JAN-JAAP OERLEMANS

Grenzen stellen aan datahonger.

De bescherming van de nationale veiligheid in een democratische rechtsstaat

Universiteit Utrecht

Grenzen stellen aan datahonger.

De bescherming van de nationale veiligheid in een democratische rechtsstaat

Oratie uitgesproken door

Prof. mr. dr. J.J. Oerlemans

bij de aanvaarding van het ambt van bijzonder hoogleraar

op het gebied van Inlichtingen en Recht

aan de Universiteit Utrecht

op maandag 16 november 2020

Universiteit Utrecht

Inhoud

Mijnheer de rector-magnificus, zeer gewaardeerde toehoorders,

NATIONALE VEILIGHEID

Een inlichtingen- en veiligheidsdienst is noodzakelijk om een democratische rechtsstaat te beschermen tegen bedreigingen van de nationale veiligheid.[1] De taakuitvoering van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) vindt ook altijd plaats in het kader van de nationale veiligheid.[2] Wat verstaan we dan onder het begrip 'nationale veiligheid'?

Van het begrip geeft de wetgever geen definitie, met de reden dat de dreiging van nationale veiligheid steeds wijzigt.[3] Voor een beeld van wat de bescherming van nationale veiligheid anno 2020 betekent, biedt het jaarverslag van de AIVD en de MIVD een uitkomst.

In het jaarverslag vertelt de AIVD over zijn activiteiten voor het tegengaan van spionage en ongewenste buitenlandse inmenging, het tegengaan van terrorisme, en het tegengaan van links- en rechts-extremisme. Bij terrorisme vooral richt de AIVD zich vooral op het jihadistisch terrorisme, omdat hiervan nog steeds de grootste dreiging voor de nationale veiligheid van Nederland uitgaat. Die dreiging van jihadistisch terrorisme bestaat meer concreet uit het gevaar van aanslagen in het Westen. De aanslagen in Frankrijk en Oostenrijk in de afgelopen weken zijn daarvoor illustratief. Nederland is vergeleken met onze buurlanden nog relatief gespaard gebleven, maar ook in Nederland komen aanslagen voor. In het jaarverslag 2019 wordt bijvoorbeeld gewezen op de aanslag van 18 maart 2019 op mensen in een tram in Utrecht. Uit de genoemde aandachtgebieden blijkt ook dat de AIVD zich met name richt op de binnenlandse veiligheid.[4] Voor het tegengaan van terrorisme brengt de AIVD onder andere 'ambtsberichten' uit aan de politie en het Openbaar Ministerie. Zij worden dan geïnformeerd over een persoon waar een dreiging voor de nationale veiligheid van uit gaat. Als gevolg van deze ambtsberichten zijn ook in 2019 bijvoorbeeld twee mannen aangehouden op verdenking van het voorbereiding van een aanslag in Nederland.

De MIVD beschermt de nationale veiligheid voor zover het de Krijgsmacht betreft.[5] Het gaat daarbij met name om de bescherming van onze strijdkrachten in missiegebieden en het verzamelen van informatie over buitenlandse strijdkrachten.[6] In het jaarverslag van de MIVD wordt ook digitale spionage genoemd als een prominente dreiging voor de nationale veiligheid.

Digitale spionage vormt volgens de MIVD één van de grootste dreigingen voor Nederland en zijn bondgenoten. Deze digitale spionage wordt uitgevoerd door landen zoals Rusland en China die bijvoorbeeld op zoek zijn naar technologie van universiteiten, biotechnologiebedrijven en de hightech industrie. In de staatsgeheime bijlage van de 'Geïntegreerde Aanwijzing Inlichtingen- en Veiligheid' staan specifieke afspraken over de aandachtsgebieden, zogenoemde 'onderzoeksopdrachten', voor de AIVD en de MIVD.[7]

Natuurlijk doen onze diensten zelf ook aan spioneren, maar dan wordt dat in wetgeving eufemistisch de 'inlichtingentaak buitenland' in de wet genoemd.[8] Bij spionage denken veel mensen aan James Bond. Dat laat zich het beste vergelijken met de bevoegdheid van het inzetten van 'agenten' (de agentenbevoegdheid) voor het verzamelen van inlichtingen. Maar, in tegenstelling tot sommige buitenlandse inlichtingen- en veiligheidsdiensten, hebben Nederlandse geheim agenten hebben geen 'license to kill'.[9]

De inzet van agenten is één van de vele bevoegdheden die de AIVD en de MIVD mogen inzetten voor hun taakuitvoering. Sterker nog, de diensten hebben de meest vergaande bevoegdheden van alle overheidsinstanties (afgezien van de Krijgsmacht) die zijn neergelegd in gedetailleerde wetgeving. Deze 'Wet op de inlichtingen- en veiligheidsdiensten 2017' staat centraal in mijn oratie vanmiddag.

1 Zie rapport Commissie-Havermans, 'De AIVD in verandering. Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst', 2004, p. 23.
2 Deze taken staan omschreven in artikel 8 en artikel 10 Wiv 2017.
3 Zie J.G.M. Rademaker en E.J. Frinking, 'Nationale veiligheid en inlichtingen', p. 189-204 in: B.A. de Graaf, E.R. Muller & J.A. van Reijn (red.), *Inlichtingen- en veiligheidsdiensten*, Kluwer 2010. Zie ook *Kamerstukken II* 1999/00, 25877, nr. 59, p. 1-2, *Kamerstukken II* 2005/06, 30566, nr. 3, p. 18 en *Kamerstukken II* 2016/17, 34588, nr. 3, p. 201.
4 De 'Binnenlandse Veiligheidsdienst' (BVD) is de voorloper van de AIVD. Zie uitgebreid over de geschiedenis van de BVD: D. Engelen, *Geschiedenis van de Binnenlandse Veiligheidsdienst*, Den Haag: Sdu Uitgevers 1998 en C. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie*, 1912-1992, Amsterdam: Boom Geschiedenis 2016.
5 Zie over de MIVD: D. Engelen, *De Militaire Inlichtingendienst 1914-2000*, Den Haag: Sdu Uitgevers 2002.
6 Zie G.R. Dimitru & A.C. Tjepkema, 'Inlichtingenondersteuning bij handhaving en bevordering van de internationale rechtsorde', pp. 225-253 in: de Graaf, Muller & Van Reijn 2010.
7 Zie *Stcrt.* 2019, 63884. P.H.A.M. Abels, 'Per undas adversas? Geheime diensten in de maalstroom van politiek en beleid', (oratie Leiden), Leiden: Universiteit Leiden 2018 voor kritiek op het systeem van de Geïntegreerde Aanwijzing en de invloed van de politiek daarop.
8 Zie over de geschiedenis van de inlichtingendienst buitenland: B.G.J. de Graaff & C. Wiebes, *Villa Maarheeze. De geschiedenis van de inlichtingendienst buitenland*, Den Haag: Sdu Uitgevers 1998.
9 In tegenstelling tot bijvoorbeeld de 'kidon' van de Mossad. Zie o.a., G. Thomas, *Gideon's spies. The secret history of the Mossad*, 17e druk, New York: Thomas Dunne Books.

