HET INTERNET

EEN WERELDWIJDE VRIJE RUIMTE MET BEGRENSDE STAATSMACHT

No. 92, november 2014

ADVIESRAAD INTERNATIONALE VRAAGSTUKKEN
ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS

AIV

Leden Adviesraad Internationale Vraagstukken

Voorzitter	Prof.mr. J.G. de Hoop Scheffer
Vicevoorzitter	Mw. mr. H.M. Verrijn Stuart
Leden	Mw. prof.dr. J. Gupta
	Prof.dr. E.M.H. Hirsch Ballin
	Mw. dr. P.C. Plooij-van Gorsel
	Mw. prof.dr. M.E.H. van Reisen
	Prof.dr. A. van Staden
	LGen b.d. M.L.M. Urlings
	Prof.dr.ir. J.J.C. Voorhoeve
Secretaris	Drs. T.D.J. Oostenbrink

Postbus 20061
2500 EB Den Haag
telefoon 070 - 348 5108/6060
fax 070 - 348 6256
aiv@minbuza.nl
www.AIV-Advies.nl

Gecombineerde Commissie Internetvrijheid

Voorzitter	Prof.mr. E.J. Dommering
Leden	Mw. mr.dr. B.T. van Ginkel
	Mw. prof.dr. M. de Goede
	Prof.dr. E.J. Koops
	Mw. dr. P.C. Plooij-van Gorsel
	Mw. mr. H.M. Verrijn Stuart
Secretaris	Drs. J. Smallenbroek

De tekst van het advies is opgesteld met gebruikmaking van teksten en ontwerpen die door voorzitter en leden van de voorbereidingscommissie zijn opgesteld voor dit advies, of met hun instemming zijn ontleend aan hun eerdere wetenschappelijke publicaties, en die deel kunnen uitmaken van hun toekomstige publicaties.

Inhoudsopgave

Woord vooraf

Op 20 februari 2014 vroeg het kabinet de Adviesraad Internationale Vraagstukken (AIV) te adviseren over internetvrijheid. Volgens de adviesaanvraag zijn het recht op privacy, het recht op bescherming van data, het recht op vertrouwelijke communicatie en de vrijheid van meningsuiting voorbeelden van internetvrijheid. Het basisbeginsel is dat rechten die *offline* gelden, ook *online* gelden. Het ontstaan en de snelle groei van het internet hebben geleid tot nieuwe vormen van communicatie, die op hun beurt hebben geleid tot nieuwe vragen hoe deze rechten gewaarborgd kunnen worden, mede omdat deze rechten soms moeten worden afgewogen tegen veiligheidsbelangen. Het kabinet legt aan de AIV de vraag voor hoe internetvrijheid verder bevorderd kan worden in nationaal en internationaal beleid, hoe ver de Nederlandse jurisdictie strekt en wat de rol van het bedrijfsleven is bij het bevorderen van internetvrijheid. De adviesaanvraag is opgenomen in bijlage II van dit advies.

De AIV heeft een gecombineerde commissie ingesteld om dit advies voor te bereiden onder voorzitterschap van prof.mr. E.J. Dommering (Commissie Mensenrechten, CMR). De leden van de commissie waren mw. mr.dr. B.T. van Ginkel (Commissie Vrede en Veiligheid, CVV), mw. prof.dr. M. de Goede (CVV), prof.dr. E.J. Koops (CMR), mw. dr. P.C. Plooij-van Gorsel (AIV/Commissie Europese Integratie) en mw. mr. H.M. Verrijn Stuart (AIV/CMR). Mw. mr. S. Halink (ministerie van Buitenlandse Zaken) was betrokken als de ambtelijke contactpersoon. De commissie werd ondersteund door drs. J. Smallenbroek (secretaris) en mw. S.F.F. Meijer en mw. L Warnier (stagiaires). De commissie sprak met de navolgende deskundigen: C. Bowden (onafhankelijk privacy-onderzoeker), mw. mr.dr. Q. Eijkman (hoofd politieke zaken en persvoorlichting van Amnesty International Nederland), mr. H. Hijmans (afdelingshoofd *Policy & Consultation bij de European Data Protection Supervisor*, op sabbatical), prof. E. Huizer (CTO van SURFnet en hoogleraar internettoepassingen aan de Universiteit Utrecht), prof. M.L. Mueller (hoogleraar Syracuse University School of Information Studies), ir. R. Zenger en H. de Zwart (beiden: *Bits of Freedom*). De AIV is allen zeer erkentelijk voor het delen van hun inzichten.

De AIV heeft dit advies vastgesteld op 1 december 2014.

I Inleiding

Het begrip internetvrijheid omvat volgens de adviesaanvraag een aantal rechten en vrijheden, dat al decennia vastligt in internationale verdragen. Zo bezien betreft het onderwerp internetvrijheid geen nieuwe rechten en vrijheden, maar bestaande rechten en vrijheden gezien door de lens van het internet.

Het internet heeft een samenleving gecreëerd die minder dan ooit aan staatsgrenzen is gebonden. Het heeft daarover een elektronisch net gelegd dat dankzij de universele standaard (het Internet Protocol) en de toepassing van het *world wide web* (www) alles en iedereen met elkaar verbindt: mensen onderling, mensen met kennis, mensen met (staats)organisaties en mensen met dingen. Dit geschiedt op een geïndividualiseerde manier die zijn weerga in de menselijke geschiedenis niet kent. De capaciteit van vaste en mobiele, met elkaar verbonden, elektronische netwerken heeft in het laatste decennium enorme sprongen gemaakt. De toegankelijkheid is steeds meer universeel geworden en steeds minder aan een vaste locatie gebonden. Door de enorme rekenkracht en opslagcapaciteit van computers is het mogelijk geworden gedragsprofielen van individuen en groepen te distilleren uit individuele menselijke gedragingen en verbindingen die sporen op het internet hebben achtergelaten. Deze profielen kunnen worden ingezet voor commerciële (marketing), bestuurlijke (welzijnszorg) en staatsveiligheidsdoeleinden (terrorismebestrijding). *Big Data* is het modewoord van het begin van de 21ste eeuw geworden, zoals *Big Brother* dat voor de tweede helft van de 20ste eeuw is geweest. De verwerking van *Big Data* dringt zich aan iedere tak van wetenschap op en dreigt een doel in zichzelf te worden.[1] Verwerking van *Big Data* maakt gebruik van technieken zoals *datamining* en het koppelen van bestanden van grote verzamelingen gegevens. Daarmee kunnen profielen worden geconstrueerd en verbanden worden blootgelegd. De verzameling gegevens kan bestaan uit inhoudelijke data, maar ook (in het kader van de elektronische communicatie waar dit advies over gaat) uit verkeersgegevens: gegevens die worden gebruikt voor de afhandeling (transport en facturering) van elektronische communicatie. Uit het blootleggen van relatiepatronen tussen verkeersgegevens zijn wel weer vergaande inhoudelijke conclusies te trekken. Tegenwoordig is de analyse van verkeersgegevens belangrijker dan het afluisteren van de inhoud van de communicatie.

De positieve kant van het internet en de daarop draaiende rijkdom aan diensten en toepassingen ligt in het enorme welvaartseffect en in de ontwikkeling van individuele ontplooiingsmogelijkheden, kennis, nieuwe economische activiteiten en vooral een ongekende transparantie van (niche-)markten. De negatieve kant is dat nog nooit in de geschiedenis van de mensheid grote commerciële, bestuurlijke en militaire organisaties zoveel macht over individuen en groepen hebben kunnen uitoefenen. Deze macht overschrijdt vaak staatsgrenzen en is meestal onzichtbaar. De nieuwe term daarvoor is alweer gemeengoed, al heeft zij vooral een marketingcontext: *behavioural targeting*. De positieve kant wordt trouwens ook wel eens overschat. Internet heeft tot een grote machtsvorming in de communicatiesector geleid. De transparantie heeft ook destructieve ontbundelingsprocessen en het ondergraven van kwaliteitsnormen op de markt veroorzaakt.

1 Zie de brede analyse van de Duitse wetenschapsfilosoof Klaus Mainzer, *Die Berechnung der Welt, Von der Weltformel zu Big Data*, München, C.H. Beck 2014.

De AIV zelf vat het begrip internetvrijheid op als de vrije organisatie van vrije en gelijke toegankelijkheid tot, en vrije (niet gecontroleerde) openbare en niet-openbare communicatie op het internet, tussen mensen onderling en met de daarop beschikbare diensten. Dat omvat dus zowel de openbare als de privécommunicatie. De adviesaanvraag legt het accent iets meer op de laatste. In hoofdstuk III zal worden uiteengezet dat het internet de overgang tussen deze twee aspecten steeds vloeiender heeft gemaakt. Beide facetten zullen wel worden geanalyseerd, maar daarin zal het accent dat in de adviesaanvraag wordt gelegd worden gevolgd.

Het internet is een open netwerk dat onderhevig is aan aanvallen die de nationale en individuele vrijheid kunnen bedreigen. De AIV hoopt dat dit advies eraan kan bijdragen de juiste balans te vinden tussen proportionele maatregelen ter voorkoming van dergelijke aanvallen en de door de rechtsstaat gewaarborgde vormen van vrij en rechtmatig gebruik.

Parameters voor normstelling en vrijheid

De normen die gelden voor het internet vormen een zeer complex stelsel. Deze normen kunnen van juridische of niet-juridische aard zijn. Ze kunnen van nationale of internationale herkomst zijn of een andere bron hebben. De politicoloog Joseph Nye heeft daarvoor een verhelderend model ontworpen.[2] Hij heeft de normatieve kracht van de verschillende normen gewaardeerd aan de hand van vier criteria:

- diepte (*depth*): de hiërarchische coherentie van de normen in een bepaald domein;
- breedte (*breadth*): het aantal partijen dat de normen aanvaardt;
- organisatiestructuur (*fabric*): de soort partijen (staten dan wel niet statelijke actoren) die zich aan de normen onderwerpen en de mate waarin samenwerkingsverbanden zijn geformaliseerd;
- naleving (*compliance*): de mate waarin men zich aan de normen onderwerpt.

