Boom

info@boomamsterdam.nl
www.boomuitgeversamsterdam.nl

Big Data in de strijd tegen terrorisme

Inlichtingen- en veiligheidsdiensten maken in toenemende mate gebruik van Big Data in de strijd tegen terrorisme. Dikwijls wordt daarbij het verzamelen van persoonsgegevens gepresenteerd als een afweging tussen veiligheid en privacy. Dat is te simplistisch. Beide belangen zijn aspecten van een 'veilige samenleving', een concept dat gebaseerd is op respect voor de menselijke waardigheid van eenieder. Deze 'human security' zou meer bepalend moeten zijn voor de beoordeling van de grenzen aan de inzet van Big Data. Nieuwe technische mogelijkheden mogen hun doel niet voorbijschieten.

door *Marianne Hirsch Ballin*

De auteur is als advocaat werkzaam bij Pels Rijcken & Droogleever Fortuijn, waar zij zich specialiseert in het strafrecht en (punitieve) bestuursrecht. Daarnaast is zij als (gast)docent en onderzoeker strafrecht en strafprocesrecht verbonden aan de Vrije Universiteit Amsterdam. Ze heeft dit artikel op persoonlijke titel geschreven.

IN HET TIJDPERK NA 11 SEPTEMBER 2001 is de westerse samenleving in toenemende mate te karakteriseren als een 'risicomaatschappij',[1] waarin als uitgangspunt geldt dat risico's zo veel mogelijk moeten worden gecontroleerd en ingeperkt. Veiligheid wordt beschouwd als een waarborg die de overheid aan haar burgers moet bieden. Daarbij hoort de verwachting dat de overheid de maatregelen treft om die veiligheid (zo veel mogelijk) te garanderen. In de politiek heeft veiligheid de afgelopen jaren dan ook een belangrijke (al dan niet retorische) rol gespeeld.[2] Mensen zijn zich – mede door de rol van de (sociale) media – steeds meer bewust geworden van risico's, terwijl te-

In de politiek heeft veiligheid de afgelopen jaren dan ook een belangrijke, al dan niet retorische, rol gespeeld

gelijkertijd door de activiteiten van mensen op het internet nieuwe risico's zijn ontstaan. Daarbij gaat het zowel om risico's die voortvloeien uit cybercrime en cyberterrorisme als om risico's voor de persoonlijke levenssfeer door de grootschalige opslag van (persoons)gegevens.[3]

De groeiende rol van het internet en mogelijkheden om data te vergaren gaan niet alleen gepaard met nieuwe risico's en een hoger bewustzijn van die risico's. Mogelijkheden voor de overheid om risico's te controleren en te beperken zijn door nieuwe technische mogelijkheden de laatste jaren enorm gegroeid. Het in kaart brengen van dreigingen en mensen die potentieel een dreiging vormen staat voorop. Mede door het massale gebruik van diverse communicatiemethoden hebben ook de technische mogelijkheden om communicatie en (meta)data te vergaren een hoge vlucht genomen. Door een sterke informatiepositie zou het mogelijk moeten zijn gevaren tijdig te identificeren en weg te nemen (*intelligence-led policing* of ILP[4]). Dat is de veronderstelling van overheden en burgers die opereren in een maatschappij waarin veel belang wordt gehecht aan het controleren en managen van risico's.

IMPACT VAN DE VERWACHTING DAT RISICO'S DOOR DE OVERHEID WORDEN GECONTROLEERD: INTELLIGENCE-LED POLICING

Deze maatschappelijke en politieke ontwikkeling laat zich illustreren door de maatregelen op het terrein van wetgeving en beleid die tussen 2001 en heden zijn genomen op het terrein van terrorismebestrijding. In het bijzonder de maatregelen die zich richten op het vergaren van zo veel mogelijk informatie om (onder meer) terroristische aanslagen te voorkomen zijn onder een vergrootglas gelegd na de 'onthullingen' van Edward Snowden, een voormalige contractant van de Amerikaanse National Security Agency (NSA) over de bevoegdheden van de NSA (en de Engelse GCHQ) in de strijd tegen het terrorisme. Een fundamentele discussie over de groeiende rol van Big Data (waaronder metadata) is daarbij onvermijdelijk.