BEVOEGDHEDEN VAN INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Damens en heren, elke dag worden gigantische hoeveelheden gegevens verzameld, of 'verworven' in het jargon, met de inzet van 'bijzondere bevoegdheden' door de AIVD en de MIVD. Voorbeelden van de bijzondere bevoegdheden die de AIVD en de MIVD mogen inzetten zijn het onderscheppen van communicatie uit telefonieverkeer, internetverkeer, satellietverkeer en radioverkeer. Het onderscheppen van dit verkeer en de analyse daarvan wordt ook wel 'signals intelligence' genoemd.[10]

In mijn oratie noem ik het gewoon "bulkinterceptie", in aansluiting met de internationale term die daarvoor wordt gebruikt.[11] Het dekt de lading ook beter, want dat is wat het is: het onderscheppen van grote hoeveelheden gegevens ('bulk'). En natuurlijk vindt dat plaats voor de uitvoering van de onderzoeksopdrachten van de diensten, net zoals bij de andere bijzondere bevoegdheden. Andere bijzondere bevoegdheden zijn bijvoorbeeld de mogelijkheden om brieven te openen, de haast ouderwetse telefoontap in te zetten en de bevoegdheid computers te hacken van 'targets'.[12] Targets zijn personen of organisaties die onder aandacht staat van de diensten.

Telkens wijzigt de combinatie van middelen in het arsenaal dat de AIVD en de MIVD nodig hebben om gegevens te verzamelen, deze te verwerken tot informatie en vervolgens daarvan inlichtingen te produceren ten behoeve van de afnemers.[13] De AIVD en de MIVD maken inlichtingenproducten voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Justitie en Veiligheid en Defensie. Inlichtingen zijn met andere woorden de producten die worden geleverd aan de afnemers zodat zij betere beslissingen kunnen nemen. Nederlandse inlichtingen- en veiligheidsdiensten doen dus niet aan opsporing en verzamelen dus geen bewijs ten behoeve van strafzaken.[14] Zij mogen ook geen personen arresteren.

Welke bijzondere bevoegdheden van de diensten waardevolle informatie oplevert, is afhankelijk van de context en dreiging. Maar ook digitalisering speelt een belangrijke rol. Een van de belangrijkste en meest recente wijzigingen aan de Wet op de inlichtingen- en veiligheidsdiensten, is het mogelijk maken van bulkinterceptie op de kabel om meer internetverkeer te onderscheppen. Het is mede geïntroduceerd omdat iedereen, en dus ook targets, steeds meer via internet communiceren in plaats van via telefonie.[15]

Vanmiddag wil ik het met u hebben over de bescherming van de nationale veiligheid door de AIVD en de MIVD in onze democratische rechtstaat en de manier waarop dat wordt gereguleerd. De democratische rechtsstaat stelt eisen aan de voorzienbaarheid, transparantie, controle van overheidsoptreden en de bescherming van grondrechten.[16] Wetgeving heeft in deze context een ordeningsfunctie, waarbij burgers moeten worden beschermt tégen de overheid.[17] Wetgeving voor inlichtingen- en veiligheidsdiensten dient er met name voor om misbruik van overheidsmacht tegen te gaan. Ik kom daar een aantal keer op terug.

Eerst bespreek ik met u op welke wijze de bevoegdheden van de diensten met regelgeving worden begrensd en aan welke principes deze wetgeving moet voldoen. Daarbij schets ik ook de totstandkoming van de Wet op de inlichtingen- en veiligheidsdiensten in Nederland. Ten slotte leg ik u uit waarom deze wet opnieuw gewijzigd moet worden.

10 Zie o.a., M.M. Aid, *The Secret Sentry. The untold history of the National Security Agency*, New York: Bloomsbury Press 2009 en Venice Commission, 'On the democratic oversight of signals intelligence agencies', study nr. 719/2013, 2015.
11 Zie o.a., EHRM 13 september 2018, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013, (*Big Brother Watch e.a.t. het Verenigd Koninkrijk*).
12 Bijzondere bevoegdheden mogen alleen worden ingezet voor bepaalde taken van de diensten. Zie artikel 28 Wiv 2017.
13 Zie voor een heldere uiteenzetting van het begrip inlichtingen: B.G.J. de Graaff, *Data en dreiging. Stap in de wereld van intelligence*, Amsterdam: Boom Geschiedenis 2019, p. 13-28, P. Gill & M. Phythian, *Intelligence in an Insecure World*, Cambridge: Polity Press 2006, p. 7, en M. Warner, 'Theories of Intelligence: The State of Play', p. 28, in: R. Dover, M.S. Goodman & C. Hillebrand (red.), *Routledge Companion to Intelligence Studies*, London: Routledge 2014.
14 Zie artikel 13 lid 1 Wiv 2017: *"De ambtenaren van de diensten bezitten geen bevoegdheid tot het opsporen van strafbare feiten"*.
15 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 13.
16 Zie o.a. ook Commissie-Havermans 2004, p. 29 met verwijzing naar *Handelingen I* 2001/03, p. 933.
17 Zie G.J. Veerman, *Over wetgeving. Principes, paradoxen en praktische beschouwingen*, derde druk, Den Haag: Sdu Uitgevers 2012, p. 150-151.

BEGRENZING VAN BIJZONDERE BEVOEGDHEDEN

Ik zal u een geheimpje verklappen: in de afgelopen 10 jaar dat ik onderzoek deed naar digitale opsporing bij de politie en de laatste jaren naar het inlichtingenwerk bij de AIVD en de MIVD, spreek ik elk jaar wel medewerkers die zuchten over de vele regeltjes die hun werk lastig maken, zeker vergeleken met private onderzoekers.

Dat is wat we noemen: een valse analogie (of: valse vergelijking). De inzet van methoden om informatie in te winnen is bij private onderzoekers genormeerd door het privaatrecht, en soms in bijzondere wetgeving zoals de Wet particuliere recherchebureaus. Verder moeten zij zich net als andere burgers aan de wet houden, zoals het Wetboek van Strafrecht en de Algemene Verordening Gegevensbescherming. Private onderzoekers hebben niet de mogelijkheid dezelfde ingrijpende bevoegdheden in te zetten als dienstmedewerkers.

Medewerkers van de AIVD en MIVD zijn aangesteld om de nationale veiligheid te beschermen binnen de grenzen van de wet, waarbij de instrumenten om hun taak te kunnen uitoefenen in wetgeving zijn gegoten. Het is noodzakelijk grenzen te stellen. Ik geloof dat dienstmedewerkers anders in hun honger naar gegevens – ik noem het "datahonger" - welhaast onbeperkte middelen willen inzetten ten behoeve van hun, overigens zeer belangrijke, taakuitvoering. Door regels in de Wet op de inlichtingen- en veiligheidsdiensten worden grenzen gesteld aan deze datahonger. Het biedt bescherming tegen willekeur van de overheid en bindt de overheid aan de wet.[18] Daarbij wordt uiteraard een zekere regeldruk ervaren. Veerman vergelijkt in zijn handboek over wetgeving regeldruk heel mooi met een hoge bloeddruk: "ook bij één regel is er sprake van regeldruk" en "elke regel schept een zekere beperking van de vrijheid van handelen". [19] Afhankelijk van de verschillende factoren, zoals de complexiteit van de regel, de hoeveelheid regels en de hoeveelheid werk die de regel in de uitvoering met zich meebrengt, wordt de regeldruk als hoger of lager ervaren.[20] Maar ook historisch gezien is een duidelijke toename van regels te bespeuren.