Op technisch-organisatorisch gebied is de organisatiestructuur zeer los en de norm-stelling informeel (dus: weinig *depth* en *fabric*), maar de naleving scoort hoog, omdat alle partijen belang hebben bij maximale interconnectiviteit en dus bij handhaving van standaarden (dus veel *breadth* en *compliance*). De niet-statelijke herkomst bevordert daar dus de kwaliteit van de naleving. Een factor die niet in Nye's systeem is opgenomen, maar naar het oordeel van de AIV van belang is, is dat de internetgemeenschap (nog steeds) staat voor een gedeeld stelsel van normen en waarden dat de sociale cohesie (naleving) bevordert. *Cybersecurity* scoort over de hele linie laag omdat de toetreding tot het internet heel open is, de diversiteit van personen groot (zeker bij niet-statelijke terreur en andere illegale activiteiten) en de consistentie en transparantie van het normenstelsel gering is. Hier ligt de kern van het vraagstuk dat bekend staat als *internetgovernance*.

Wat betreft de vrijheidswaarden verbonden met het begrip internetvrijheid, is gebruik gemaakt van de categorieën die de organisatie *Freedom House* hanteert in rapporten waarin de vrijheid op het internet per land wordt gemeten. Die categorieën zijn:[3]

2 Joseph S. Nye, The regime complex for managing global cyber activities, Global Commission on Internet Governance Paper Series, no. 1, May 2014. Zie: <www.ourinternet.org>.

3 Freedom House, Freedom on the Net 2013, zie: <http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf>, p. 16, geraadpleegd op 1 september 2014.

- toegangsobstakels: dit omvat infrastructurele en economische toegangsbarrières (soms ook via andere, niet rechtstreeks op het internet gebaseerde maatregelen), regeringsmaatregelen om specifieke applicaties te blokkeren, wettelijke en eigendomsrechtelijke controle over internetdienstverleners;
- inhoudsbeperkingen: dit omvat wettelijke regelingen van de inhoud, technische filtering en blokkering van websites, zelfcensuur, de diversiteit van *online* nieuwsmedia en de rol van informatie- en communicatietechnologie (ICT) bij mobilisatie van burgerbewegingen;
- schending van gebruikersrechten: dit omvat rechtsbescherming, surveillance, privacy en repercussies van *online* activiteiten, zoals vervolging, opsluiting of fysieke intimidatie.

Hoewel dit relevante factoren zijn, laat het model – dat uitsluitend vanuit het perspectief van vrijheidsrechten kijkt – de rol van het internet in de economie buiten beschouwing; die is aanzienlijk. Een land als China, dat in de rapporten van *Freedom House* slecht scoort, kent grote vrijheden als het om commerciële en niet-politieke communicaties op het internet gaat.

Afbakening

Het begrip *cybersecurity* kent meerdere betekenissen. In de eerste plaats heeft het betrekking op de beveiliging van de toegang en het gebruik van het internet om de risico's van fraude, andere criminele handelingen en terreuraanvallen zoveel mogelijk te beperken. In een ruimere betekenis ziet het ook op de bescherming van grondrechtelijke waarden. Een onveilig internet kan daarvoor ook een bedreiging vormen. De AIV is in het advies 'Digitale oorlogvoering' dieper op deze aspecten ingegaan.[4] Hoewel *cybersecurity* en *cybercrime* raakvlakken hebben met internetvrijheid, wordt in verband met de noodzakelijke inperking van het advies niet dieper op deze onderwerpen ingegaan. Het onderwerp van dit advies is onder meer hoe – in een situatie waarin de bestrijding van terrorisme een blijvend gegeven is – de verworvenheden van de rechtsstaat en de daarin verankerde vrijheidsrechten kunnen worden gewaarborgd en hoe Nederland daarin een voortrekkersrol kan spelen. De vraag is hoe beperkingen van grondrechten in dit kader kunnen voldoen aan de eisen van wettelijke verankering, proportionaliteit en effectieve rechtsbescherming tegen inbreuken. Het huidige idee van permanente dreiging en de cruciale rol van het internet daarin[5] mag niet leiden tot een permanente surveillance van *alle* burgers en ongerichte datavergaring. Juist in dit verband is het van cruciaal belang om de juridische kaders te waarborgen en verder te ontwikkelen en de burgerlijke vrijheden te beschermen.

De vrije toegang tot het internet wordt tegenwoordig (zeker in de Nederlandse discussie) in verband gebracht met het begrip netwerkneutraliteit. Aangezien dit onderwerp veel raakvlakken heeft met het (Europese) mededingingsrecht, laat de AIV netwerkneutraliteit in dit advies buiten beschouwing.

4 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken, Digitale oorlogvoering, advies nummer 77, AIV, nummer 22, CAVV, Den Haag, december 2011.

5 Algemene Inlichtingen en Veiligheidsdienst, Het jihadistisch internet, kraamkamer van de hedendaagse jihad, januari 2012. Zie: <https://www.aivd.nl/@2872/jihadistisch/>.

Het internet is in toenemende mate het toneel van een botsing tussen conflicterende rechten, zoals vrijheid van meningsuiting, privacy en auteursrecht. Hoewel die botsingen natuurlijk raken aan het begrip internetvrijheid zoals het hiervoor is gedefinieerd, zullen zij in dit advies slechts zijdelings ter sprake komen, omdat zij buiten de adviesaanvraag vallen. Bovendien gaat het om een problematiek waarmee in de eerste plaats de rechter wordt geconfronteerd.

Opzet van het advies

In hoofdstuk II zal zeer kort worden ingegaan op de geschiedenis van de telecommunicatie (waar komt het internet vandaan?) en de huidige staat van de organisatie van het internet. Een meer uitgebreide toelichting is te vinden in bijlage I. Het is van belang daaraan afzonderlijk aandacht te wijden, aangezien het internet een (geslaagd) voorbeeld is van internationale *governance* die niet uitsluitend bestaat uit multilaterale organisaties en staten, maar waarin ook belangengroepen (*stakeholders*) participeren. Omdat het daarnaast gaat om een los, niet in hiërarchisch verband opererend samenstel van groepen, kan deze vorm van *governance* mede als een *multi-agent* systeem worden gekarakteriseerd.[6] Het is vermoedelijk een van de succesvolste voorbeelden daarvan. In dit hoofdstuk wordt verder geschetst hoe sommige staten proberen en hebben geprobeerd het internet onder een klassiek internationaal systeem van *governance* te brengen. Voorts hebben zij geprobeerd het begrip op te rekken, zodat het allerlei inhoudgerelateerde aspecten zou gaan omvatten. Dit hoofdstuk behandelt verder de vraag welke delen van het internet in de nationale invloedssfeer liggen.

In hoofdstuk III wordt geanalyseerd hoe het conceptuele kader van communicatie- en privacygrondrechten, dat is gevormd in een fysiek zichtbare wereld, in de wereld van *cyberspace* moet worden heroverwogen. Dit is nodig omdat voorheen conceptueel gescheiden rechten steeds meer met elkaar verknoopt zijn geraakt. Dat hoofdstuk laat voorts zien hoe rechtsbegrippen steeds minder vat hebben op de onderliggende werkelijkheid en hoe de rol van de klassieke hoeksteen van het internationale publieke recht, de soevereine staat, fundamenteel verandert.

Hoofdstuk IV bespreekt kort de relevante internationaalrechtelijke kaders, toegespitst op de problematiek die ons hier bezighoudt.

In hoofdstuk V worden vier kwesties besproken die typisch zijn voor internetvrijheid en hoe die gevallen ieder een eigen aanpak vragen. Hoofdstuk VI sluit af met een samenvatting, conclusies en aanbevelingen.

6 Voor de *multi-agent* benadering, zie Luciano Floridi, The 4th Revolution, How infosphere is reshaping human reality, Oxford, Oxford University Press 2014, Chapter 8: Politics: The Rise of the Multi-Agent System.

II Korte voorgeschiedenis van de huidige telecommunicatie: de wording van het internet

In dit hoofdstuk wordt uiteengezet hoe de organisatie van de telecommunicatie (tegenwoordig aangeduid als elektronische communicatie),[7] mede als gevolg van het ontstaan van het internet, is veranderd van staatsgebonden monopolies naar een organisch gegroeid systeem van organisaties. Tussen die organisaties bestaan geen hiërarchische relaties. Bovendien zijn ze niet aan een staat gebonden, zij het dat sommige een losse band met de Verenigde Staten hebben. Daarmee is de controle over telecommunicatie meer diffuus verdeeld dan in het verleden. In bijlage I is aanvullende informatie opgenomen.

II.1 De totstandkoming van de nationale nutsbedrijven (de PTT's) verenigd in de Internationale Telecommunicatie Unie

Aan het eind van de 19de eeuw zijn de Europese landen en de Verenigde Staten begonnen met de aanleg van het vaste telefoonnet binnen hun staatsterritoiren. Het Verenigd Koninkrijk was koploper bij de vorming van een wereldwijd (het *Commonwealth* ondersteunend) telegraafnet. Het Europese model was de staatsonderneming, die ook belangrijke nutstaken kreeg, zoals het verzorgen van een aansluiting op het telefoonnet van de hele bevolking tegen een betaalbare prijs (de zogenaamde universele dienst). Dit staatsbedrijf kreeg een monopolie binnen het nationale territoir omdat het onderdeel van de nutstaak was om ook een fysieke infrastructuur te bouwen in onrendabele gebieden. In de Verenigde Staten werd de facto hetzelfde model gevolgd, omdat het monopolie van AT&T werd gerespecteerd, zolang de monopolist de fysieke infrastructuur in het hele nationale territoir zou uitrollen. Deze nutsmonopolisten waren verticaal geïntegreerde bedrijven die de hele productieketen van de geleverde dienst controleerden tot en met het randapparaat bij de consument door middel waarvan de dienst werd afgenomen. Dit monopolie voor telefoon, telegraaf en telex werd meestal toegevoegd aan het bestaande monopolie van de posterijen (vandaar: PTT, post, telefoon en telegrafie).

De eerste helft van de 20ste eeuw liet de grote sprong zien naar de draadloze communicatie met behulp van radiofrequenties. Voor zover radiofrequenties gebruikt werden voor de typische PTT-diensten, werden ze toebedeeld aan de bestaande nutsmonopolisten. Voor zover de frequenties werden aangewend voor het nieuw opkomende massamedium omroep, werden zij ondergebracht in oligopolistische structuren (Verenigde Staten) of in aparte nutseenheden die de frequenties ten behoeve van de omroeporganisaties gingen exploiteren.