Nederland

Wetgeving ter uitbreiding van bevoegdheden om informatie te vergaren heeft in Nederland voornamelijk betrekking op het strafrecht. Vooral de ontwikkeling dat bijzondere opsporingsbevoegdheden – zoals het afluisteren van telecommunicatie en het vorderen van informatie – in een strafrechtelijk opsporingsonderzoek van politie en justitie naar terroristische misdrijven kunnen worden ingezet op grond van 'aanwijzingen van een terroristisch misdrijf', springt in het oog. Bij de opsporing van andere strafbare feiten is de inzet van dergelijke bijzondere opsporingsmethoden beperkt tot

een verdenking van een (ernstig) strafbaar feit of, in geval van georganiseerde criminaliteit, tot een verdenking dat strafbare feiten worden beraamd of gepleegd in georganiseerd verband. De wetgever heeft met het aanpassen van het criterium voor inzet van bijzondere opsporingsmethoden bij terroristische misdrijven voor ogen gehad dat op een 'eerder' moment, (ruim) voordat het terroristisch misdrijf is gepleegd, kan worden begonnen met het vergaren van strafrechtelijk bewijsmateriaal jegens vermeende terroristen die een aanslag voorbereiden. Door deze wijziging is bovendien de samenwerking met de AIVD versterkt. Aanleiding voor het opsporingsonderzoek zou veelal informatie verstrekt door de AIVD moeten zijn.[5]

Zeker na 9/11 en de aanslagen in 2004 en 2005 in respectievelijk Madrid en Londen is terrorisme een van de speerpunten van de Nederlandse inlichtingen- en veiligheidsdiensten geworden, met een coördinerende rol van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De rol van het strafrecht is erin gelegen dat – met name op basis van informatie afkomstig van de inlichtingen- en veiligheidsdiensten – vermeende terroristen strafrechtelijk worden vervolgd en berecht. Recent heeft het Nederlandse antiterrorismebeleid een nieuwe impuls gekregen door de dreiging die uitgaat van terugkerende jihadgangers, zichtbaar geworden bij de aanslag door een Franse voormalige jihadganger in het Joods Museum van België in Brussel op 24 mei 2014. Dit heeft zich onder meer geuit in de aankondiging op 29 augustus 2014 van een 'Actieprogramma' met nieuwe maatregelen, zoals het versterken van de strafrechtelijke aanpak van uitreizende en terugkerende jihadgangers, het ontnemen van het Nederlanderschap bij terroristische misdrijven, het verder intensiveren van samenwerkingsverbanden tussen Europese inlichtingendiensten, het versterken van proactieve informatie-uitwisseling en de introductie van nieuwe bestuursrechtelijke bevoegdheden, zoals een meldplicht en een contactverbod.[6]

Door de groei van technische mogelijkheden en de digitalisering van de samenleving zijn de afgelopen jaren ook de mogelijkheden van de inlichtingen- en veiligheidsdiensten vergroot om – binnen het kader van de in de Wet op de inlichtingen- en veiligheidsdiensten van 2002 (Wiv 2002) geregelde bevoegdheden – op grote schaal informatie te vergaren omtrent terroristische dreigingen.[7] Grote verzamelingen van (persoons) gegevens (Big Data) zijn daardoor een belangrijke bron geworden voor de inlichtingen- en veiligheidsdiensten. Hierbij wordt ook samengewerkt met buitenlandse inlichtingendiensten, waaronder de NSA. Mede naar aanleiding van de discussie die is ontstaan over de reikwijdte van bevoegdheden van inlichtingendiensten na de onthullingen van Snowden, heeft de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) op verzoek van de Tweede Kamer onderzoek gedaan naar de