Een blik op het verleden laat zien dat het niet vanzelfsprekend is dat er überhaupt publieke wetgeving voor inlichtingen- en veiligheidsdiensten bestaat. Deze - vanuit rechtsstatelijk perspectief - noodzakelijke wetgeving is van recente datum. Pas sinds 1987 kennen wij in Nederland een 'Wet op de inlichtingen- en veiligheidsdiensten'.[21] Deze 'Wiv 1987' is volledig ondermaats volgens de wetgevingsstandaarden van nu.[22] Het bevatte in totaal slechts 26 bepalingen met 17 pagina's toelichting en ging met name over de taakstelling en organisatie van de diensten, met daarnaast enige bepalingen over de verwerking van gegevens. Voor die tijd konden de diensten op

basis van een Koninklijk Besluit nog meer in de schaduw opereren.[23] Bijzondere bevoegdheden en onafhankelijke externe controle op de naleving van deze wet- en regelgeving is pas in Wiv 2002 geregeld.[24]

De Wiv 2017 kent welgeteld 172 artikelen, met 283 pagina's aan toelichting. De Wiv 2017 kent naast de regulering van bevoegdheden, nog andere belangrijke mechanismen om de rechten en vrijheden van betrokkenen te beschermen. Daarbij wijs ik hier in het bijzonder op de regels voor een zorgvuldige verwerking van gegevens, de klachtregeling en de regeling voor het melden van misstanden, de notificatieregeling in de Wiv na de inzet van bepaalde bijzondere bevoegdheden en regelgeving omtrent de verstrekking van gegevens aan nationale instanties en buitenlandse partnerdiensten.[25]

Kennis over deze complexe wet is schaars. Het is belegd bij de juristen van de diensten zelf, de toezichthouders en een klein deel bij de ondersteuning van de beide verantwoordelijke ministers over dit onderwerp (de minister van BZK voor de AIVD en de minister van Defensie voor de MIVD). Met deze leerstoel 'Inlichtingen en Recht', die ik voor vijf jaar mag bekleden, draag ik bij aan kennisontwikkeling en kennisverspreiding de Wiv en andere wetgeving op het gebied van inlichtingen, ook wel 'intelligence' genoemd. Deze kennisverspreiding is noodzakelijk, omdat het wetgeving betreft die burgers moeten beschermen tegen misbruik van de overheid. Voor het maatschappelijk debat en de kwaliteit van de wetgeving is het van belang dat er geschreven en gediscussieerd wordt over het onderwerp.

Ik heb al een aantal keer gezegd dat de Wiv 2017 mensen moet beschermen tegen misbruik van overheidsmacht. Maar u denkt misschien: zonder een 'license to kill' en een arrestatiebevoegdheid valt er toch niet zoveel te beschermen? In de context waar wij het vanmiddag over hebben gaat het natuurlijk over de, minder tastbare, inbreuk op het recht op privacy bij mensen door de inzet van bevoegdheden.[26] Maar het gaat ook om dingen die grote gevolgen kunnen hebben voor mensen, zoals de intrekking van de nationaliteit of verblijfsvergunning, het stopzetten van een bankrekening, en (toch ook) de arrestatie van individuen door de politie. Dat komt omdat van overheidspartijen als de IND, FIOD, financiële instellingen, de politie, en de Koninklijke Marechaussee, wordt verwacht dat zij actie ondernemen als zij een ambtsbericht van de diensten ontvangen. De mogelijkheden om de meest vergaande van alle overheidsbevoegdheden in te zetten en ambtsberichten uit te brengen brengt dus een grote verantwoordelijkheid met zich mee. Zonder regels en waarborgen bestaat het gevaar dat mensen worden overgeleverd aan de willekeur van een veiligheidsdienst en dat willen we voorkomen.

Onze volksvertegenwoordiging bepaalt deze grenzen via wetgeving. Het bepalen van deze grenzen gaat volgens een bepaald mechanisme. Bevoegdheden die een ernstige inbreuk maken op de rechten en vrijheden van de betrokken, moeten helder in de wet beschreven zijn met bijpassende waarborgen.[27] Op die manier wordt duidelijk wat AIVD en de MIVD precies mogen onder welke omstandigheden.[28] Het fungeert hier ook als toetsingsmaatstaf voor het optreden van de overheid en vormt de basis voor controle op dit handelen van de AIVD en de MIVD.[29] Deze uitwerking van het zogenoemde 'legaliteitsbeginsel' is echt een kernprincipe van de rechtsstaat.[30] Bijzondere procedures, zoals een voorafgaande toetsing voorafgaand aan de inzet door een onafhankelijke commissie, zijn verder in de Wiv 2017 ingevoerd om de rechten en vrijheden van de betrokkenen te beschermen.[31] Dat is een voorbeeld van waarborg om misbruik van overheidsmacht te voorkomen.

In onze Grondwet, in verdragen en jurisprudentie van met name het Europees Hof voor de Rechten van de Mens is deels bepaald waar deze wetgeving aan moet voldoen. Nederland heeft zich bij het maken van regelgeving gecommitteerd aan deze regelgeving en minimumnormen te houden. Dit is wat wetgeving in een democratische rechtsstaat in deze context zich meebrengt. Net zo belangrijk: de wetgeving moet óók voldoende instrumenten geven voor de inlichtingen- en veiligheidsdiensten om hun werk effectief te kunnen uitvoeren. In het geval van de AIVD en de MIVD is dat de bescherming van de nationale veiligheid.

