oordeelde over de nieuwe regulering en de toepassing van digitale bevoegdheden door inlichtingendiensten. De bevindingen van de rechters waren ontluisterend

Dat de Wiv in 2002 tot stand is gekomen, is niet zonder betekenis. De aanslag op de Twin Towers in New York ('9/11') vond plaats in 2001. De aanslagen in Londen en Madrid in 2004 en 2005 resulteerden in Europese regulering die telecomaanbieders verplichtte om grootschalig informatie te verzamelen over gebruikers: de Dataretentierichtlijn van 2006.[1] 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. Bevoegdheden bleken zeer ruim te zijn en ongekende mogelijkheden te bieden tot onder meer 'mass surveillance'. Bovendien bleek dat verschillende inlichtingendiensten niet alleen de grenzen van de regulering hadden verkend maar deze ook hadden overschreden. Het gaat dan vooral om de Amerikaanse diensten, over de Europese diensten is relatief weinig bekend. Verder werd duidelijk dat de regulering in de Verenigde Staten, neergelegd in de Patriot Act, vrijwel ongelimiteerde spionage van buitenlanders mogelijk maakte.[2]

Buiten de maatschappelijke discussie die ontstond door de onthullingen – wie heeft niet de Oscarwinnende documentaire over Snowden, *Citizenfour*, gezien – oordeelde ook de rechterlijke macht over de nieuwe regulering 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 zeer extreem 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] In deze beschikking waren met name onvoldoende waarborgen ingebouwd voor wat betreft het gebruik van de gegevens door inlichtingendiensten. In Straatsburg volgde het Europese Hof voor de Rechten van de Mens met de *Zakharov*-zaak.[5] Het Hof scherpt in deze uitspraak haar eerdere jurisprudentie aan en geeft duidelijke grenzen voor digitale surveillance. Overigens was Nederland al

* Prof.dr. N.A.N.M. van Eijk is als hoogleraar informatierecht verbonden aan het Instituut voor Informatierecht (IViR, Universiteit van Amsterdam).

1 Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken.

2 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: IVIR 2012 (*www.ivir.nl/publicaties/download/684*).

3 HvJ EU 16 mei 2014, C-293/12, ECLI:EU:C:2014:238.

4 HvJ EU 6 oktober 2015, C-263/14, ECLI:EU:C:2015:650.

5 EHRM 4 december 2015, 47143/06, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov v. Russia*).

eerder door het Hof veroordeeld vanwege het ongeoorloofd aftappen van journalisten door de geheime dienst om een bron te achterhalen.[6] In Nederland is door de rechter inmiddels de nationale implementatie van de Dataretentie-richtlijn 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 noodmaatregel waarbij een onafhankelijke toetsingscommissie is ingesteld die voorafgaand toestemming moet geven voor het inzetten van bevoegdheden jegens advocaten en journalisten.[8]

In Nederland is door de rechter inmiddels de nationale implementatie van de Dataretentie-richtlijn buiten werking gesteld en zijn nieuwe grenzen gesteld aan het toezicht via een zaak over het afluisteren van advocaten

Al deze jurisprudentie geeft in de eerste plaats het falen van de regelgever weer. Het Europese parlement, de Europese Raad, de Europese Commissie, de Nederlandse regering, de Tweede Kamer en de Eerste Kamer blijken ingestemd te hebben met regelgeving die in strijd is met de geldende fundamentele rechtskaders. Dit kan niet licht worden genomen en zou moeten leiden tot substantiële herbezinning. Nieuwe wetgeving(sinitiatieven) in diverse Europese landen – het Verenigd Koninkrijk, Frankrijk, Nederland – bevestigen slechts dat er weinig lering is getrokken uit de recente jurisprudentie.[9]

Een analyse van de genoemde jurisprudentie levert duidelijke randvoorwaarden op voor digitale informatievergaring door inlichtingendiensten. In deze opinie komen er drie aan de orde: de in te zetten middelen, de proportionaliteit ervan en het toezicht erop.[10] Telkens wordt aangegeven hoe een en ander zich verhoudt tot de Nederlandse wetgeving, zoals neergelegd in de Wet op de inlichtingen en veiligheidsdiensten (Wiv) en/of de voorstellen tot herziening ervan.[11]

Gezien de snelle technologische ontwikkelingen wordt er in het wetsvoorstel voor een nieuwe Wiv ten aanzien van de bevoegdheden van inlichtingendiensten een technologieneutrale benadering bepleit

Inlichtingendiensten mogen meer

Over het algemeen hebben inlichtingendiensten ruimere bevoegdheden dan gewone rechtshandhavers, zoals de politie. Zo hoeven de diensten niet te voldoen aan dezelfde procedurele waarborgen als neergelegd in het Wetboek van Strafvordering en beschikken zij over mogelijkheden zoals het massaal verzamelen van telecommunicatiedata. 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 omgeving.