omvang en de aard van datavergaring door de Nederlandse diensten en de samenwerking en uitwisseling van gegevens met buitenlandse diensten.[8] De CTIVD concludeert onder meer dat de door de AIVD en MIVD gebruikte methoden om gegevens te verzamelen op het gebied van telecommunicatie 'passen binnen de bevoegdheden die in de Wiv 2002 aan de diensten zijn toegekend', maar dat technologische ontwikkelingen het mogelijk hebben gemaakt 'om bestaande bevoegdheden op nieuwe, niet altijd door de wetgever voorziene, manieren in te zetten'.[9] In een op 4 september 2014 aan de Tweede Kamer toegezonden toezichtsrapport over het onderzoek van de AIVD op sociale media wordt deze ontwikkeling door de CTIVD nogmaals benadrukt.[10] Voorts constateert de CTIVD dat de AIVD en MIVD ruime bevoegdheden hebben om samen te werken met buitenlandse diensten, waarbij verzamelingen (ruwe) persoonsgegevens worden uitgewisseld. Die samenwerking wordt in beginsel als rechtmatig beoordeeld.[11]

Verenigde Staten

In de Verenigde Staten zijn de maatregelen in het kader van de strijd tegen het terrorisme voornamelijk gericht geweest op het verbeteren van de informatiepositie over terroristische dreigingen en daarmee op het uitbreiden van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Met name de USA PATRIOT Act van 26 oktober 2001 en de FISA Amendments Act van 2008 hebben de bevoegdheden voor het vergaren van informatie substantieel uitgebreid. Dit betreft vooral sectie 702 van de Foreign Intelligence Surveillance Act (FISA) en sectie 215 van de USA PATRIOT Act. Deze bepalingen zouden ook ten grondslag liggen aan het door Snowden bekendgemaakte PRISM-programma, een programma waarin vergaarde data wordt verwerkt.

Sectie 702 van de FISA geeft de bevoegdheid om voor een periode van maximaal een jaar buitenlands inlichtingenmateriaal te vergaren over personen ten aanzien van wie het redelijke vermoeden bestaat dat zij zich buiten de Verenigde Staten bevinden. Hieronder valt ook inlichtingenmateriaal ten aanzien van personen in het buitenland die communiceren met personen binnen de Verenigde Staten. Op grond van deze bepaling wordt persoonlijke informatie vergaard, waaronder de inhoud van communicatie via internet, e-mail en telefoon. Ook worden metadata (gegevens óver communicatie, zoals telefoonnummers en e-mailadressen, of het onderwerp van een e-mailbericht; dus geen inhoud) verzameld en worden foto's en activiteiten op het internet onderschept. Doel van de vergaring dient de bescherming van de nationale veiligheid te zijn. Sectie 215 van de USA PATRIOT Act (de 'FISC document production order') geeft aan de inlichtingen- en veiligheidsdiensten de bevoegdheid om bij derde partijen, zoals providers van telecommunicatiediensten, metadata te vorderen. Ook deze bevoegd-

heid kan worden ingezet in het kader van een onderzoek dat zich richt op de vergaring van 'buitenlands inlichtingenmateriaal'. Voorwaarde is dat het gevraagde materiaal relevant is voor een onderzoek naar internationaal terrorisme of spionage. Een met sectie 215 vergelijkbare bevoegdheid (die in de praktijk veel vaker, maar meestal met een beperktere reikwijdte wordt ingezet) is de bevoegdheid van de FBI om een National Security Letter uit te vaardigen aan een bedrijf dat persoonsgegevens bewaart. Ook de inzet van deze bevoegdheid is beperkt tot onderzoeken naar internationaal terrorisme of spionage.[12] Zowel sectie 702 van de FISA als sectie 215 van de USA PATRIOT Act 2001 vereist een machtiging van een gespecialiseerd rechterlijk college, het Foreign Intelligence Surveillance Court (FISC). Voor het uitvaardigen van de National Security Letter door de FBI is geen machtiging door een rechter vereist.[13]