18 Idem.
19 Idem, p. 275.
20 Idem, p. 278-280.
21 *Stb.* 1987, 635 (inwerkingtreding op 1 februari 1988).
22 Dit werd overigens ook vroegtijdig gesignaleerd door B. Chorus, 'Nieuwe wettelijke regeling veiligheidsdiensten. Kontrole op BVD onmogelijk', *Privacy en Registratie* 1987, nr. 2, p. 4-10. Zie ook Commissie-Dessens, 'Evaluatie Wet op de inlichtingen-en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen', 2013, p. 23.
23 De organisatie, de werkwijze, de taak en de samenwerking tussen de diensten was geregeld in het (geheime) Koninklijk Besluit van 9 april 1946, nr. 27. Dit Koninklijk Besluit werd niet gepubliceerd en was als 'vertrouwelijk' geclassificeerd. Het Koninklijk Besluit werd bij de griffies van de Tweede Kamer en Eerste kamer ter inzage voor parlementariërs gedeponeerd. In 1972 werd het (inmiddels gewijzigde) Koninklijk Besluit gepubliceerd. Zie D. van Engelen, 'Per Undas Adversas. Een institutioneel onderzoek naar het handelen van de Binnenlandse Veiligheidsdiensten zijn voorgangers', PIVOT-rapport nummer 122, Rijksarchiefdienst / PIVOT & Ministerie van Binnenlandse Zaken en Koninkrijksrelaties: Den Haag 2002, p. 42 en p. 62.
24 In de zaak ABRvS 16 juni 1994, AB 1995, 238 (*Van Baggum*) oordeelde de afdeling bestuursrechtspraak van de Raad van State dat de Wiv in strijd was met artikel 8 EVRM, omdat de Wiv geen bepalingen bevatte onder welke omstandigheden, welke inlichtingenmiddelen de BVD mocht inzetten. Zie Commissie-Dessens 2013, p. 24-25. Zie ook T. Barkhuysen, 'Artikel 8 juncto 13 EVRM: de Sleutel die past op het slot van de BVD-dossierkast?', *NJCM-Bulletin* 19-8 (1994), p. 966-980.
25 Zie over de klachtregeling ook A.H. Toe Laer, 'Klachtbehandeling in de WIV 2017', *NJB* 2019/581.
26 Zie voor alle facetten van de persoonlijke levenssfeer B.J. Koops e.a., 'A typology of privacy', *University of Pennsylvania Journal of International Law* 2017, 38, nr. 2, p. 483-575.
27 *Kamerstukken II* 1997/98, 25877, nr. 3, p. 26 en *Kamerstukken II* 2016/17, 34588, nr. 3, p. 195-198. Zie over dit mechanisme ook J.H. Gerards, *EVRM. Algemene beginselen*, Den Haag 2011, p. 112 en J.J. Oerlemans, *Investigating Cybercrime*, diss. Leiden, Amsterdam: Amsterdam University Press 2017, p. 77-80.
28 Zie ook *Kamerstukken II* 1997/98, 25877, nr. 3, p. 2. De regels dienen hiermee ook rechtszekerheid van betrokkenen. Zie ook A.J. Nieuwenhuis, 'Tussen geheimhouding en controle: de AIVD in de democratische rechtsstaat', *TvCR* 2016, p. 79-98.
29 Zie ook Veerman 2012, p. 25.
30 Zie voor een mooie bespreking over het legaliteitsbeginsel: W.J.M. Voermans, 'Legaliteit als middel tot een doel', p. 3-101, in: W.J.M. Voermans, M.J. Borgers, C.H. Sieburgh (red.), *Controverses rondom legaliteit en legitimatie*, Handelingen Nederlandse Juristen Vereniging nr. 141, Deventer: Kluwer 2011.
31 Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 198.

GRENZEN STELLEN EN TOEZICHT

Op de Wet op de inlichtingen- en veiligheidsdiensten moet onafhankelijk en effectief toezicht worden gehouden.[32] Het gevaar is anders dat wetgeving slechts op papier iets voorschrijft en de praktijk anders is, oftewel het gevaar dat de wet een 'dode letter' is. Toezicht en handhaving zorgen ervoor dat de afgesproken regels daadwerkelijk worden uitgevoerd.[33]

Het punt bij inlichtingen- en veiligheidsdiensten is dat de werkzaamheden geheim zijn en tot op zekere hoogte geheim blijven. Daar zijn goede redenen voor. Het gaat daarbij bijvoorbeeld om de precieze werkwijze van de diensten en namen zogenoemde 'informanten' en 'agenten' die de diensten van informatie voorzien. Als dat bekend wordt dan kunnen de targets van de AIVD en de MIVD of buitenlandse inlichtingen- en veiligheidsdiensten hun gedrag er op aanpassen, waardoor het belangrijke werk van inlichtingen- en veiligheidsdiensten minder effectief wordt. Zelfs de rechterlijke macht heeft in Nederland maar beperkt toegang tot informatie bij de inlichtingen- en veiligheidsdiensten.[34] Dat is anders dan de strafrechtelijke praktijk, waarbij rechters ook oordelen over de rechtmatigheid van de gedragingen van opsporingsinstanties, waarvan de grenzen eveneens in wetgeving zijn aangegeven. Extern toezicht via openbare rapporten van de toezichthouder vormt een tegenwicht en compensatie voor de uitgebreide bevoegdheden van de geheime diensten, waarbij de burger zich over het algemeen niet bewust is van de tegen hem ingezette bevoegdheden en daarom vaak niet in staat zich daartegen te verzetten.[35]

In Nederland wordt dit toezicht uitgevoerd door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), tevens mijn werkgever en het instituut dat de leerstoel 'Inlichtingen en Recht' bij de Universiteit Utrecht heeft gevestigd. De CTIVD heeft toegang tot alle informatie bij de AIVD en de MIVD, dus ook staatsgeheime informatie, voor het controleren van de naleving van de wetgeving. In openbare rapporten wordt beschreven in hoeverre de AIVD en de MIVD de wet naleven. Hierover moet de minister van BZK en de minister van Defensie verantwoording afleggen in vaste Kamercommissies van de Tweede Kamer. Soms bevat een CTIVD-rapport een geheime bijlage die is bestemd voor het parlementaire toezichtsorgaan de 'Commissie voor de Inlichtingen- en Veiligheidsdiensten' ((CIVD), ook wel 'Commissie Stiekem' genoemd).[36] Daarnaast hebben we in Nederland een Toetsingscommissie Inzet Bevoegdheden - de TIB - die een vorm van rechtmatigheidstoezicht uitoefent op de bijzondere bevoegdheden, door al dan niet toestemming te geven voor de inzet van bepaalde bijzondere bevoegdheden.[37]

Het positieve effect van externe toezichthouders is dat de afgesproken regels

door de AIVD en de MIVD beter worden nagekomen. Het zou de maatschappij meer vertrouwen moeten geven in het functioneren van de diensten. Dat vertrouwen is mijns inziens overigens op zijn plaats. In de jaren dat ik voor de toezichthouder heb gewerkt, komen de diensten op mij over als een professionele organisatie waar gedreven en intelligente mensen werken. Voor het overgrote merendeel van de praktijk wordt de wet gewoon nageleefd. Maar 'waar gewerkt wordt, vallen spaanders'. Het zal u niet moeten verbazen dat in zo'n beetje elk toezichtsrapport van de CTIVD onrechtmatigheden staan, oftewel situaties waar één van de bepalingen uit de Wiv 2017 wordt overtreden. Het is de rol van de toezichthouder dat door middel van aanbevelingen en de opvolging daarvan, onrechtmatigheden in de toekomst worden voorkomen.

Wel spreek ik in deze oratie dus over 'datahonger'. Daarmee bedoel ik dat inlichtingen- en veiligheidsdiensten altijd op zoek zijn naar nieuwe informatie om zogezegd de 'dreiging te onderkennen'. Het gaat dan bijvoorbeeld over het verzamelen van informatie over bestaande targets en hun intenties, maar juist ook naar potentiële gegevens over onbekende targets, om op die manier de mogelijke nieuwe dreiging voor de nationale veiligheid te identificeren. Het is daarbij van belang dat de gegevens worden bewaard, omdat ze later misschien belangrijk zijn in onderzoeken van de AIVD en de MIVD. Toch betekent dit wat mij betreft niet dat gegevens onbeperkt bewaard mogen worden. Ik vind het vreemd dat de Wiv 2017 geen maximale bewaartermijn voor gegevens kent. Dat is namelijk één van de basisbeginselen voor de bescherming van persoonsgegevens.