Het internationale telefoonverkeer (de coördinatie van tarieven en standaarden) en het eenduidige gebruik van frequenties (het koppelen van frequenties aan bepaalde diensten) vergden een stabiel internationaal juridisch kader en een overlegstructuur. Daartoe werd in 1865 de *International Telegraph Union* opgericht, de voorloper van de Internationale Telecommunicatie Unie (ITU). De kenmerken van deze internationale telecommunicatiestructuur waren een dienstgebonden en staatsgebonden piramideorganisatie. Daarbij werd al snel een scheiding gemaakt tussen wat

7 Elektronische communicatie is de term die de Europese wetgeving hanteert voor wat in de volksmond telecommunicatie wordt genoemd: telefonie en het internet.

kortheidshalve als ‘inhoud’ en ‘transport’ kan worden aangeduid. De PTT’s gingen over het transport en de daaraan toe te rekenen diensten.

Nieuwe ruimtelijke infrastructuur

De eerste grote doorbraak van dit gesloten piramidemodel was de bouw van een satellietinfrastructuur in de jaren zestig en zeventig van de 20ste eeuw. De eerste commerciële satelliet – de Telstar – werd gelanceerd in 1962. Weliswaar behielden staten het monopolie op het aardesegment (de toedeling van frequenties aan het grondstation van de satelliet), maar het ruimtelijke bereik van de satelliet viel nauwelijks samen met het territorium van staten. Het staatsmonopolie werd daarmee doorbroken. Dit leidde tot de volgende tegenstellingen in de internationale telecommunicatiewereld en in de omroepwereld, waar het gebruikelijk was nationale territoiren af te schermen met technische standaarden en juridische middelen (auteursrecht).

Een eerste tegenstelling was tussen Oost en West: autoritair geregeerde staten zoals Rusland en China verlangden dat het signaal van buitenlandse satellieten niet op hun grondgebied werd gericht. Dit leidde binnen de VN tot de discussie die bekend staat als de controverse tussen *prior consent* en *free flow of information*. Deze tegenstelling resulteerde in een compromisbepaling in het Radio reglement (*World Administrative Radio Conference*) van de ITU. Volgens deze bepaling zouden de leden binnen de technische mogelijkheden vermijden het signaal op een vreemd grondgebied te richten, tenzij er vooraf toestemming door het ontvangende land werd gegeven. Dit lijkt een overwinning voor het *prior consent* beginsel. In de praktijk is de verstrooiing van het signaal echter niet te voorkomen, zodat de bepaling legaliseert dat het signaal van een satelliet te ontvangen is op het grondgebied van een vreemde staat. Satellietsignalen waren dus voor een belangrijk deel wel te ontvangen buiten het gebied waarop het signaal was gericht, ook als daar geen toestemming voor bestond.[8]

Ook op een ander front werd het nationaal gesloten systeem doorbroken. De *prior consent*bepaling was bedoeld voor satellieten die uitzonden op een voor de omroep bestemde band naar het algemene publiek (*direct broadcasting*). Echter, allengs werden de telecommunicatie satellieten, die bedoeld waren voor geadresseerde signalen, ook voor omroepdoeleinden gebruikt. Het onderscheid tussen *direct broadcasting* en telecommunicatiesatellieten verloor daardoor zijn betekenis. Met name commerciële satellietorganisaties gingen de telecommunicatiesatellieten voor omroepdoeleinden gebruiken. Aanvankelijk werd dit als illegaal gebruik gezien (de signalen waren immers geheim, want ze waren niet bestemd voor het algemene publiek), maar uiteindelijk won hier het *free flow of information*beginsel. Dat beginsel houdt in dat niet de technische definitie, maar het sociale gebruik beslissend is.[9] Dit was de eerste stap om de dienst los te maken van een daarvoor bestemde infrastructuur, hetgeen kenmerkend is voor het latere internet. Men kan de huidige discussie over (de omvang van) de internationale regulering van het internet zien als een opleving van die Oost-Westdiscussie. Deze discussie zal wel altijd verbonden blijven met het destijds beroemde McBride-rappport

8 Over de geschiedenis van deze internationale discussie rond satellieten, J.E.S. Fawcett, Outer Space, New Challenges to Law and Policy, Oxford: Clarendon Press 1984.

9 Autronic AG t. Switzerland, 22 mei 1990, Series A, vol. 178.

Many Voices One World uit 1980.[10]

De tweede tegenstelling was de Noord-Zuidcontroverse. Deze ging over de vraag aan wie de schaarse hulpbonnen toebehoorden. De satellieten maken immers gebruik van de geostationaire baan boven de evenaar en Afrikaanse landen stelden zich op het standpunt dat die hun eigendom was. Deze claim is nooit verzilverd. De discussie over de schaarse hulpbronnen en de achterstand daarin van de ontwikkelingslanden beheerst nog steeds het elektronische communicatiedebat in de Noord-Zuidverhoudingen. Deze tegenstelling geldt onverminderd. Dat betekent dat het ontbreken van een behoorlijk ontwikkelde fysieke infrastructuur het belangrijkste aspect van internetvrijheid is in ontwikkelingslanden. Aangezien dit geen onderdeel van de adviesaanvraag vormt, wordt dit onderwerp niet nader behandeld.

De aanleg van de kabel in verschillende Europese landen en in de VS betekende dat de satellietomroep een gemakkelijke alternatieve landingshaven in de nationale staten kreeg. Dat was in feite de hefboom voor het liberaliseren van de omroepmarkt. Deze markt werd met name in Europa tot dan toe gedomineerd door de publieke omroep.

Ontwikkelingen komen samen: Data, Digitalisering en Demonopolisering

Op het internet komen een aantal ontwikkelingen samen, die te karakteriseren zijn als de drie D's: Data, Digitalisering en Demonopolisering.

In de jaren zeventig en tachtig werden aan beide zijden van de Atlantische Oceaan nieuwe telecommunicatiemarkten ontwikkeld, met name voor digitale datadiensten.[11] De ontwikkeling van spraak naar data begon in de jaren tachtig van de 20ste eeuw. De institutionele en commerciële gebruikers van het telecommunicatienet en de telecommunicatiediensten hadden in toenemende mate behoefte aan de opslag en verspreiding van data, waarmee zakelijke berichten snel en efficiënt konden worden overgebracht en bewaard. Men kan daarbij denken aan cijfermatige berichten, zoals het bancaire betalingsverkeer. De PTT's ontwikkelden daarvoor binnen hun nutsmonopolie een datadienst, waarmee zij deze nieuwe markt hoopten te bewerken en de computerfabrikanten aan zich te binden. De liberalisering van de vaste infrastructuur maakte het mogelijk dat steeds meer alternatieve datatoepassingen op netten van instellingen en bedrijven werden ontwikkeld. Het bekendste initiatief op dit punt is dat van de Amerikaanse overheid, die behoefte had aan een efficiënt en veilig datanetwerk. De universitaire gemeenschap ontwikkelde in opdracht van de defensieorganisatie ARPA protocollen voor de overdracht van berichten en data via een elektronisch netwerk: het internetprotocol (IP), het *Transmission Control Protocol* (TCP) en het *Datafile Transfer Protocol* (DTP). In de strijd om de standaarden heeft het protocol van de PTT's het uiteindelijk afgelegd en wereldwijd plaats moeten maken voor het veel eenvoudiger TCP/IP protocol.[12] Ondersteund door de *National Science Foundation* ontwikkelde het zich allengs tot een commercieel wereldwijd open net dat de door de PTT's ontwikkelde

10 Zie: <http://unesdoc.unesco.org/images/0004/000400/040066eb.pdf>.

11 Zie Manuel Castells, Communication Power, Oxford: Oxford University Press 2009, Chapter 2, Communication in the Digital Age.

12 Voor een gedetailleerde analyse van deze ontwikkeling, zie Janet Abbate, *Inventing the Internet,* Cambridge: The MIT Press, 1999, Chapter 5, The Internet in the Arena of International Standards.

toepassingen heeft verdrongen. In de ontwikkelingsfase ontstond in 2001 een periode die economen wel aanduiden als creatieve destructie; een crisis die afbreekt, maar die leidt tot nieuwe innovatieve impulsen,[13] gevolgd door nieuwe innovatieve groei, maar ook verdere commercialisering en pogingen tot toe-eigening van het net: in deze periode ontstonden giganten als Google, Facebook, Twitter en Netflix.

De technische kenmerken van het internet maken het tot een platform voor iedere dienst die volgens de juiste standaarden worden aangeboden. Het TCP/IP protocol maakt elke dienst los van de infrastructuur en verzekert daarmee voor elke dienst die volgens dat protocol wordt aangeboden, een universele *end-to-end* connectiviteit. Het *end-to-end* principe houdt in dat de intelligente toepassingen, voor zover zij niet op het transport betrekking hebben, buiten het net worden gehouden. Binnen de computers voltrok zich dezelfde ontwikkeling: de software kan nu functioneren op alle hardware en vice versa. Bovendien heeft de liberalisering van de elektronische communicatiemarkt de toegang tot het netwerk vrijgemaakt voor diensten, die met de netwerkexploitant concurreren. Naast een diversiteit van diensten voor korte berichten (van e-mail tot Twitter) kent het internet door het *world wide web* krachtige toepassingen van verkenners- en zoekmachines die het hele net afgrazen en documenten, beeld en geluid wereldwijd toegankelijk maken (bijvoorbeeld door Google en YouTube).

II.2 De technische organisatie van het internet, het *world wide web,* de rol van klassieke internationale organisaties en nationale staten

Het internet is buiten de ITU-kaders gevormd en voornamelijk gebaseerd op privaatrechtelijke afspraken of op vrijwillige samenwerking. Tussen de meeste internetorganisaties bestaan geen hiërarchische relaties, al zijn er wel overlappende lidmaatschappen. Hoewel er een groot aantal partijen betrokken is bij het ontwikkelen en operationeel houden van het internet, functioneert het internet goed als platform voor de daarop draaiende toepassingen zoals browsers, zoekmachines, het *world wide web*, e-mail en vele andere.