INTELLIGENCE-LED POLICING MET BEHULP VAN BIG DATA EN PRIVACY

Deze maatregelen in de strijd tegen het terrorisme hebben een nieuwe dimensie gekregen door het gebruik door inlichtingendiensten – met name in de Verenigde Staten – van omvangrijke, ongestructureerde gegevensverzamelingen. Data uit allerlei bronnen (zowel open bronnen als het internet,[14] als de inzet van bevoegdheden tot het onderscheppen van metadata en/of communicatie) worden verwerkt en gecombineerd. Tegelijkertijd zijn de technische mogelijkheden voor het doorzoeken en analyseren van de vergaarde gegevens enorm gegroeid. Dit leidt tot de vaststelling van risicoprofielen, die niet altijd zijn ontleend aan aanwijzingen die op een persoon betrekking hebben, maar ook berusten op statistische waarschijnlijkheden, gelet op de combinatie van bepaalde factoren die volgen uit de vergaarde data. Door de enorme groei van technische mogelijkheden en het massale gebruik van internet en sociale media is de daadwerkelijke impact van bevoegdheden van opsporings- en inlichtingendiensten voor de privacy niet altijd volledig te voorzien geweest bij het uitbreiden van die bevoegdheden. Inlichtingendiensten delen de vergaarde data – vaak naar aanleiding van het identificeren van een 'risico' – bovendien, indien daar aanleiding voor bestaat, met opsporingsinstanties, waardoor ook het strafrechtssysteem door het vergaren en verwerken van Big Data wordt beïnvloed. Alhoewel de vergaring en verwerking van Big

Door nieuwe technische mogelijkheden is de impact van bevoegdheden van opsporingsdiensten voor de privacy niet altijd volledig te voorzien geweest

Data veelal plaatsvindt op grond van bestaande wettelijke kaders,[15] geeft dit aanleiding tot nieuwe vraagstukken ten aanzien van de reikwijdte van die bevoegdheden en de verhouding tot het recht op privacy.

Deze vraagstukken zijn met name sinds de al genoemde onthullingen van Snowden hoger op de politieke (en maatschappelijke) agenda komen te staan.[16] Terwijl aanvankelijk (de uitbreiding van) de wettelijke mogelijkheden om terrorisme adequaat te kunnen bestrijden vooropstonden, gaat het thans (óók) om de vraag of diezelfde mogelijkheden niet een bedreiging vormen voor de persoonlijke levenssfeer van (onschuldige) burgers. Dit geldt in de eerste plaats voor de hiervoor beschreven bevoegdheden van de NSA (en naar aanleiding daarvan in beperktere mate ook voor de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten). Maar ook in de Europese Unie heeft het onderwerp – mede in het kader van de samenwerking tussen de EU en de Verenigde Staten – volop de aandacht.[17] Dat geldt ook voor de Raad van Europa.[18]

BIG DATA TER BESCHERMING TEGEN TERRORISME: EEN BEDREIGING VOOR DE VEILIGHEID?

De beoordeling van de inzet van maatregelen die beogen de veiligheid te vergroten, wordt vaak in de sleutel geplaatst van een afweging tussen enerzijds het (maatschappelijke) belang van veiligheid en anderzijds het (individuele) belang van bescherming van de persoonlijke levenssfeer. Daar valt echter wel wat tegen in te brengen. Beide belangen zijn aspecten van een 'veilige samenleving', gebaseerd op respect voor de menselijke waardigheid van eenieder. In een samenleving waarin respect voor de menselijke waardigheid vooropstaat – niet alleen respect voor de 'wil en keuzes' van eenieder, maar ook voor hun 'zijn', hun persoonlijkheid[19] – wordt veiligheid geboden tegen bedreigingen van die menselijke waardigheid. Dat betekent bescherming tegen (fysieke) bedreigingen door anderen én bescherming tegen aantasting van de integriteit en de persoonlijke levenssfeer. Een samenleving gebaseerd op respect voor de menselijke waardigheid van eenieder biedt ruimte voor persoonlijke ontplooiing en aldus 'human security'.[20] Waarborgen voor menswaardige behandeling maken hiervan deel uit.