Wij als maatschappij bepalen via onze volksvertegenwoordiging hoe ver de diensten mogen gaan in die informatieverzameling door grenzen te stellen en beperkingen op te leggen aan de gegevensverwerking. Dat zijn geen eenvoudige keuzes. Daarvoor is niet alleen juridische kennis, maar ook kennis over de inlichtingenpraktijk noodzakelijk om het werkbaar te houden. Inlichtingen- en veiligheidsdiensten zullen steeds duidelijk moeten maken welke instrumenten voor hun taakuitoefening noodzakelijk zijn en in hoeverre deze wetgeving werkbaar is.

Want wet- en regelgeving beperken het werk van inlichtingen- en veiligheidsdiensten en dat heeft consequenties. Effectieve toezichthouders zorgen ervoor dat waar nodig dat de teugels soms worden aangetrokken. Maar als negatief effect daarvan wordt in literatuur er ook wel op gewezen dat het risico bestaat dat diensten door streng toezicht bureaucratisch of 'stroperig' kunnen worden.[38] Dat kan het vergaren van inlichtingen in de weg staan. De bescherming van nationale veiligheid is een zeer belangrijke taak dat effectief moet worden uitgeoefend, binnen de grenzen van de democratische rechtstaat natuurlijk.

De Commissie-Jones-Bos is gevraagd in de evaluatie Wiv 2017 onder andere te onderzoeken of de wet in de praktijk werkbaar is gebleven.[39] Dat lijkt mij een goede zaak en ik zal de uitkomsten van het onderzoek bestuderen en zo goed mogelijk uitleggen aan geïnteresseerden, mét de nodige kritiek natuurlijk.

32 Zie ook S. Eskens, O. van Daalen & N. van Eijk, '10 standards for oversight and transparency of national intelligence services', *Journal of National Security Law and Policy* 2016, nr. 3, p. 553-594.
33 Zie ook M. Samadi, *Normering en toezicht in de opsporing. Een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen*, diss. Leiden, Boom Juridisch Uitgevers 2020, p. 35-38.
34 Zie hierover o.a. ABRvS 30 november 2011, ECLI:NL:RVS:2011:BU6382, AB 2012/142, m.nt. van T. Barkhuysen & M.L. van Emmerik. Zie ook EHRM 25 juli 2017, nr. 2156/10, ECLI:CE:ECHR:2017:0725JUD000215610, *EHRC* 2017/215, m.nt. M. Hagens (*M. t. Nederland*).
35 Zie ook *Kamerstukken II* 1997/98, 25877, 3, p. 79. Zie uitgebreid M. Hagens, 'Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van terrorismebestrijding', *Strafblad* 2016, p. 283-292. De Wiv 2017 biedt een regeling om in kennis te worden gesteld van de toepassing van bijzondere bevoegdheden via de notificatieverplichting in artikel 59 Wiv 2017. Zie ook CTIVD-rapport nrs. 24 (2010), 34 (2013) en 51 (2017) over de naleving van de notificatieverplichting.
36 Zie uitgebreid R.H.T. Jansen, 'Parlementaire controle op de inlichtingen- en veiligheidsdiensten in Nederland', *THEMIS* 2019 nr. 5, p. 149-194.
37 Zie artikel 32 lid 2 Wiv 2017.
38 N. Wegge, 'Intelligence Oversight and the Security of the State', *International Journal of Intelligence and CounterIntelligence*, p. 689. DOI:10.1080/08850607.2017.1337445. Muller en Voermans waarschuwen hier ook voor in E.R. Muller & W.J.M. Voermans, 'Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Een nieuw evenwicht tussen veiligheid en waarborgen', *NJB* 2017, nr. 2, p. 107.
39 Zie voor de opdrachtomschrijving *Stcrt.* 2020, 21256. Ook de Algemene Rekenkamer heeft een onderzoek ingesteld naar de incidentele en structurele effecten van de Wiv 2017 op de operationele taakuitoefening van de diensten. Zie Algemene Rekenkamer, Resultaten verantwoordingsonderzoek 2019. Ministerie van Defensie (X). Rapport bij het jaarverslag. Den Haag: 2020, p. 41-42.

DE WIV IN BEWEGING

Jurisprudentie van het Europees Hof van de Rechten van de Mens (EHRM) is een belangrijke drijfveer geweest voor wijzigingen van de Wet op de inlichtingen- en veiligheidsdiensten.[40] Door de zaak *Telegraaf t. Nederland*[41] werd het bijvoorbeeld noodzakelijk een regeling te creëren waardoor een rechter toestemming moet geven voor de inzet van bijzondere bevoegdheden op advocaten en journalisten. De instelling van de TIB werd ook door de wetgever noodzakelijk geacht door EHRM-jurisprudentie.[42] De instelling van de CTIVD als onafhankelijke instantie en de rol van de CTIVD bij klachtbehandeling is daarnaast een uitvloeisel van artikel 13 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), dat gaat over het recht op een effectief rechtsmiddel bij een nationale instantie.[43] Andere waarborgen in de Wiv, zoals het instrument van wegingsnotities bij internationale samenwerking, zijn duidelijk geïnspireerd op aanbevelingen van de CTIVD uit toezichtsrapporten.

Ook wijzigingen in dreigingen voor de nationale veiligheid van Nederland en digitalisering beïnvloeden de Wiv 2017. In de 15 jaar tussen de Wiv 2002 en de Wiv 2017 is er veel veranderd in Nederland. Het dreigingsbeeld is veranderd door de moord op Pim Fortuyn en Theo van Gogh, de aanslagen in Madrid, Londen en Parijs, het uitreizen van mensen voor deelname aan de jihad én natuurlijk de terugkomst van deze personen. In het kader van mijn leerstoel zal ik de komende vijf jaar scherp blijven op de uitbreiding van bevoegdheden via wetswijzigingen op het thema van Inlichtingen en Recht. Juist ook als Nederland een keer slachtoffer wordt van een grote terroristische aanval en een populistische roep tot meer maatregelen of bevoegdheden ontstaat, is gebalanceerde en zorgvuldige wetgeving van belang.[44]

Ook op het gebied van ICT zijn er in de afgelopen 20 jaar grote ontwikkelingen geweest die hun weerslag hebben op het verzamelen en de verwerking van gegevens in het belang van de nationale veiligheid. Bedenk wel: in 2002 waren er nog geen iPhones, geen sociale mediadiensten met miljarden klanten zoals Facebook, geen gratis communicatie-apps en geen online opslagdiensten. Dit zijn allemaal internetdiensten waar ook targets van de diensten gebruik van maken, en de AIVD en de MIVD moeten daar op inspelen om hun werk effectief te blijven uitvoeren. De uitbreiding tot de bevoegdheid voor ‘bulkinterceptie’ op de kabel om meer internetverkeer te onderscheppen en te analyseren moest bijvoorbeeld voorkomen dat de diensten “doof en blind dreigen te worden”, zoals toenmalig minister Jeanine Hennis-Plasschaert in de Eerste Kamer (ietwat dramatisch) toelichtte.

Vandaag, op 16 november 2020, staan wij als Nederland opnieuw voor de vraag of de Wet op de inlichtingen- en veiligheidsdiensten gewijzigd moet worden. Het antwoord daar op is "ja". Dat komt vanwege de bestaande praktijk bij de AIVD en de MIVD waarbij enorme hoeveelheden gegevens worden verzameld en verwerkt uit zogeheten 'bulkdatasets'.