De technische organisatie van het internet is voortgekomen uit wat globaal kan worden aangeduid als de internetgemeenschap, een verzameling clubs, voor een deel afkomstig uit de academische wereld.[14] Eén van de pioniers van het internet, David Clark, formuleerde het anarchistische *governance*-uitgangspunt in 1992 als volgt: *We reject presidents, kings and voting; we believe in rough consensus and running code.*[15]

Daarmee bracht hij tot uitdrukking dat het ging om een universele code (het internet protocol) waarover op hoofdlijnen overeenstemming bestond, zodat het *end-to-end* principe was verzekerd. Deze door iedereen gevoelde noodzaak tot consensus over de technische standaard is de drijvende kracht achter de internetgemeenschap, hoe

13 Carlota Perez, Technological Revolutions and Financial Capital, The Dynamics of Bubbles and Golden Ages, Cheltenham: Edward Elgar (EE), 2002.

14 Voor een geschiedenis van de vorming van de internetgovernance, zie Milton Mueller, Ruling the Root, Massachusetts: Massachusetts Institute for Technology 2002.

15 Idem, noot 11 op p. 91.

ingewikkeld die ook in elkaar zit. Dit is ook de constatering van de in de inleiding geciteerde Nye.[16]

In 1992 werd de nog steeds actieve Internet Society (ISOC) gevormd. Zij vormde het intellectuele centrum waarin mensen als Vint Cerf (een andere nog altijd actieve pionier van het internet) een centrale rol speelden en nog steeds spelen. ISOC beoogde de coördinatie van al deze informeel naast elkaar werkende groepen die hun gezag voornamelijk ontleenden aan het gezag van personen.[17] ISOC is nog steeds een juridische paraplu voor de personen die zich bezighouden met de ontwikkeling van standaarden.

Begin jaren negentig was er niet meer dan een tamelijk losse structuur: de internet-gemeenschap, die bestond uit Amerikaanse overheids- en academische organisaties en het Amerikaanse ministerie van Defensie. Daar kwam echter verandering in door het ontstaan van het *world wide web*, de grafische schil die het navigeren op het internet ingrijpend veranderde en de doorbraak van het internet betekende naar het grote publiek en de markt. Domeinnamen legden een link tussen het internet en beschermde merken en andere commerciële onderscheidingstekenen. Domeinnamen kregen zodoende een grote commerciële waarde. Het bedrijfsleven en internationale organisaties als de *World Intellectual Property Organization* (WIPO) en de *World Trade Organization* (WTO) kregen daardoor belangen bij het internet. Dit krachtenveld leidde tot institutionalisering van de zeggenschap over de *root*, het adresseringssysteem dat domeinnamen verbindt met IP-adressen. In dat proces kwam de *Internet Corporation for Assigned Names and Numbers* (ICANN) tot stand, een compromis tussen de internetgemeenschap en de voorstanders van meer traditionele belangen.

De wording van de Internet Corporation for Assigned Names and Numbers (ICANN)

De discussie was in hoeverre het domeinnamensysteem (DNS) in het Amerikaanse reguleringssysteem zou worden ingelijfd. In dit vrij intensieve lobbyproces kwam uiteindelijk ICANN tot stand. Dit werd in 1998 gedragen door de zogenoemde dominante coalitie, waarin oude en nieuwe spelers gezamenlijk optrokken tegen de Amerikaanse regering, die het DNS in de Amerikaanse invloedssfeer beoogde te houden. In 1998 kondigde de regering Clinton echter in een *White Paper* aan bereid te zijn een contract over DNS aan te gaan met een nieuwe non-profit rechtspersoon, gevestigd in de VS en met een internationaal bestuur, die het DNS zou gaan administreren. Het *White Paper* zag daartoe voorstellen van belanghebbenden tegemoet. Er moest dus een compromis worden gevonden tussen de Amerikaanse regering, internetclubs, belangrijke bedrijven (zoals IBM), belangenorganisaties van merkgerechtigden, de Europese Commissie en buitenlandse regeringen (met name Australië, Frankrijk, Japan). De organisatie zou moeten worden gebouwd rond de informele structuur voor de toewijzing van internetadressen, de *Internet Assigned Numbers Authority* (IANA). Gekozen werd voor een *non-profit corporation* naar Californisch recht, een rechtsvorm die in de VS veel wordt gebruikt voor charitatieve en onderwijsinstellingen. Eind 1998 gingen ICANN en het ministerie van Handel een *Memorandum of Understanding* aan, dat uiteindelijk heeft geleid tot de huidige opzet.

16 Joseph S. Nye, The regime complex for managing global cyber activities, Global Commission on Internet Governance Paper Series, no. 1, May 2014. Zie: <https://www.ourinternet.org>.

17 Milton Mueller, Ruling the Root, Massachusetts: Massachusetts Institute for Technology 2002, p. 94.

ICANN heeft een *Joint Project Agreement* en een contract met het Amerikaanse ministerie van Handel voor de toewijzing van internetadressen en het beheer van algemene *toplevel* domeinen (gTLD's). Het Amerikaanse ministerie van Handel is dus de formele band met het overheidsgezag, met daarnaast het *Governmental Advisory Committee* (GAC). Het GAC oefent geen overheidsgezag uit, zoals het Amerikaanse ministerie voor Handel dat kan doen.

De ICANN-structuur is wel gekarakteriseerd als *baroque in its complexity*, die de brede waaier weerspiegelt van belangen die worden geraakt door domeinnamenbeleid.[18] De *Internet Engineering Task Force* (IETF, zie bijlage I) en dergelijke hebben afgevaardigden in de commissies van ICANN, maar ze maken geen deel uit van dezelfde organisatie. Alle organisaties zijn autonoom. Er is immers geen hiërarchische relatie tussen al deze organisaties. Er kan dus inderdaad van een *multi agency*-model worden gesproken waarbinnen *multi stakeholders* zijn vertegenwoordigd.[19]

Het *Joint Project Agreement* is herhaaldelijk verlengd en gewijzigd, waarbij de autonomie van ICANN geleidelijk is vergroot, al houdt het ministerie van Handel een toezichthoudende rol.[20] In de *Affirmation of Commitments* tussen het ministerie van Handel en ICANN van 30 september 2009 is het *Joint Project Agreement* voor onbepaalde tijd verlengd.[21] Het Amerikaanse ministerie van Handel heeft zich ontwikkeld tot een soort procesbewaker. Alle betrokkenen konden daarmee leven, maar de band tussen ICANN en de VS is door de Snowdenaffaire onhoudbaar geworden (zie daarover verder paragraaf V.2.1).

II.3 Andere fora die bij de organisatie van en controle over het internet betrokken (willen) zijn

Een aantal landen probeert de greep van staten op het internet te vergroten, door het bestuur van het internet onder het gezag van multilaterale organisaties te brengen. Daarin hebben niet-statelijke actoren immers geen stemrecht. Momenteel vindt de discussie over de *governance* van het internet plaats in diverse fora, zowel binnen de VN als daarbuiten. In VN-kader zijn met name van belang de *World Summit on the Information Society*, het *Internet Governance Forum* en de ITU. Daarnaast vinden discussies plaats over de normatieve kaders voor het gebruik van het internet, bijvoorbeeld in de AVVN en in de Mensenrechtenraad. In deze discussies wordt ook het begrip *internetgovernance* gebruikt; daaraan wordt dikwijls een ruimere strekking gegeven dan de technische organisatie van het internet.

18 L.B. Solum, Models of internet governance, pp. 59-60, zie: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825>, geraadpleegd op 6 juni 2014.

19 Luciano Floridi, *The 4th Revolution, How infosphere is reshaping human reality*, Oxford: Oxford University Press 2014, Chapter 8: Politics: The Rise of the Multi-Agent System.

20 Lee A. Bygrave c.s., The naming game: governance of the Domain Name System, in: Lee. A. Bygrave and Jon Bing, Internet Governance, infrastructure and institutions, Oxford, Oxford University Press, 2009, pp. 151-153.

21 Zie: <http://www.ntia.doc.gov/page/docicann-agreements>, geraadpleegd op 5 juni 2014.

De World Summit on the Information Society[22]

In 1998 werd tijdens de *Plenipotentiary Conference* van de ITU een resolutie aangenomen over de wenselijkheid van een *World Summit on the Information Society* (WSIS). Het doel was onder andere om te komen tot een beter begrip van de informatiemaatschappij, daarvoor een strategisch plan te formuleren en rollen te definiëren voor de diverse partners om de informatiemaatschappij tot stand te brengen. In 2001 nam de AVVN een resolutie aan over een te houden Top, die uiteindelijk twee bijeenkomsten kende. In 2003 werd de eerste bijeenkomst gehouden in Genève. Daaraan namen ongeveer 11.000 personen deel, waaronder circa 50 staatshoofden of regeringsleiders. De overige deelnemers waren vertegenwoordigers van regeringen, internationale organisaties, niet-gouvernementele organisaties, het bedrijfsleven en de media. De agenda was zeer breed en omvatte onder andere de uitdagingen voor het tot stand brengen van en de toegang tot de informatiemaatschappij, vrijheid van meningsuiting en de *governance* van het internet. Daarnaast stelden diverse landen de controle van de Verenigde Staten over ICANN aan de orde. De uitkomst van deze top bestond uit twee documenten: een beginselverklaring en een actieplan. In de beginselverklaring staat onder andere dat beleidsvraagstukken ten aanzien van het internet behoren tot de soevereine competentie van staten, dat de private sector een belangrijke rol heeft in de technische en economische ontwikkeling van het internet, dat non-gouvernementele organisaties ook een belangrijke (maar ongespecificeerde) rol spelen en dat internationale organisaties coördinatie van beleidsvraagstukken ten aanzien van het internet kunnen faciliteren, alsmede de ontwikkeling van internationale standaarden. De beginselverklaring wijst dus specifieke rollen toe aan diverse actoren.