Gezien de snelle technologische ontwikkelingen wordt er in het wetsvoorstel voor een nieuwe Wiv ten aanzien van de bevoegdheden van inlichtingendiensten een technologieneutrale benadering bepleit. De bestaande Wiv (art. 27) laat alleen toe dat draadloze informatie massaal wordt vergaard, de nieuwe breidt dit uit naar vaste infrastructuur. Bovendien richt de wet zich niet meer alleen op traditionele telecommunicatie, maar vallen ook diensten als Facebook en WhatsApp onder de reikwijdte. 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. Een volstrekt technologieneutrale benadering staat hiermee op gespannen voet. Als er al voor technologieneutraliteit wordt gekozen, dan hoort er een onderscheid te worden gemaakt tussen de methode en de toepassing ervan. Denk daarbij bijvoorbeeld aan het heimelijk in het lichaam plaatsen van op afstand uitleesbare sensoren. Willen we een dergelijk surveillance-middel wel introduceren? Vooraf behoort via een bredere toetsing te worden vastgesteld of een nieuwe methode in het algemeen aanvaardbaar is of niet. Het wetsvoorstel zou op dit punt moeten worden aangepast.

Vooraf behoort via een bredere toetsing te worden vastgesteld of een nieuwe methode in het algemeen aanvaardbaar is of niet. Het wetsvoorstel zou op dit punt moeten worden aangepast

Doelmatigheidstoetsing vereist

Bij digitale informatievergaring dient de inzet van de middelen proportioneel te zijn. De proportionaliteitstoetsing is een standaardelement in de toetsing door de rechter en hoofdzakelijk ontwikkeld in de jurisprudentie van het Europese Hof voor de Rechten van de Mens. Beperkingen op de fundamentele rechten zijn alleen mogelijk als deze 'noodzakelijk zijn in een democratische samenleving'. Er worden ook wel vergelijkbare termen gehanteerd zoals 'nut en noodzaak' of 'subsidiariteit'. De vraag is evenwel hoe aan dergelijke vereisten invulling te geven. Zo is wel betoogd dat het afluisteren van een telefoonverbinding minder ingrijpend zou zijn dan het plaatsen van afluisterapparatuur in een woning. Ook de kosten en complexiteit zijn van een andere orde. Het plaatsen van afluisterapparatuur vraagt beduidend meer dan het leggen van een telefoontap. In de meest recente Europese jurisprudentie wordt echter aangegeven dat het inzetten van mass surveillance juist als zeer ingrijpend moet worden gezien omdat primair gegevens worden verzameld van onschuldige burgers. Naar verwachting zal de Europese jurisprudentie op

6 EHRM 22 november 2012, 39315/06, ECLI:CE:ECHR:2012:1122JUD003931506 (*Telegraaf Media Nederland, Landelijke media b.v. and others v. The Netherlands*).

7 Rb. Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498; Gerechtshof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.

8 Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten, *Stcrt.* 2015, 46477.

9 Zie bijvoorbeeld *www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers*; *www.theguardian.com/law/2016/mar/14/investigatory-powers-bill-not-up-to-the-task*.

10 Aangesloten wordt bij de bevindingen van recent onderzoek: S.J. Eskens, O.L. van Daalen & N.A.N.M. van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Amsterdam: IVIR 2015 (*www.ivir.nl/publicaties/download/1591*).