40 Zie ook J.P. Loof e.a., 'Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten', Universiteit Leiden 2015. Zie vanuit internationaal perspectief: I. Cameron, *National Security and the European Convention on Human Rights*, Martinus Nijhoff 2000.
41 EHRM 12 november 2012, nr. 39315/06, ECLI:-CE:ECHR:2012:1122JUD003931506 (*Telegraaf e.a. t. Nederland*).
42 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 5, 193 en 198, met verwijzing naar, o.a., EHRM 12 september 2016, nr. 27138/14, ECLI:CE:ECHR:2016:0112JUD003713814 (*Szabó en Vissy t. Hongarije*).
43 Zie over de noodzaak van een onafhankelijke toezichthouder *Kamerstukken II* 1997/98, 25877, nr. 3, p. 1. Zie *Kamerstukken II* 2016/17, 34588, nr. 3, p. 211 over de noodzaak tot een bindende uitspraken door een onafhankelijke klachteninstantie bij de CTIVD en EHRM 6 maart 2006, nr. 62332/00, ECLI:-CE:ECHR:2006:0606JUD006233200, par. 118 (*Segerstedt-Wiberg t. Zweden*).
44 Gelukkig sta ik daar niet alleen in. Zie bijvoorbeeld M.A.H. van der Woude, *Wetgeving in een Veiligheidscultuur: totstandkoming van antiterrorismewetgeving in Nederland bezien vanuit maatschappelijke en (rechts)politieke context*, diss. Leiden, Den Haag: Boom Juridische Uitgevers 2010.

“Vandaag, op 16 november 2020, staan wij als Nederland opnieuw voor de vraag of de Wet op de inlichtingen- en veiligheidsdiensten gewijzigd moet worden.
Het antwoord daar op is “ja”. Dat komt vanwege de bestaande praktijk bij de AIVD en de MIVD waarbij enorme hoeveelheden gegevens worden verzameld en verwerkt uit zogeheten ‘bulkdatasets’.”

DE NOODZAAK VAN EEN ‘BULKBEVOEGDHEID’ IN DE WIV

Dit is de officiële definitie van een bulkdataset: “een set van gegevens waarvan het merendeel van de mensen niet onder de aandacht van de diensten staat en dat ook nooit zullen staan”. Dit klinkt nog wat abstract, vindt u het niet? Laten we een klein experiment doen om het voor u concreet te maken.

Zoals u misschien weet zijn grote bedrijven en instellingen in de afgelopen jaren vaak slachtoffer van een ‘hack’, waarbij persoonsgegevens worden gestolen.[45] Deze ‘datasets’ aan informatie worden soms tegen betaling en soms gratis op internet aangeboden. Als bijvoorbeeld een combinatie van een inlognaam en wachtwoord van een persoon is gestolen, dan kunnen anderen dit gebruiken om proberen in te loggen in een account met die inlognaam en wachtwoord. Helaas blijkt het menselijke natuur te zijn dat mensen vaak wachtwoorden hergebruiken. Deze gegevens in datasets kunnen dus worden gebruikt om accounts van mensen te hacken. Het is een bekende techniek waar bijvoorbeeld criminelen van gebruik maken.

Om de privacy-inbreuk bij het gebruik maken van gelekte gegevens concreet te maken heb ik een experiment gedaan. Op de website ‘HaveIbeenPwned.com’ kan iedereen op een veilige manier controleren of hun e-mailadres of gebruikersnaam voorkomt in één van de gelekte datasets. Mijn eigen privé-emailadres kwam bijvoorbeeld in twee gelekte datasets voor, waarvan er één van die datasets bestond uit 2,7 miljard bestanden met 773 miljoen e-mailadressen. Mijn e-mailadres, inlognaam en wachtwoord zijn daarbij gelekt en kunnen dus worden misbruikt door anderen.

Om te kijken van wie nog meer gegevens gelekt zijn heb ik nog een aantal e-mailadressen van de Universiteit Utrecht ingevoerd. Het departement rechtsgeleerdheid van de faculteit REBO wordt geleid door onze decaan en drie andere leden van het faculteitsbestuur. Ik ben zo vrij geweest hun e-mailadressen even door de zoekmachine te halen. Hieruit bleek dat alle leden van mijn faculteitsbestuur voorkomen in ten minste één van de gelekte datasets. Maar ook de inlognamen, wachtwoorden en andere gegevens van vier van de vijf leden van het bestuur van mijn departement rechtsgeleerdheid zijn gelekt. Dus als jullie meekijken met de livestream en nog steeds jullie wachtwoord van bijvoorbeeld Dropbox gebruiken, raad ik bij deze met klem aan een ander wachtwoord te nemen!

“Waarom is dit nu relevant voor deze oratie?”, vraagt u zich misschien af. Het gaat mij natuurlijk niet om de verstrekking van mijn beveiligingsadvies uw wachtwoorden

te wijzigen; het gaat mij er om dat persoonsgegevens van u en mij zich in deze datasets bevinden en de AIVD en de MIVD die in het kader van hun taakuitvoering verzameld kunnen hebben. Dat is geen louter theoretische exercitie. Op 13 februari 2018 publiceerde de CTIVD bijvoorbeeld een rapport over 'het verwerven van op internet aangeboden bulkdatasets', dus u kunt zich op basis van het hier voorafgaande wel voorstellen waar dat over gaat.

Uit dat rapport blijkt dat de AIVD en de MIVD de gegevens in deze bulkdatasets kunnen gebruiken om mogelijk later de hackbevoegdheid in te zetten in het kader van de bescherming van de nationale veiligheid. De datasets worden ook gebruikt om targets te kunnen identificeren.[46] Door gegevens in datasets al dan niet met elkaar te combineren, zoals het verbinden van een naam en e-mailadres, kan meer informatie over personen worden verkregen.[47] In het rapport ging het onder andere om een dataset van 'meer dan honderd miljoen personen, waaronder veel Nederlanders'[48] die niet onder de aandacht van de diensten staan en dat ook nooit zullen staan.

Overigens concludeerde CTIVD op basis van een diepteonderzoek dat de gegevens in de bulkdatasets in een duidelijke inlichtingenbehoefte voorzien en de verwerving ervan noodzakelijk was om targets te kunnen identificeren.[49] Met andere woorden is het belang van deze gegevens voor de onderzoeken van diensten dus groot. Uit het onderzoek bleek verder dat de AIVD en de MIVD zich bewust waren over de mogelijke grote privacy-inbreuk die zou plaatsvinden en om die reden een intern beleid hadden opgesteld, waarbij strenge voorwaarden golden voor het verzamelen en gebruik maken van de gegevens. Dit beleid is nu geüpdatet en 1,5 week geleden gepubliceerd in de Staatscourant.[50]

Maar het verzamelen van bulkdatasets van internet is niet de enige manier waarop de diensten bulkdatasets verzamelen. Nog geen twee maanden geleden publiceerde de CTIVD een rapport over hoe met de inzet van de hackbevoegdheid in de onderzoeksperiode in zestien operaties bulkdatasets zijn vergaard en een ander rapport hoe met de inzet van de zogenoemde 'informantenbevoegdheid' een bulkdataset met passagiersgegevens van vliegtuigmaatschappijen van miljoenen personen is vergaard.[51] Voor de inzet van de hackbevoegdheid gelden strenge waarborgen voorafgaand aan de inzet, zoals de voorafgaande toets op rechtmatigheid door de minister en de TIB. Bij de inzet van de informantenbevoegdheid gelden deze extra waarborgen niet. Uit het rapport blijkt ook dat de diensten ook het interne beleid van destijds niet hebben nageleefd.