Tijdens deze bijeenkomst slaagden de deelnemers er niet in overeenstemming te bereiken over substantiële kwesties, waaronder een definitie van *internetgovernance*. Het punt waarbij het daarom draait is dat er landen zijn die meer over de inhoud van het internet te zeggen willen hebben. Daarbij werd dus de oude waterscheiding tussen inhoud en transport verlaten. Een meerderheid wil die echter wel handhaven. Daarom werd de Secretaris-Generaal van de VN gevraagd een *Working Group on Internet Governance* (WGIG) in te stellen. Het WGIG-rapport kwam uit vlak voor de tweede bijeenkomst van de WSIS, die in 2005 in Tunis werd gehouden.[23]

Ook in Tunis bleek het wederom bijzonder moeilijk overeenstemming te bereiken over inhoudelijke kwesties. ICANN kwam centraal te staan in de discussies. Een groep ontwikkelingslanden steunde het voorstel van WGIG om ICANN onder te brengen bij een orgaan van de VN. Dat zou betekenen dat alleen staten stemrecht zouden hebben. De VS gaf te kennen zijn historische rol in het beheer van domeinnamen niet snel op te zullen geven. De EU drong aan op een nieuw toezichtmechanisme voor ICANN. De bijeenkomst van de WSIS in Tunis resulteerde in twee documenten: de *Tunis Commitment* en de *Tunis Agenda for the Information Society*. Daarin stond onder andere een verzoek aan de Secretaris-Generaal van de VN tot de instelling van een *multistakeholder* beleidsdialoog: het *Internet Governance Forum* (IGF). Het IGF

22 Amanda Hubbard, Lee A. Bygrave, Internet governance goes global, in: Lee A. Bygrave and Jon Bing, Internet Governance, Infrastructure and Institutions, Oxford, Oxford University Press, 2009, pp. 213-235. Zie ook: Milton L. Mueller, *Networks and States*, The MIT Press, Cambridge, Massachusetts, 2010, pp. 55-80.

23 Zie: <http://www.wgig.org/docs/WGIGREPORT.pdf>.

is een forum waar de dialoog tussen regeringen, bedrijven en non-gouvernementele organisaties kan worden voortgezet, maar het kan geen bindende besluiten nemen of toezicht uitoefenen.

Het Internet Governance Forum

Het IGF heeft zich ontwikkeld tot een belangrijk forum waar vertegenwoordigers van belanghebbenden en de internetgemeenschap proberen consensus te bereiken over de beginselen van internet *governance*. Deze voortschrijdende consensus wordt vastgelegd in rapporten, zoals in het verslag van de bijeenkomst in Baku (Azerbeidzjan) in 2012.[24] Op die bijeenkomst was 33% van de deelnemers vertegenwoordiger van het maatschappelijk middenveld, 10% van de internetgemeenschap, 26% van nationale overheden, 6% van intergouvernementele organisaties, 17% van de private sector en 8% van de media. In september 2014 vond de negende conferentie in Istanbul plaats. Het door Nye gesignaleerde probleem van zeer uiteenlopende normen en waarden is een belemmering voor het bereiken van consensus over zaken die buiten de techniek liggen.

De International Telecommunications Union

Tijdens de ITU *World Conference on International Telecommunications*, die plaatsvond in december 2012 in Dubai, werd onder andere onderhandeld over een nieuwe versie van de *International Telecommunications Regulations* (ITR). De meeste westerse landen hebben het voorstel tot wijziging en de vijf daarop aansluitende resoluties niet ondertekend, maar de meeste Aziatische en Arabische landen wel, terwijl het beeld in Zuid-Amerika en Sub-Sahara Afrika gemengd is. De westerse landen hadden bezwaren tegen het voorstel omdat het ook controle op de toegang en communicatie over het internet behelsde. Hiermee lijkt de poging van de ITU om het internet te brengen onder het model van post en telefonie mislukt. Toch zal de ITU haar pogingen niet staken, omdat zij als internationale organisatie die niets over het internet te zeggen heeft, haar bestaansrecht dreigt te verliezen. Voor autoritair geregeerde landen als Rusland en China is de ITU een mogelijk instrument om de inrichting van het internationale internet te modelleren naar de strikte regimes die in eigen land gelden voor de inhoudelijke controle van internet.

World Wide Web Consortium (W3C)

Het internet (de technische infrastructuur) moet worden onderscheiden van het *world wide web*, waarmee het wel eens wordt verward. Wat ze met elkaar gemeen hebben is dat staten en belangenorganisaties proberen over beide controle uit te oefenen. Het door Tim Berners-Lee begin jaren negentig bedachte *world wide web* creëerde een nieuw massamedium.[25] Het domeinnamensysteem kreeg met name door dit openbare gebruik een sterke merkfunctie. Deze nieuwe onderscheidingsfunctie leidde tot een botsing met het bestaande systeem van merkenrechten.

24 Zie: <http://www.intgovforum.org/cms/documents/publications/177-igf-2012-baku-internet-governance-for-sustainable-human-economic-and-social-development/file>.

25 Tim Berners-Lee, Weaving the Web, New York: Harper Collins 1999; zie voor een uitvoerige analyse van de merkenrechtelijke functie ook Mueller 2002, hoofdstuk 8.

De groeiende economische betekenis van de domeinnamen bracht de coördinatie- en verdeelvraag scherper op de agenda. Alle belanghebbenden in dit spel gingen met elkaar in de slag; de Amerikaanse en Europese overheden, de 'internetwereld' en de 'oude' telecommunicatiewereld van de merkgerechtigden. De recente, lange discussies over de nieuwe algemene topdomeinen vormen daarvan een herhaling.

Het W3C is opgericht om de (technische) ontwikkeling van het *world wide web* te bevorderen, onder andere door standaarden te ontwikkelen. Het is geen rechtspersoon, maar opereert juridisch onder de vlag van vier academische instituten. Iedere organisatie en ieder individu kan lid worden. De leden zijn vooral bedrijven, academische instituten en overheidsorganisaties, die contributie betalen. De uitvinder van het *world wide web*, Tim Berners-Lee is nog steeds directeur van W3C.

II.4 De rol van de nationale staten: toegang tot het net en controle op de private toegangverschaffers

Nationale staten houden via de fysieke infrastructuur invloed op de toegang van gebruikers tot het internet en op de activiteiten van de daarbij betrokken dienstverleners, voor zover die (deels) op hun nationale grondgebied opereren. Zij kunnen proberen invloed uit te oefenen door bepaalde eisen te stellen aan de voorwaarden voor de toegang tot het netwerk en aan de aftapbaarheid van het netwerk, via wetgeving of informele arrangementen. Hier ligt ook de basis voor wat men wel de hernationalisatie of balkanisering van het internet is gaan noemen: de trend dat het internet en het wereldwijde web worden opgesplitst in regionale of nationale gebieden waar (samenwerkende) staten heer en meester zijn. Zo kunnen bindende politieke en rechtsbeslissingen in nationale jurisdicties wereldwijde dienstverleners dwingen hun diensten aan de regio of het nationale gebied aan te passen. Google doet dit bijvoorbeeld al vrijwillig. De zoekresultaten verschillen per taal, land of regio. In deze context rijzen bredere vragen over de mogelijkheid dat internationaal opererende ondernemingen met dominante posities in hun markten, zoals Google en Facebook, zich aan nationale jurisdicties onttrekken. Zij zijn echter wel onmisbare schakels in het wereldwijde communicatieproces geworden.

Begin en eindpunt van het internet liggen binnen de invloedssfeer van nationale en regionale jurisdicties vanwege de invloed die staten hebben op de fysieke laag. Staten kunnen derhalve hun juridische en politieke stempel drukken op het gebruik van het internet. Hier ligt ook de basis van conflicten over jurisdictie en normen, die onder meer de Snowdenaffaire tekenen. In autoritair geregeerde landen verschaft dit staten de macht om individuele communicaties te controleren, websites en blogs te reguleren en om diverse vormen van censuur toe te passen.

III Conceptuele vragen: privacy, vrijheid en grondrechten

Volgens de adviesaanvraag zijn het recht op privacy, het recht op bescherming van persoonsgegevens, het recht op vertrouwelijke communicatie en de vrijheid van meningsuiting voorbeelden van internetvrijheid. In dit hoofdstuk worden deze begrippen en daarmee verwante conceptuele vragen toegelicht.

III.1 Het grondrechtelijk systeem opgeschud

Het recht op eerbiediging van de persoonlijke levenssfeer

Het recht op eerbiediging van de persoonlijke levenssfeer (hierna: privacy) is een recht met vele facetten dat alle aspecten van de privésfeer van burgers beschermt. Dit loopt van de bescherming van de intimiteit en vrijheid van de eigen levenssfeer, het huisrecht (ruimtelijke privacy), de integriteit van het lichaam, het recht op gezinsleven en bescherming van communicatie (relationele privacy) tot aan alle informatie met betrekking tot de persoon (informationele privacy).[26] Hier wordt slechts opgemerkt dat veel van wat hieronder wordt opgemerkt over de ineenvloeiing van rechten, ook voor de ruimtelijke privacy geldt. Het huis is door de informatietechnologie van glas geworden, terwijl ook de intiemste levenssfeer niet meer ruimtelijk aldaar te lokaliseren is. De muren van het huis zijn door krachtige informatietechnologie doordringbaar geworden, terwijl de informatie over de persoon niet meer thuis in kasten wordt bewaard, maar in de *cloud* op een server. Het individu draagt met zijn *smartphone* of *tablet* overal alle persoonlijke informatie bij zich die een duidelijk inzicht geeft in zijn relaties, communicatie en dagelijkse contacten. De integriteit van het lichaam is niet meer beperkt door een zichtbare fysieke grens, omdat *bodyscanners* van afstand kunnen doordringen in die integriteit en omdat met het lichaam verknoopte techniek, zoals sensoren en applicaties die lichaamsfuncties meten, van een afstand kunnen worden afgeluisterd.[27]

(Informationele) privacy en de vrijheid van meningsuiting

Privacy en vrijheid van meningsuiting zijn deels complementaire, deels conflicterende rechten. Zij zijn complementair omdat zij de geuite gedachten en gevoelens van de persoon in de privésfeer beschermen, alvorens zij in de openbaarheid komen.[28] Zij zijn conflicterend waar geheime of privé-informatie in de openbaarheid wordt gebracht als met publicatie een algemeen belang is gediend. De rol van de overheid ziet in de eerste categorie op het bespioneren van iemands privégedragingen en meningen, in de

26 P. Blok, *Het recht op privacy*, Den Haag, Boom juridische uitgevers, 2002. B. Roessler, New Ways of Thinking about Privacy, In: Anne Phillips, Bonnie Honig and John Dryzek (eds) *Oxford Handbook of Political Theory*. Oxford: Oxford University Press, 2006. G. Overkleeft-Verburg, Commentaar op artikel 10 van de grondwet. In: E.M.H. Hirsch Ballin en G. Leenknegt (red.), *Artikelsgewijs commentaar op de Grondwet*, webeditie 2014. Zie: <http://www.nederlandrechtsstaat.nl>.

27 B.J. Koops, On legal boundaries, technologies, and collapsing dimensions of privacy, *Politica e Società*, 3(2), pp. 247-264.