11 Hier wordt gebruik gemaakt van de tekst van het wetsvoorstel zoals dat op 29 april 2016 is uitgelekt. Zie: *http://vkplusmobilebackend.persgroep.net/rest/content/assets/13a3edbf-7dfb-4515-99b1-2d6abd32f832*.

dit punt zich in de komende jaren verder ontwikkelen. In het wetsvoorstel voor de nieuwe Wiv staat daarom terecht een afzonderlijke bepaling over noodzakelijkheid, proportionaliteit en subsidiariteit. Toezichthouders kunnen dus niet alleen de rechtmatigheid maar ook de doelmatigheid beoordelen. Dit is belangrijk omdat, bijvoorbeeld uit de *Zakharov*-zaak, blijkt dat 'rubberstamping' niet voldoende is. Bij toetsing kan derhalve niet worden volstaan met te beoordelen of aan alle formaliteiten is voldaan.

In recente Europese jurisprudentie wordt aangegeven dat het inzetten van mass surveillance als zeer ingrijpend moet worden gezien omdat primair gegevens worden verzameld van onschuldige burgers

Onafhankelijk toezicht

Deugdelijk toezicht is een van de belangrijkste waarborgen bij het inzetten van digitale opsporing door veiligheidsdiensten. Dat toezicht dient in de eerste plaats onafhankelijk te zijn en kan daarom het beste bij een rechterlijke instantie worden ondergebracht. Er is in de regel geen twijfel over de onafhankelijkheid van de rechter. In beginsel is het mogelijk dat het toezicht bij een andere instantie wordt gelegd, maar die zal over dezelfde onafhankelijkheid moeten beschikken. De enige vorm van onafhankelijk toezicht in de Wiv is de CTIVD, die alleen achteraf kan oordelen over het handelen van de activiteiten van de inlichtingendiensten. De CTIVD beschikt niet over handhavingsinstrumenten. Dit toezichtssysteem van de Wiv is onvoldoende, zoals de jurisprudentie bevestigt.[12] Toezicht behoort betrekking te hebben op alle activiteiten van de inlichtingendiensten in alle stadia (vooraf, tijdens en achteraf) en gepaard te gaan met daadwerkelijke handhavingsinstrumenten. In de huidige Wiv is alleen voorafgaande rechterlijke toestemming vereist bij inbreuken op het briefgeheim. Dit is nu eenmaal zo bepaald in artikel 13 Grondwet, dat het zogenaamde communicatiegeheim regelt. Er ligt een voorstel om artikel 13 Grondwet te wijzigen.[13] 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. In het licht van de recente jurisprudentie heeft de minister van Binnenlandse Zaken evenwel verzocht de behandeling op te schorten. Zoals eerder aangegeven, is er inmiddels een tijdelijke maatregel getroffen waarbij voorafgaand een toetsingscommissie moet instemmen met de inzet van middelen tegen advocaten en journalisten.

Deugdelijk toezicht is een van de belangrijkste waarborgen bij het inzetten van digitale opsporing door veiligheidsdiensten

Foto: Irene Poppelier | © Ars Aequi

In het wetsontwerp dat bij de Raad van State ligt, wordt een duaal systeem van voorafgaand toezicht geïntroduceerd. Voor het inzetten van middelen tegen advocaten en journalisten dient vooraf toestemming te worden verkregen van de Rechtbank Den Haag, in andere gevallen is voorafgaande toestemming vereist van een speciale toetsingscommissie waarin personen zitting hebben die voldoen aan de vereisten om te worden benoemd in de rechterlijke macht. Dit voorstel roept diverse vragen op. In de eerste plaats, waarom is er een onderscheid tussen advocaten en journalisten enerzijds en 'gewone burgers' anderzijds? Is de procedure bij de rechtbank met meer en die bij de toetsingscommissie met minder waarborgen omkleed? Dat lijkt niet verenigbaar met de jurisprudentie. Hooguit kan worden betoogd dat voor zogenaamde verschoningsgerechtigden hun verschoningsaspect om bijzondere en aanvullende waarborgen vraagt. Zo is bij advocaten de rol als verdediger van de belangen van de cliënt in het geding en bij journalisten komt hun rol als 'watchdog' in het geding wanneer bronnen kunnen worden achterhaald. Er is dan alle reden om de kring van bijzondere bescherming verder uit te breiden. De rol van journalisten als 'watchdog' is niet alleen in het geding bij bronbescherming. Anderen spelen eveneens een bijzondere rol bij de bescherming van de rechtsstaat. Zo genieten in veel landen politieke ambtsdragers extra bescherming. Dat is ook in Nederland het geval wanneer bijvoorbeeld parlementsleden uitspraken doen in het parlement. Onder de bestaande Wiv, maar ook in het wetsvoorstel, genieten politici geen enkele bijzondere bescherming. Het beoogde duale stelsel is niet wenselijk. Het is beter om een bijzondere kamer