Om het weer even concreet te maken: deze dataset met passagiersgegevens ging over zogenoemde 'Advance Passenger Information' die luchtvaartmaatschappijen

sinds 2004 op basis van een Europese richtlijn moeten opslaan. Het gaat dan om gegevens zoals de volledige naam, nationaliteit, geboortedatum, geslacht en het vertrekpunt en aankomstpunt. Deze informatie wordt bij alle vluchten van buiten de EU naar een Nederlandse luchthaven geregistreerd en doorgegeven aan de Marchechaussee. De richtlijn verplicht dit en de Marechaussee verwerkt deze gegevens voor onder andere immigratiedoeleinden en de bescherming van de nationale veiligheid bij grenspassages. Maar deze gegevens worden dus ook onderhands verstrekt aan de AIVD. Dat is een goed voorbeeld van wat we 'function creep' noemen, waarbij gegevens dus op een andere manier worden gebruikt dan oorspronkelijk de bedoeling was.

Dus wat betekent dat voor u? Staan uw gegevens mogelijk in die bulkdataset? Gaat u maar na of u een vliegreis van buiten de EU naar een Nederland luchthaven heeft gemaakt. Mijn gegevens staan er mogelijk ook in, omdat ik een jaar of vijf geleden een mooie reis naar Nieuw-Zeeland met mijn vrouw heb gemaakt.

Het punt die ik hier vanmiddag wil maken is dat de wetgever grenzen moet stellen aan het verzamelen en verwerken van gegevens uit bulkdatasets. Nu kunnen bulkdatasets worden verzameld met verschillende bevoegdheden, zoals de informantenbevoegdheid.

De informantenbevoegdheid in artikel 39 Wiv 2017 is echt een gedrocht van een artikel. De meeste mensen denken bij een informant aan een persoon, een individu, die meewerkt en informatie geeft aan de AIVD of de MIVD op vrijwillige basis. Maar pas als je het artikel goed leest, zie je dat ook overheidsinstellingen op vrijwillige basis gegevens kunnen verstrekken. Na het lezen van de toelichting op deze bepaling en het 'Besluit maatregelen rechtstreeks geautomatiseerde toegang inlichtingen- en veiligheidsdiensten'[52] , krijg je het idee dat de diensten de gegevens kunnen raadplegen bij de Marechaussee zelf op een 'hit, no hit'-basis. Zoiets als: "Komt Pietje voor bij jullie? Ja? Ok, dan bekijken we de gegevens".

Maar daar is geen sprake van. In plaats daarvan is hier sprake van de verstrekking van deze gegevens door de Koninklijke Marechaussee aan de AIVD, waarbij de gegevens in bulk worden verzameld, worden opgeslagen en vervolgens bij de AIVD worden gecombineerd met andere gegevens om targets te identificeren.

De huidige regeling voor het verzamelen van bulkdatasets is met andere – meer juridische - woorden onvoldoende voorzienbaar. Ook uit recente jurisprudentie van het Europees Hof voor de Rechten van de Mens en het EU Hof van Justitie over de opslag en verwerking van bulkdata, leid ik af dat voor deze massale opslag van

gegevens met personen die niet onder de aandacht van de diensten staan, strikte regels moeten gelden.[53] Deze regels moeten kenbaar en voorzienbaar zijn voor mensen.

Bulkinterceptie is eigenlijk de enige regeling in de Wiv 2017 die een specifiek kader met regels stelt voor de verzameling en verwerking van bulk. Voor de verzameling van de gegevens uit bulkdatasets moeten mijns inziens ook specifieke regels gelden in de vorm van een bijzondere bevoegdheid, met een apart autorisatieregime bij de verwerking van de gegevens en een uiterste bewaartermijn.

Nogmaals, het is de wetgever in Nederland die de grenzen bepaald voor de verzameling van bulkdatasets en van de gewenste waarborgen voorziet. De Wiv 2017 moet worden aangepast, omdat de huidige regelingen op basis waarvan bulkdatasets mogen worden verzameld onvoldoende voorzienbaar zijn en de regelingen zelf onvoldoende waarborgen bevatten. Mijn hoop is dat de Commissie-Jones-Bos in hun evaluatierapport begin 2021 tot dezelfde conclusie komt. De wetgever zal bij een wetsvoorstel moeten beargumenteren dat de verzameling en regels voor de verwerking van gegevens in bulkdatasets voldoet aan de vereisten die worden afgeleid uit met name het recht op privacy en recht op bescherming van persoonsgegevens. Het is daarbij spannend om te zien hoe de jurisprudentie over bulkdatasets zich de komende tijd nog verder ontwikkeld.

45 Zie bijvoorbeeld het bericht door Olaf van Miltenburg, 'Datalek Blackbaud betrof bij Universiteit Utrecht ook 6000 burgerservicenummers', 14 augustus 2020, Tweakers.net.
46 Zie ook de toelichting op de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017, Stcrt. 2020, 56482.
47 Zie CTIVD-rapport nr. 55 (2018) over het verwerven van door derden op internet aangeboden bulkdatasets, p. 8.
48 CTIVD-rapport nr. 55 (2018), p. 11.
49 Ook in de beleidsreactie op CTIVD-rapport nr. 70 en nr. 71 (2020) lichtten de ministers toe dat de gegevens in bulkdatasets zijn gebruikt voor het 'onderkennen van locaties van Nederlandse uitreizigers in (voormalig) ISIS-gebied, in onderzoek naar de inzet van 'Improvised Explosive Devices (IED's) tegen Nederlandse militairen, in het onderzoek naar de betrokkenheid van de Iraanse dienst bij liquidaties in Nederland en voor het vaststellen van de identiteit van personen die betrokken zijn bij zenuwgasaanvallen in Syrië in 2016/2017'. Dat gegevens in die gevallen van belang zijn geweest voor de veiligheid van militairen en de nationale veiligheid van Nederland lijkt daarmee helder. Maar de *noodzaak* om gegevens te gebruiken, maakt slechte wetgeving niet opeens goed. Een nieuwe bijzondere bevoegdheid voor bulkdatasets zou de Wiv 2017 een stukje beter maken.
50 *Stcrt.* 2020, 56482.
51 CTIVD-rapport nr. 70 (2020) over het verzamelen van bulkdatasets met de hackbevoegdheid en CTIVD-rapport nr. 71 (2020) over het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen.
52 *Stb.* 2018, 115.
53 Zie o.a. EHRM 4 december 2008, nr.30562/04 en 30566/04, ECLI:CE:ECHR:2008:1204JUD003056204 (*S. en Marper t. Het Verenigd Koninkrijk*), HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, ECLI:EU:C:2020:791, par. 117 en 153 (*La Quadrature du Net e.a. t. Frankrijk*) en EHRM 13 september 2018, nrs. 58170/13, 62322/14, 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch e.a.t. het Verenigd Koninkrijk*) (sinds februari 2019 aanhangig bij de Grote Kamer).