28 Zie: E.J. Dommering e.a,. Informatierecht, Amsterdam: Otto Cramwinckel 2000.

tweede op bescherming van iemands privéleven en reputatie. Een te grote repressie van de overheid kan bovendien een *chilling* effect hebben op de individuele (geestelijke) ontplooiing: mensen durven dan ook in de privésfeer niet meer te communiceren wat zij denken.

Gedachten en gevoelens die niet in het openbaar zijn geuit, kunnen variëren van het persoonlijke geweten tot aan een uitwisseling van meningen tussen enkelen of binnen een besloten groep zonder dat de inhoud van de informatie of identiteit van de betrokkenen buiten die kring wordt onthuld. Ook de informatieverwerking in de privésfeer valt eronder, zoals het lenen, kopen en lezen van een boek of het bekijken van een film of het beluisteren van een geluidsdrager thuis of – anoniem – in de openbare ruimte (bioscoop of openbare leeszaal). Of het kan gaan om niet-gepubliceerde geschriften en eigen dataverzamelingen. Tegenwoordig moet men daarbij ook denken aan het stellen van zoekvragen aan zoekmachines of het raadplegen en downloaden van (multimediale) webpagina's. Een andere vorm van het privé tot uitdrukking brengen van een overtuiging is de geheime stemming bij verkiezingen en het anonieme stemresultaat. De voormalige Speciale Rapporteur voor de bevordering en bescherming van het recht op vrijheid van meningsuiting, Frank LaRue, heeft het verband tussen communicatievrijheid en privacy in zijn rapport van 17 april 2013 aan de Mensenrechtenraad als volgt verwoord:[29] '*Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a private sphere with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used.*'

Dit betekent dat voor LaRue privacy en vrijheid van meningsuiting onlosmakelijk met elkaar zijn verbonden. Hij schrijft: '*The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas.*'

De bescherming van vrije en vertrouwelijke uitwisseling van gedachten en gevoelens in de privésfeer kreeg met de organisatie van het postnetwerk een nieuwe dimensie. Ook die gedachten en gevoelens die over grote afstand en door tussenkomst van een derde (de posterijen) werden uitgewisseld tussen geadresseerde personen, zijn verzekerd van hetzelfde beschermingsniveau als wanneer die uitwisseling binnen een afgebakende plek (zoals het huis) plaatsvindt. Dat betekent dus een bescherming van het communicatiekanaal, welke bescherming zich ook uitstrekt tot de identiteit van de zender en de ontvanger: het briefgeheim. Deze bescherming is in de loop der tijd uitgebreid tot andere communicatiekanalen, zoals de telegraaf en de telefoon.[30]

De openbare meningsuiting wordt beschermd, omdat zij een kritische functie vervult bij de openbare waarheidsvinding, de openbare artistieke expressie en de openbare

29 A/HRC/23/40, paragraaf 22 en paragraaf 24.

30 Zie: W. Steenbruggen, Publieke dimensies van privé-communicatie. Een onderzoek naar de verantwoordelijkheid van de overheid bij de bescherming van vertrouwelijke communicatie in het digitale tijdperk, Amsterdam, Otto Cramwinckel 2009; E.J. Koops, Commentaar op artikel 13 van de grondwet. In: E.M.H. Hirsch Ballin en G. Leenknegt (red.), Artikelsgewijs commentaar op de Grondwet, webeditie 2014, <http://www.nederlandrechtsstaat.nl>.

democratische besluitvorming; alle kernwaarden van een open samenleving en een democratische rechtsstaat. Het Europese Hof voor de Rechten van de Mens beschouwt de vrijheid van meningsuiting daarom als de hoeksteen van de democratie.[31] Anonimiteit kan daarbij in zoverre een rol spelen, dat de bescherming van de identiteit het onbevangen uiten van een mening kan bevorderen. Het kan ook een beschermingslaag vormen in een land waar de vrijheid om in het openbaar zijn gedachten of gevoelens te uiten, niet wordt erkend of riskant is. De bescherming van de anonimiteit van klokkenluiders en in het algemeen van de bronnen van de pers zijn ook bedoeld om het onbevangen uiten van meningen te bevorderen.

De rechten op privacy en de vrijheid van meningsuiting vinden in Europa hun oorsprong in de 17de eeuw. Privacy had aanvankelijk vooral de vorm van gewetensvrijheid en een onschendbaar privaat eigendomsrecht. Deze begrippen kregen geleidelijk aan een positiefrechtelijke invulling in de constituties die aan het eind van de 18de en begin van de 19de eeuw werden opgesteld. Daarbij zag men het briefgeheim en het in de privésfeer gedachten kunnen uiten en vormgeven als het beginpunt van de openbare meningsuiting. Later zijn de rechten op privacy en de vrijheid van meningsuiting verder uit elkaar geraakt, omdat via het postkanaal ook puur persoonlijke mededelingen bescherming behoefden. Het briefgeheim werd daardoor een algemene bescherming van het geheim van het postkanaal en het geheim van de ongeopende brief. Het is naast het later opgekomen algemene privacyrecht een eigen positie blijven behouden als bescherming van het niet-openbare communicatiemiddel.

In het verlengde van de openbare meningsuiting ligt de toegang tot openbare informatiebronnen, die onontbeerlijk is om tot een verantwoorde meningsvorming te kunnen komen. In de tweede helft van de 20ste eeuw zette dit in het merendeel van de westerse democratieën een beweging in gang om tot wetten van openbaarheid van bestuur te komen, die overheden ertoe verplichten in beginsel alle informatie die voor bestuurlijke processen van belang is, openbaar toegankelijk te maken.

Privacyrecht en dataprotectie

In de loop van de 20ste eeuw is het privacyrecht een algemeen recht op bescherming van de persoonlijke levenssfeer geworden. Het is het recht om door de overheid en anderen met rust te worden gelaten. Het is dus de beschermingswal tussen enerzijds de burger, zijn eigen leven en dat van zijn naasten en anderzijds de samenleving en de staat. Het gaat daarbij niet zozeer om wat voor type informatie er over het individu wordt verkregen (bescherming van gedachten en gevoelens), maar om het feit *dat* er informatie over het individu zonder diens toestemming wordt *verzameld, opgeslagen, verwerkt of gedistribueerd*. Ook het *verzamelen* van gegevens over personen raakt daarbij al de privacy, omdat het een inmenging van de staat in het privéleven betekent.

Uit het privacyrecht ontwikkelde zich een dataprotectierecht, dat typisch het recht is van de welzijnsbureaucratie en de marketingeconomie. Net als bij de communicatie door middel van een netwerk, maakt het individu deel uit van bestuurlijke en economische netwerken, waarmee hij al dan niet persoonsgegevens (tot de persoon herleidbare gegevens) uitwisselt, die worden opgeslagen, bewerkt en gebruikt. Het bezit van persoonsgegevens verschaft de instantie die ze systematisch ordent en gebruikt, bestuurlijke of commerciële macht over de persoon op wie ze betrekking hebben.

31 Sunday Times t. Verenigd Koninkrijk, 26 april 1979, Series A, Vol. 30.

Dit was al zo in het papieren tijdperk, maar nam een enorme vlucht met de opmars van de computer en de informatietechnologie. Dit leidde in de tweede helft van de 20ste eeuw tot aparte wetgeving die het verzamelen, de opslag en het gebruik van persoonsgegevens reguleert. Binnen deze wetgeving kennen de zogenaamde gevoelige gegevens een verhoogd beschermingsregime; zo worden gegevens die samenhangen met iemands politieke en geloofsovertuigingen, maar ook met andere wezenlijke identiteitsaspecten zoals het seksuele leven of de gezondheid, zwaarder beschermd dan andere persoonsgegevens. Aan de andere kant genieten ook de door de pers verwerkte persoonsgegevens een bijzondere status, omdat niet alle regels met betrekking tot dataprotectie daarop van toepassing zijn.

Het dataprotectierecht heeft een zelfstandige plaats gekregen in het Handvest van de grondrechten van de Europese Unie, naast de bescherming van de persoonlijke levenssfeer. Het is een hybride recht dat de privacy beschermt en het gebruik van informatie door machthebbers reguleert.[32] Met privacy heeft het gemeen dat het zijn aanknopingspunt vindt in het begrip persoonsgegeven, dat wil zeggen tot de persoon herleidbare informatie. Waar het privacyrecht beoogt het individu zeggenschap te geven over de persoonlijke levenssfeer en deze aldus af te schermen van de buitenwereld, gaat het dataprotectierecht verder door het individu ook zeggenschap te geven over de persoonsgegevens die zich buiten de persoonlijke levenssfeer bevinden. Het beoogt gebruik van informatie door de macht te normeren (door de gebruiksdoelen te formuleren en eisen te stellen aan proportioneel verzamelen, bewerken en gebruiken) en transparant te maken (de over de persoon beschikbare informatie voor deze toegankelijk, controleerbaar en corrigeerbaar te maken).

Het dataprotectierecht neemt in belang toe, omdat het begrip persoonsgegeven vervaagt. Door de groeiende verzamel- en rekenkracht van de computer en de toenemende elektronische registratie van individuele bewegingen en gedragingen van burgers, wordt het steeds gemakkelijker uit grote hoeveelheden gegevens persoonlijke profielen van burgers te maken en voor machtsuitoefening te gebruiken. Deze gegevens kunnen zonder toestemming van de betrokken persoon zijn verzameld en hoeven op zich geen persoonsgegevens te zijn. Profielen kunnen de privacy bedreigen, omdat zij niet alleen gepersonaliseerde dienstverlening kunnen bevorderen, maar ook kunnen leiden tot discriminatie en beslissingen tot machtsuitoefening jegens iemand zonder dat er verder concrete aanwijzingen jegens het individu zijn.[33]

De groeiende praktijk van het verzamelen van gegevens is dus een steeds grotere bedreiging van de privacy. Op termijn tast dit het vertrouwen van de burger in overheid en organisaties steeds meer aan.

Verkeersgegevens

Individuele communicatie via netwerken kan slechts tot stand komen als het bericht van de verzender(s) de beoogde ontvanger(s) bereikt. Adressering is dus essentieel. Het adres en de afzender op de envelop vallen onder de zogeheten verkeersgegevens:

32 Zie: Lee A. Bygrave, Data protection law, approaching its rationale, logic and limits, The Hague, London, New York, Kluwer Law International, 2002.