12 Zie noot 9.

13 *Kamerstukken II* 2014/15, 33989.

in te stellen bij de rechtbank die alle verzoeken vooraf toetst. Een uniforme procedure voorkomt ook mogelijke afstemmingsproblemen en dubbele toestemmingen (de rechtbank en toetsingscommissie geven een verschillende uitleg aan begrippen; voor het volledig kunnen volgen van advocaten en journalisten is zowel toestemming van de rechtbank als de toetsingscommissie nodig). Eventueel worden voor de bijzondere categorieën extra waarborgen ingebouwd.

Het beoogde duale stelsel is niet wenselijk. Het is beter om een bijzondere kamer in te stellen bij de rechtbank die alle verzoeken vooraf toetst. Een uniforme procedure voorkomt ook mogelijke afstemmingsproblemen en dubbele toestemmingen

Het kunnen bieden van tegenspraak is een van de fundamentele waarborgen in het recht. In de context van de activiteiten van inlichtingendiensten (evenals bij reguliere rechtshandhaving) zijn er belemmeringen om in alle fasen van het toezicht tegenspraak mogelijk te maken. Zo kan een verdachte niet vooraf geïnformeerd worden over het feit dat hij wordt afgeluisterd of dat gegevens worden verzameld. Het is nog ingewikkelder wanneer massaal data van burgers worden ingezameld. Dat de rechters of anderen alleen op basis van verzoeken van inlichtingendiensten moeten afwegen of een middel kan worden ingezet is evenmin optimaal. Zoals aangegeven is er juist bij digitale inlichtingenvergaring sprake van snelle technologische ontwikkelingen. In recente Amerikaanse wetgeving zijn beide problemen aangepakt.[14] De speciale rechtbank die toestemming verleent voor het inzetten van middelen, kan experts aanstellen voor zowel fundamentele rechten als technische aspecten. In het Wiv-wetsvoorstel zou de mogelijkheid om externe deskundigen te raadplegen moeten worden toegevoegd.

14 De USA Freedom Act, die de eerdere Patriot Act vervangt (*www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf*).

De herziening van de wetgeving op de inlichtingen- en veiligheidsdiensten biedt een nieuwe kans om het vertrouwen in de rechtsstaat te herstellen en het opereren van de inlichtingendiensten van een juiste legitimatie te voorzien.

Conclusie

Bij inlichtingendiensten gaat het om het inzetten van bijzondere middelen. Dit vereist bijzondere verantwoording om deze inzet te legitimeren en aldus de belangen van de rechtsstaat zeker te stellen. Door technologische ontwikkelingen is het mogelijk om nieuwe middelen met een hoge impact in te zetten. Het grootschalig verzamelen van digitale informatie ('mass surveillance') is daarvan het meest zichtbare voorbeeld. Als gevolg van deze technologische ontwikkelingen zijn niet alleen de mogelijkheden toegenomen, ook zijn traditionele remmingen weggenomen. Zo zijn de kosten verbonden aan het verzamelen en de opslag van digitale data dramatisch gedaald.

Recente jurisprudentie laat zien dat de klassieke normatieve kaders zoals neergelegd in de Europese Conventie voor de Rechten van de Mens en het EU-Handvest onverkort van toepassing zijn. Tegelijkertijd geeft deze jurisprudentie aan dat de wetgever heeft gefaald in het voldoende onderkennen van het belang ervan.

De herziening van de wetgeving op de inlichtingen- en veiligheidsdiensten biedt een nieuwe kans om het vertrouwen in de rechtsstaat te herstellen en het opereren van de inlichtingendiensten van een juiste legitimatie te voorzien. Daarvoor is wel vereist dat het voorliggende wetsvoorstel daadwerkelijk en ruimhartig voldoet aan het normatieve kader. Er kan niet worden volstaan met een 6-, dat past niet bij de rol van beschermer van fundamentele rechten die Nederland internationaal graag opeist.