INLICHTINGEN EN RECHT IN BREDER PERSPECTIEF

In mijn oratie heb ik het tot nu toe alleen gehad over het vergaren van inlichtingen door de AIVD en de MIVD. Maar mijn onderzoek en taakopvatting vat ik breder op. Ook andere overheidsinstellingen en zelfs private partijen, verwerken inlichtingen. Daarbij kan gedacht worden aan de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de Belastingdienst, de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) en de Koninklijke Marechaussee.

Toch is er voor hen meestal geen gedetailleerd wettelijk kader voorhanden met betrekking tot de inlichtingenmethoden die worden ingezet en bestaat er geen gespecialiseerde toezichthouder die de naleving van deze wetgeving controleert. Het gebrek aan transparantie over deze inlichtingenpraktijk en controle daarop baart mij zorgen en heeft daarmee zeker ook mijn interesse.

Het vakgebied hoop ik samen te verkennen en te ontwikkelen met onze nieuwe promovenda Sophie Harleman en mijn nieuwe collega's bij het Willem Pompe Instituut en Montaigne Centrum van de Universiteit Utrecht.

DANKWOORD

Daarmee kom ik ook tot mijn dankwoord. Ten eerste bedank ik het College van Bestuur van de Universiteit Utrecht voor mijn aanstelling als bijzonder hoogleraar en het in mij gestelde vertrouwen. Ten tweede bedank ik mijn werkgever, de CTIVD, die de vestiging van deze leerstoel mogelijk gemaakt. Dat komt met name door het enthousiasme van de voormalige voorzitter van de CTIVD, Harm Brouwer. Ik heb een aantal jaar veel van hem mogen leren door zijn ervaring als bestuurder bij diverse overheidsinstellingen.

Het rechtmatigheidsonderzoek dat ik bij de CTIVD mag uitvoeren ervaar ik als een bijzondere en verantwoordelijke taak. Werken in een hoogbeveiligde omgeving kent zo zijn nadelen, maar ik vind het inhoudelijk bijster interessant en ik ervaar een fijne samenwerking met mijn collega's van de staf en de commissieleden. De huidige voorzitter, Nico van Eijk, heeft mij meer dan 10 jaar geleden nog als bevlogen hoogleraar lesgegeven in het telecommunicatierecht op de UvA. Daarna zijn we een tijd lang collega's geweest bij de redactie van het tijdschrift Computerrecht. Gelukkig kunnen we ook in deze nieuwe verhouding goed met elkaar opschieten en samenwerken. Maar ik wil met name ook mijn collega Mireille Hagens bedanken voor de fijne samenwerking die wij hebben op academisch vlak. Het heeft al tot veel gezamenlijke publicaties geleid, met als voorlopig hoogtepunt toch wel onze bijdrage voor de serie Tekst & Commentaar op de Wet op de inlichtingen- en Veiligheidsdiensten 2017.

Het was mij nooit gelukt bijzonder hoogleraar te worden zonder de solide basis die ik heb kunnen leggen tijdens mijn onderzoek naar cybercriminaliteit en digitale opsporing. Mijn promotor Jaap van den Herik heeft mij beter leren schrijven en structureren. Ik merk dat ik nu al sommige lessen kan doorgeven aan mijn eigen promovenda. Bart Schermer en Pinar Ölçer waren daarbij ook fijne copromotoren met een machtige kennis op het snijvlak van ICT-recht, mensenrechten en strafrecht. In de afgelopen jaren heb ik veel samengewerkt met andere auteurs en dat hoop ik te blijven doen. Voor mijn samenwerking in het verleden bedank hier in het bijzonder Bert-Jaap Koops, Bart Custers, Rolf van Wegberg, Sofie Royer, Wytske van Wagen en Marleen Weulen Kranenbarg. Ook op sociaal vlak wil ik al mijn collega's bedanken die voor de nodige gezelligheid en inspiratie zorgen. Het is bijzonder te werken in een omgeving met zulke scherpe geesten om je heen, waarbij om de haverklap interessante symposia en congressen worden georganiseerd. Na de coronatijd hoop ik daar weer wat meer van te genieten in Utrecht.

Voor studenten is het online onderwijs natuurlijk niet hetzelfde als fysiek onderwijs in de prachtige gebouwen en omgeving van de Universiteit Utrecht, waarbij ook de koffiepauzes bijvoorbeeld belangrijk zijn voor de sociale dimensie van studeren. Het is nu even doorbijten met online onderwijs, maar ik hoop dat jullie snel weer 'in real life' met docenten kunnen praten en les kunnen krijgen. Tegelijkertijd wil ik meegeven dat je op intellectueel vlak je studententijd ook deels in eigen hand hebt. Als je iets écht interessant vindt, dan loont het om ook buiten onderwijsuren je daar in te verdiepen, ook als daar niet direct iets tegenover staat. Ik hoop dat jullie dan net zo door een onderwerp worden gegrepen, zoals ik destijds zelf heb meegemaakt met mijn onderzoek naar cybercrime en nu met inlichtingen en recht.

Tot slot wil ik op meer persoonlijk vlak uiteraard mijn vrouw, mijn ouders, en overige familie en vrienden bedanken voor de onvoorwaardelijke steun en liefde die ik al heel mijn leven van jullie ontvang. Die steun vertaalt zich bijvoorbeeld in een luisterend oor als ik nieuwe ideeën of plannen heb, maar bijvoorbeeld ook in de regelmatige borrels en andere gezellige gelegenheden waar over de – laten we zeggen – meer aardse zaken gesproken wordt.

Lieve kinderen, zonder jullie was ik in deze periode van thuiswerken ongetwijfeld veel eerder klaar geweest met het schrijven van deze oratie en mijn andere publicaties. Maar dan had ik ook minder van jullie kunnen genieten van jullie aanwezigheid, geklets, en liefde.

Damens en heren, met veel enthousiasme ga ik aan de slag met deze leerstoel. Of, zoals mijn peuter zou zeggen: "Schip ahoy piraatjes, met volle kracht vooruit!".

Ik heb gezegd.

Fotografie — Ed van Rijswijk

JAN-JAAP OERLEMANS

Jan-Jaap Oerlemans studeerde strafrecht en informatierecht aan de Universiteit van Amsterdam. Hij is in 2017 aan de Universiteit Leiden gepromoveerd op het proefschrift 'Investigating Cybercrime'. In de afgelopen 10 jaar heeft hij onderzoek gedaan en gepubliceerd over cybercrime, digitale opsporing en de Wiv 2017.

Vanaf 2017 is hij werkzaam als senior onderzoeker bij de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). Hij is auteur voor de serie 'Tekst & Commentaar' op de Wet op de inlichtingen- en veiligheidsdiensten 2017 en het Cybercrimeverdrag. Tevens is hij redacteur bij het tijdschrift Computerrecht en lid van de expertgroep van het Kenniscentrum Cybercrime van het Hof Den Haag.

uu.nl/medewerkers/JJOerlemans
@jjoerlemans
jjoerlemans.com

Universiteit Utrecht