33 M. van Otterlo, A Machine Learning Perspective on Profiling, in: M. Hildebrandt and K. de Vries (eds.), Privacy, due process and the computational turn, London, Routledge, 2013.

gegevens wie met wie wanneer communiceert, ter onderscheiding van de inhoud van communicatie. Tegenwoordig worden verkeersgegevens ook vaak aangeduid als metadata. Bij de brief werden ook de verkeersgegevens tot het briefgeheim in ruime zin gerekend (de postbode mag er kennis van nemen, maar het niet doorvertellen), ter bescherming van de identiteit van de verzender en de ontvanger. De posterijen hadden slechts een functionele relatie met het adres, in zoverre dat zij het adres moesten kunnen uitlezen om de brief te kunnen sorteren en bezorgen. Het bericht is van de adressering gescheiden door de dichtgeplakte enveloppe. Bij de organisatie van het netwerk en de centrales van de telefonie was dat tot op grote hoogte ook nog het geval, omdat bericht en adressering gescheiden circuits volgden.

Van oudsher is er over de betekenis van het briefgeheim in de Nederlandse literatuur discussie geweest of dit betrekking had op de inhoud (de brief) of ook op het geheim van het transport, door sommigen ook wel aangeduid als het post- en telecommunicatiegeheim in ruime zin.[34] Het Europees Hof voor de Rechten van de Mens (EHRM) heeft beide onder dat begrip geschaard bij de uitleg van het begrip *correspondence* in artikel 8 van het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), maar aan verkeersgegevens een lager beschermingsniveau toegekend, omdat zij niet betrekking zouden hebben op de inhoud van de communicatie.[35] Door ontwikkelingen in de elektronische communicatie is dat inmiddels achterhaald (zie paragraaf III.4.1).

III.2 Specifieke privacyvragen

Targeted surveillance, profilering, onzichtbaar registreren

Grondrechten zijn niet absoluut, omdat zij kunnen worden beperkt als zij conflicteren met andere rechten of belangen. Bij de openbare meningsuiting gaat het om bestrijding van onrechtmatige uitingen, zoals belediging, racisme, terrorisme en schendingen van de privacy. Bij niet-openbare uitingen gaat het bijvoorbeeld om het opsporen van strafbare feiten of het voorkomen van aanslagen op de maatschappelijke veiligheid of staatsveiligheid. Grondrechten mogen alleen worden ingeperkt indien er een duidelijke en voorspelbare grondslag in wetgeving is. Bovendien moeten de beperkingen nodig en proportioneel zijn voor wat betreft het middel, de tijdsduur en gebaseerd zijn op redelijke vermoedens omtrent concrete gevaarlijke gedragingen, ook als het gaat om de verrichtingen van inlichtingen- en veiligheidsdiensten.[36]

Een van de grootste risico's van het opstellen van profielen op grond van analyse van ongericht verzamelde metadata is dat beslissingen tot machtsuitoefening jegens iemand kunnen worden gebaseerd op een geconstrueerd profiel zonder dat er verder concrete aanwijzingen jegens het individu zijn. Het systeem van *checks and balances* verwordt dan tot een systeem van preventief beperken of zelfs uitschakelen van risicofactoren. Het gaat dan niet om *mass surveillance*, zoals bij cameratoezicht, maar om *targeted*

34 Zie: E.J. Dommering e.a Informatierecht, Amsterdam: Otto Cramwinckel 2000, pp. 76 e.v. en A.J.A. van Dorst, Het postgeheim, in: A.K. Koekkoek, W. Konijnenbelt en F.C.L.M. Crijns, Grondrechten. Commentaar op Hoofdstuk 1 van de herziene Grondwet. Nijmegen, Ars Aequi, 1982, pp. 279-297.

35 Malone t. Verenigd Koninkrijk, 2 augustus 1984, Series A, nummer 82.

36 EHRM, 1 juli 2008, Liberty e.a. t. Verenigd Koninkrijk, nummer 58243/00.

surveillance, het isoleren en volgen van groepen op basis van bepaalde kenmerken. De verschuiving van oorlogvoering tussen staten naar terreurbestrijding binnen de eigen staatsgrenzen heeft ertoe geleid dat een systeem van concrete beperkingen jegens individuen geleidelijk aan plaats maakt voor een systeem van vrijheidsbeperkingen voor risicogroepen en -categorieën. Het gevolg kan zijn dat iemand wordt gefouilleerd uitsluitend omdat deze persoon past in het profiel van een dader, zonder concrete verdenking tegen deze persoon.

Historische verkeersgegevens zijn van groot belang voor de bestrijding van misdaad. In een studie van het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC) over de Wet bewaarplicht telecommunicatiegegevens[37] wordt onder andere het gebruik beschreven dat opsporingsdiensten, het Openbaar Ministerie en de rechterlijke macht maken van verkeersgegevens. De studie is gebaseerd op literatuuronderzoek en interviews. Opsporingsdiensten maken zeer frequent gebruik van bijvoorbeeld historische gegevens over telefoonverkeer in een breed scala van misdrijven, vooral voor het lokaliseren van personen en het in kaart brengen van contacten. Dit kan ontlastend of belastend bewijs opleveren. In vonnissen wordt ook regelmatig verwezen naar dergelijke gegevens. Ten aanzien van internetverkeersgegevens stelt deze studie dat de gegevens die wettelijk moeten worden bewaard, niet meer aansluiten bij de huidige techniek en het internetgebruik. De Wet bewaarplicht gaat er nog vanuit dat internetgebruikers inloggen via een modem, terwijl tegenwoordig mobiel internet of inloggen via Wi-Fi zeer veel voorkomt. Verder verloopt tegenwoordig veel internetcommunicatie via aanbieders die niet in Nederland zijn gevestigd en dus niet onder de Wet bewaarplicht vallen.

Opsporingsdiensten gebruiken voor het volgen en lokaliseren van personen soms niet-geregistreerde sms-berichten (*stealth* sms) of vergelijkbare middelen. Het gebruik van dit soort middelen is niet te traceren, omdat zij niet in de dossiers terechtkomen. De locatie-informatie wordt vervolgens gebruikt als sturingsinformatie. Het bestaan ervan wordt ontkend (een *known unknown* in de terminologie van de voormalige Secretary of Defense Rumsfeld) of is hogerop in de hiërarchie niet eens bekend (een *unknown unknown* volgens diezelfde terminologie).

Dit roept vragen op ten aanzien van het privacyrecht, het recht op geheime elektronische communicatie, dataprotectierecht en daaraan gerelateerde wetgeving.

De rol en de positie van de inlichtingen- en veiligheidsdiensten

'If we want to preserve the liberties that define us as a democratic society, we must learn to live with risk.[38]

De hiervoor aangeduide problemen culmineren in de discussie over de inlichtingen- en veiligheidsdiensten, die hier afzonderlijk aandacht krijgt. De Snowdenaffaire heeft de discussie over de onafhankelijkheid en de effectiviteit van het toezicht op inlichtingen- en veiligheidsdiensten wereldwijd weer hoog op de politieke agenda gezet. In hoofdstuk V wordt daarop nader ingegaan.

37 G. Odinot, D. de Jong, R.J. Bokhorst en C.J. de Poot, De Wet bewaarplicht telecommunicatiegegevens. Over het bewaren en gebruiken van gegevens over telefoon- en internetverkeer ten behoeve van de opsporing, Meppel, Boom Lemma, 2013.

38 David Cole, Can the NSA be controlled?, in: New York Review of Books, 19 June 2014, p. 17.

Inlichtingen- en veiligheidsdiensten gaan bij de huidige stand van de techniek steeds meer ongericht gegevens verzamelen, die verder verwerkt worden naar tot groepen (profielen) en individuen herleidbare gegevens. Op dit moment doet de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) dit al met het opvangen van satellietsignalen in het kader van het SIGINT-programma (*signals intelligence*). Als die bevoegdheid in de toekomst zou worden uitgebreid tot kabelgebonden communicatie, zou dit kunnen betekenen dat de kabel en websites kunnen worden afgetapt. In paragraaf V.2.2 wordt hierop nader ingegaan. De AIVD kan op grond van artikel 28 van de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002) verkeersgegevens opvragen over gebruikers van Nederlandse telecommunicatiebedrijven, die zij op grond van de Wet bewaarplicht telecommunicatiegegevens moeten opslaan. Deze wet berust op een richtlijn die inmiddels door het Hof van Justitie van de Europese Unie (HvJ EU) onverbindend is verklaard.[39]

Deze bulkgegevens kunnen met buitenlandse bevriende inlichtingen- en veiligheidsdiensten worden gedeeld. De huidige Wiv 2002 bevat in artikel 59 lid 1 slechts een taakstellende bepaling ten aanzien van het onderhouden van contacten met buitenlandse diensten, zonder dat waarborgen ten aanzien van proportionaliteit en rechtsbescherming bij deze uitwisseling worden geformuleerd. De commissie Dessens heeft bepleit uitwisseling van gegevens met bevriende inlichtingen- en veiligheidsdiensten wettelijk te regelen.[40] Thans bestaan daarvoor alleen beleidsregels, die de uitwisseling laten afhangen van de mate waarin buitenlandse diensten voldoen aan criteria zoals democratische inbedding van die diensten en respect voor de mensenrechten. Daarin moet naar het oordeel van de AIV ook de rechtspositie van de eigen burgers worden beschermd met *safe harbour*bepalingen, gebruiksbeperkingen en toegang tot een rechter. In de kabinetsreactie op de evaluatie van de Wiv 2002 (het rapport van de commissie Dessens) schrijft de minister van Binnenlandse Zaken en Koninkrijksrelaties dat de uitwisseling van bulkdata met buitenlandse diensten zal worden onderworpen aan een systeem van ministeriële toestemming.[41]

Het EHRM heeft vastgesteld dat alleen al het verzamelen en opslaan van persoonsgegevens moet worden gezien als een ingreep in de privacy, die al dan niet gerechtvaardigd kan zijn als voldaan is aan de eisen van artikel 8 lid 2 van het EVRM.[42] Massale verzameling van ogenschijnlijk onschuldige gegevens kan een schending inhouden van de beginselen van legitimiteit, proportionaliteit en effectiviteit. Aangezien de gegevens in de inzamelfase in de praktijk vaak niet (meer) als persoonsgegevens worden gekwalificeerd, verliest de norm van dataminimalisatie tussen individu en staat

39 HvJ EU, 8 april 2014, C-293 (Digital Rights Ireland Ltd) en C-594/12 (Kärntner Landesregierung); zie over de gevolgen voor de Nederlandse wetgeving Kamerstukken II 2014-2015, 33870, nr. 3, <https://zoek.officielebekendmakingen.nl/dossier/33870/kst-33870-2?resultIndex=0&sorttype=1&sortorder=4 en de op 19 november 2014 gepubliceerde voorlichting daarover door de Afdeling advisering van de Raad van State, <http://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=287&summary_only=>.