De beoordeling van de hiervoor beschreven maatregelen die beogen de (fysieke) veiligheid te vergroten door zo veel mogelijk informatie te vergaren (Big Data), dient dan ook plaats te vinden vanuit de gedachte dat een overheid beide belangen (zo veel mogelijk) dient te waarborgen en na te streven. In feite is ook de regulering van bevoegdheden in het kader van het strafrecht en het veiligheidsrecht (ten aanzien van de bevoegdheden van inlichtingen- en veiligheidsdiensten) op dit uitgangspunt gebaseerd.

Zo is in het Wetboek van Strafvordering de bevoegdheid tot het afluisteren van telecommunicatie beperkt tot de situatie waarin sprake is van een verdenking van een ernstig strafbaar feit (een strafbaar feit waarvoor iemand ook in voorlopige hechtenis kan worden genomen) en dient voorafgaand aan de inzet van de bevoegdheid een machtiging te worden verkregen van de rechter-commissaris. Daarnaast is de mogelijkheid deze bevoegdheid in te zetten ruimer als de aard van het misdrijf daartoe aanleiding geeft. Zo kan indien sprake is van een opsporingsonderzoek naar terroristische misdrijven op grond van 'aanwijzingen' worden getapt: het belang van tijdige interceptie van terroristische misdrijven is daarbij doorslaggevend.

Dezelfde maatstaf zal moeten worden aangelegd bij de beoordeling van de uitbreiding van (vaak al bestaande) bevoegdheden ten gevolge van groeiende technologische mogelijkheden in combinatie met de digitalisering van de samenleving. Dergelijke ontwikkelingen vereisen een heroverweging van de reikwijdte van bevoegdheden tot het vergaren van informatie en daarmee een herijking van de bestaande regulering. In deze heroverweging dienen verschillende elementen te worden betrokken. Die elementen dienen zowel te worden ontleend aan mensenrechten (zoals het recht op bescherming van de persoonlijke levenssfeer, de onschuldpresumptie en het recht op een eerlijk proces), als aan argumenten op grond waarvan gekozen wordt voor de toekenning van bevoegdheden tot informatievergaring. Die laatste argumenten betreffen de reden en dus de legitimatie voor het vergaren van data, waarbij de aard van het 'kwaad' of het misdrijf doorslaggevend zal zijn, naast de effectiviteit (en daarmee noodzakelijkheid en proportionaliteit) van de betreffende bevoegdheid.

Een pasklaar antwoord of een bepaalde bevoegdheid (zowel qua regulering als qua toepassing) bijdraagt aan het realiseren van human security is hiermee nog niet te geven. Het blijft gaan om een afweging tussen meerdere, min of meer abstracte, concepten. De politieke en de maatschappelijke oordeelsvorming over Big Data ten behoeve van meer veiligheid zullen niettemin zorgvuldiger en volledige worden, indien als uitgangspunt voor die oordeelsvorming wordt genomen dat human security aandacht vergt voor zowel fysieke veiligheid als privacy (en andere waarden die verband houden met de menselijke waardigheid). Dit betreft een afweging die niet is gericht op het prioriteren van ofwel het belang van de fysieke veiligheid ofwel het belang respect voor de persoonlijke levenssfeer, maar een afweging die een dubbele toets moet doorstaan.

Voor de rol van Big Data in de strijd tegen het terrorisme vergt dit een herbeoordeling van het gebruik van de (bestaande) bevoegdheden die hiervoor worden ingezet. Bij die herbeoordeling moet zowel worden gelet op het belang van Big Data voor de beoogde bestrijding van terrorisme als op

een adequate regulering van die bevoegdheden. Door die regulering moet immers worden gewaarborgd dat het recht op de persoonlijke levenssfeer bij de vergaring en het gebruik van (omvangrijke) gegevensverzamelingen wordt gerespecteerd. Vandaar dat het gaat om een dubbele toets: een beoordeling op grond van zowel het zo veel mogelijk benutten van de technische mogelijkheden om de fysieke veiligheid te garanderen (en die door middel van regulering van legitimatie wordt voorzien) als de waarborgen die zijn ingebouwd. Die waarborgen zullen er onder meer op moeten zijn gericht misbruik te voorkomen, de situaties te beperken waarin omvangrijke gegevensverzamelingen en daaraan ontleende (en mogelijk voorbarige) verbanden gebruikt mogen worden voor – bijvoorbeeld – het voorkomen van terrorisme, en beperkingen te stellen aan de duur van de opslag en de verdere verwerking van de vergaarde data. Zulke waarborgen zijn – anders dan men soms meent – geen handenbinders die de bestrijding van terrorisme schaden, maar behoren tot de noodzakelijke legitimatie daarvan. De 'dubbele toets' is het beoordelingskader van wetgeving en beleid ten dienste van human security, zoals dat een rechtsstaat past.

Rechterlijke waarborgen zijn geen handenbinders die de bestrijding van terrorisme schaden, maar behoren tot de noodzakelijke legitimatie daarvan

Hiervoor is nodig dat eenieder in de keten van verantwoordelijken voor die bevoegdheden – wetgevers, beleidsmakers, beleidsbepalers en degenen die de bevoegdheden in de praktijk toepassen – zich bewust is van dit uitgangspunt van human security en de bij het reguleren en toepassen van die bevoegdheden in acht te nemen dubbele toets. Hierdoor moet worden voorkomen dat de inzet van nieuwe technische mogelijkheden zijn doel voorbijschiet. Human security zal toenemen indien de redelijkheid bij zowel de (her)overweging van bestaande bevoegdheden als de inzet van die bevoegdheden in het oog wordt gehouden.

Noten

1 U. Beck, *Risk Society. Towards a New Modernity*. Londen: Sage, 2005. Vergelijkbare (sociologische en politicologische) theorieën over een verandering in de maatschappij waarbij het controleren en managen van risico's wordt vooropgesteld, zijn onder meer beschreven door Garland als een 'culture of control' en door Sunstein op grond van het voorzorgsprincipe ('precautionary principle'); zie D. Garland, *The culture of Control. Crime and Social Order in Contemporary Society*. New York/Oxford: Oxford University Press, 2002; en C.R. Sunstein, *Laws of Fear. Beyond the Precautionary Principle*. Cambridge: Cambridge University Press, 2005.

2 De omdoping in 2010 van het Ministerie van Justitie tot Ministerie van Veiligheid en Justitie past in dat plaatje.

3 Zie hierover bijvoorbeeld: E. Schmidt en J. Cohen, *The New Digital Age.*

Reshaping the Future of People, Nations and Business. New York: Google Inc., 2013, pp. 54-81 en 151-182.

4 L. Bachmaier Winter, 'General Report. Section III: Criminal Procedure. Information Society and Penal Law', *International Review of Penal Law* 85 (2014), nr. 1-2, pp. 89-90.

5 Zie *Stb.* 2006, 580 (artikelen 126za-126zs Wetboek van Strafvordering) en *Kamerstukken II* 2004/2005, 30 164, nr. 3 (MvT).

6 Zie Brief 'Integrale Aanpak Jihadisme' van de Minister van Veiligheid en Justitie en de Minister van Sociale Zaken en Werkgelegenheid van 29 augustus 2014 aan de Voorzitter van de Tweede Kamer, met als bijlage *Actieprogramma Integrale Aanpak Jihadisme. Overzicht maatregelen en acties*.

7 Zo gaat het niet langer alleen om het onderscheppen van telecommunicatie, maar ook om communicatie via e-mail en informatie en communicatie die wordt geplaatst en/of verzonden via sociale media als Twitter en Facebook of op webfora of ter beschikking wordt gesteld aan bedrijven ten behoeve van marketing.

8 *Kamerstukken II* 2013/2014, 30 977, nr. 76.

9 CTIVD, *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD* (CTIVD nr. 38). Den Haag: CTIVD, 5 februari 2014, p. ix.

10 CTIVD, *Toezichtsrapport inzake onderzoek door de AIVD op sociale media* (CTIVD nr. 39). Den Haag: CTIVD, 16 juli 2014, pp. vi-viii. Dit rapport is gevoegd bij een brief van 4 september 2014 door de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Voorzitter van de Tweede Kamer.

11 CTIVD nr. 38 (5 februari 2014), pp. xi-xii; CTIVD nr. 39 (16 juli 2014), pp. viii-ix.

12 De bevoegdheid tot het uitvaardigen van een National Security Letter is in verschillende federale wetten opgenomen, waaronder de Electronic Communications Privacy Act van 1986 en de National Security Act van 1947 (bij een amendement uit 1994).

13 Zie voor een uitgebreide bespreking van deze bevoegdheden: M.F.H. Hirsch Ballin, *Anticipative Criminal Investigation. Theory and Counterterrorism Measures in the Netherlands and the United States* (dissertatie Universiteit Utrecht). Den Haag: T.M.C. Asser Press, 2012, pp. 392-400 (sectie 215 van de USA PATRIOT Act), 422-425 (sectie 702 van de FISA) en 426-429 (National Security Letters).

14 Hoewel het gaat om 'open bronnen' raakt de vergaring van data van het internet mede door het grootschalige gebruik van sociale media niet alleen het 'publieke domein' maar ook de persoonlijke levenssfeer.

15 Juridische procedures en rapporten van toezichthoudende instanties hebben tot op heden veelal tot de conclusie geleid dat binnen de – al dan niet aangepaste – wettelijke kaders wordt geopereerd. Zie bijvoorbeeld: *CTIVD* nr. 38; *CTIVD* nr. 39; *Kamerstukken II* 2013/2014, 33 820, nr. 1 (Rapport Commissie Dessens); en de uitspraak van het Amerikaanse FISC in *In Re: Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F. 3d 1004 (FISC of Review 2008)* en *In Re: Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*. Amended Memorandum opinion, FISC, 29 augustus 2013, WL6741573, 1-3.

16 Met name juristen hebben van meet af aan discussie gevoerd over de reikwijdte van ten behoeve van de strijd tegen het terrorisme geïntroduceerde bevoegdheden.

17 Zie bijvoorbeeld Council of the European Union, *Report on the Findings by the EU Co-chairs and the ad hoc EU-US Working Group on Data Protection*, 27 november 2013, 16987/13. Zie ook de rechtszaak van een collectief 'burgers' (strafrechtadvocaten, journalisten en de stichtingen Internet Society Nederland en Privacy First tegen de Nederlandse staat: Rechtbank Den Haag, 23 juli 2014, ECLI:NL:RBDHA:2014:8966.

18 Vanuit de Raad van Europa is een onderzoek 'Massive eavesdropping in Europe' gestart; zie http://assembly.

coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=20050&lang=EN.

19 Vergelijk D. Luban: 'Honoring someone's human dignity means honoring their being, not merely their willing' (*Legal Ethics and Human Dignity*. New York: Cambridge University Press, 2007, p. 76).

20 Zie voor het gebruik van dit 'meeromvattende' begrip van veiligheid bijvoorbeeld de *2005 World Summit Outcome* van de Verenigde Naties over human security (A/RES/601, par. 143). Daarin wordt de nadruk gelegd op 'the right of all people to live in freedom and dignity, free from poverty and despair' en erkend dat 'all individuals, in particular vulnerable people, are entitled to freedom from fear and freedom from want, with an equal opportunity to enjoy all their rights and fully develop their human potential'; zie http://unocha.org/humansecurity/about-human-security/human-security-all.