40 Commissie Dessens, Evaluatie van de Wet op de inlichtingen- en Veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, december 2013, p. 119.

41 Tweede Kamer der Staten-Generaal, 33820, nr. 2, p. 7.

42 EHRM, 4 december 2008, S. en Marper t. Verenigd Koninkrijk, nrs. 30562/04 en 30566/04.

steeds meer aan betekenis. Dat maakt het des te noodzakelijker om de verwerkings-, gebruiks- en verspreidingsfase aan een scherpe normering en toezicht te onderwerpen. Dit is de kern van de discussie rond de inlichtingen- en veiligheidsdiensten.

Onafhankelijk toezicht op inlichtingen- en veiligheidsdiensten

Een van de belangrijkste vragen waarmee de samenleving wordt geconfronteerd is hoeveel risico zij bereid is te accepteren in het vinden van de balans tussen veiligheid en waarborging van grondrechten. In de theorievorming over *cybersecurity* wordt onderscheid gemaakt tussen enerzijds *precluded event security* en anderzijds *marginal security cost*. De eerste absolute veiligheidsnorm wordt gehanteerd voor bepaalde vitale systemen, zoals in de luchtvaart, maar is voor veel maatschappelijke systemen onaanvaardbaar hoog, bijvoorbeeld omdat de financiële kosten voor absolute veiligheid te hoog worden.[43] In dat geval wordt gekozen voor de tweede norm. Eenzelfde vraag moet worden gesteld bij het vinden van de balans tussen veiligheid en handhaving van de waarden van de rechtsstaat. Als het om veiligheid gaat, lijkt de samenleving het onbereikbare ideaal van *precluded event security* na te streven, waardoor de noodzakelijke rechtsstatelijke balans verstoord kan raken.

Een dergelijke tendens het begrip (on)veiligheid te definiëren als *precluded event security* en naar steeds verdergaande maatregelen te grijpen om alle risico's uit te sluiten, zou zelfs kunnen neerkomen op een risico voor de rechtsstaat, zij het van geheel andere aard dan via het internet voorbereide terreuraanslagen. In dat kader is de vraag relevant hoe een effectief en onafhankelijk toezicht moet worden georganiseerd, dat betrekking heeft op de rechtmatigheid en proportionaliteit.

Voor het behoud van de rechtsstatelijkheid is effectief en onafhankelijk toezicht op de geheime activiteiten van de inlichtingen- en veiligheidsdiensten essentieel.[44] Het langetermijnbelang dat daarmee is gediend, is het behoud van vertrouwen in de rechtsstaat. Voor het toezicht bestaan verschillende modellen, die vaak ook in combinatie worden toegepast. De interne controle is die van ministerieel toezicht, hetgeen moet uitmonden in parlementaire verantwoordelijkheid. Een bezwaar van dit systeem kan zijn dat de minister *captive* wordt van de beter geïnformeerde veiligheidsdienst, terwijl parlementaire controle is omgeven met geheimhouding, die zich slecht verdraagt met de gebruikelijke openbare parlementaire verantwoording. Extern bestuurlijk toezicht heeft het voordeel dat deze mede ziet op controle op de doelmatigheid, maar het nadeel is dat zij vaak uitmondt in niet-bindende adviezen. Van belang is ook de effectiviteit van de controle. Dit heeft betrekking op expertise, toegankelijke en volledige voorlichting en presentatie van voor- en nadelen.

In een democratische rechtsstaat moet de grondslag voor beperkingen op grondrechten niet alleen vastgelegd zijn in toegankelijke wettelijke normen, maar moeten de beperkingen die de overheid in het kader van een klemmend algemeen belang stelt aan de uitoefening van grondrechten ook onder een effectief en onafhankelijk toezicht staan.

43 M. van Eeten, Johannes M. Bauer, Emerging Threats to Internet Security: Incentives, Externalities and Policy Implications, Journal of Contingencies and Crisis Management, volume 17, Issue 4, pp. 221-232.

44 Zie daarover Hans Born en Marina Caprini (eds.), Democratic Control on Intelligence Services, Ashgate, Aldershot 2007 en zie ook: I. Cameron, National Security and the European Convention on Human Rights, Den Haag, Kluwer Law International 2000.

Het EHRM[45] heeft, net als de Parlementaire Assemblee van de Raad van Europa[46], een sterke voorkeur voor preventief rechterlijk toezicht. Ten aanzien van inlichtingen- en veiligheidsdiensten heeft het EHRM die eis van rechterlijk toezicht niet als een absolute voorwaarde gesteld, mits het toezicht anderszins voldoende onafhankelijk en effectief is.

Preventief (rechterlijk) toezicht omvat meer dan individuele gevallen, omdat inlichtingen- en veiligheidsdiensten ook op zoek zijn naar onbekende risico's. In die (collectieve) gevallen zou het toezicht zich moeten richten op de vraag of een bepaald gericht programma het minst ingrijpende alternatief is en op de feitelijke onderbouwing en voorspellende waarde van bepaalde profielen. Voorts kan preventief (rechterlijk) toezicht controle uitoefenen op de tijdsduur en modaliteit van een programma.

Bovendien kan preventief rechterlijk toezicht inlichtingen- en veiligheidsdiensten dwingen zowel hun programma's als hun concrete activiteiten beter te onderbouwen. Ook transparantie (zoals het publiceren van statistische gegevens en openbare verslaggeving) is een middel om programma's kritisch te kunnen volgen.

Het rapport van de commissie Dessens bespreekt in hoofdstuk 4.4 de externe controle op de Nederlandse inlichtingen- en veiligheidsdiensten, met name het toezicht door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), het parlement en de Algemene Rekenkamer.

In hoofdstuk 5 gaat de commissie Dessens uitvoerig in op de verschillende varianten van preventief toezicht in een aantal landen. De commissie bespreekt drie vormen van preventief toezicht op inzet van bijzondere bevoegdheden van inlichtingen- en veiligheidsdiensten.[47] De eerste variant houdt in dat de verantwoordelijke politieke ambtsdrager toestemming geeft, of een ambtenaar namens hem. Dit is de variant die Nederland en het Verenigd Koninkrijk hebben gekozen. Besluitvorming vindt vooral intern plaats en dat maakt de uitoefening van bevoegdheden kwetsbaar voor misbruik, volgens het EHRM. De commissie Dessens meent dan ook dat deze vormen van toezicht alleen kunnen functioneren als ze worden aangevuld met externe vormen van toezicht. Een tweede variant is voorafgaand advies van een onafhankelijke commissie. Deze variant bestaat in Duitsland, België en Frankrijk. De commissie Dessens meent dat een risico bij deze vorm van preventief toezicht is, dat het toezicht marginaal zal zijn en vooral gericht op procedurele aspecten. Voldoende bevoegdheden, een goede benoemingsprocedure, informatievoorziening en voldoende ondersteuning ziet de commissie Dessens als essentiële voorwaarden. Verder zal een dergelijke commissie permanent beschikbaar moeten zijn om snel te kunnen beslissen of een bijzondere bevoegdheid mag worden ingezet. Ook bestaat het risico dat de instantie teveel begrip gaat tonen voor de belangen van de diensten en te weinig oog heeft voor waarborgen voor burgers. De derde variant die de commissie Dessens onderscheidt is preventief

45 EHRM, 29 juni 2006, Weber & Saravia t. Duitsland, nr. 35623/05 onder verwijzing naar 41 in de Klass e.a. t. Duitsland, 6 september 1978, nr. 5029/71, § 41 en Malone t. Verenigd Koninkrijk, 2 augustus 1984, § 64, Series A, nr. 82.

46 Recommendation 1402 (1999) 1 van de Parlementaire Assemblee van de Raad van Europa, Control of internal security services in Council of Europe member states.

47 Commissie Dessens, Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, december 2013, pp. 95-100.

rechterlijk toezicht: een rechter moet een machtiging verlenen voordat een bijzondere bevoegdheid mag worden ingezet. Deze variant bestaat onder andere in Canada, de Verenigde Staten en Zweden. In Nederland bestaat deze variant alleen ten aanzien van het briefgeheim en zal ook worden ingevoerd voor inzage in telecommunicatiegegevens. Het toezicht wordt in de meeste landen uitgevoerd door één rechterlijke instantie, zodat informatie niet wijd verspreid hoeft te worden en deze rechters zich kunnen specialiseren.

De commissie Dessens stelt dat niet met zekerheid valt te zeggen of preventief rechterlijk toezicht effectiever is dan andere toestemmingsvereisten; daarvoor ontbreken de gegevens. De commissie Dessens merkt op dat een rechter zich niet zal bezighouden met de vraag of inzet van bijzondere bevoegdheden vanuit beleidsmatig oogpunt wenselijk is, maar met de juridische aspecten, zoals of inzet in redelijke verhouding staat tot het beoogde doel. Uiteindelijk concludeert de commissie Dessens dat het in brede zin invoeren van een externe preventieve toets op de inzet van de bijzondere bevoegdheden pas aan de orde komt als er geen andere manieren blijken te bestaan om het toezicht effectief te versterken, die beter binnen het bestaande stelsel zijn in te voegen. Alles afwegende kiest de commissie uiteindelijk voor toezicht achteraf, mits dit tijdig en effectief is en juridisch bindende aanbevelingen kan doen.

III.3 Het internet en de vrijheid van meningsuiting: nieuwe intermediairs, vervaging tussen openbaar en privé, commercialisering van de publieke sfeer en mobilisatie

Tot dusver is veel aandacht besteed aan de verschillende aspecten van de privé-communicatie omdat de adviesaanvraag daar een accent legt. Er zijn ook belangrijke vragen aan de orde als het gaat om de openbare communicatie op internet.

Intermediairs krijgen in het kader van de klassieke openbare en besloten communicatie bijzondere bescherming. Ook de boodschappers krijgen een voorkeursbehandeling: journalisten hebben een zwijgrecht over hun bronnen, omdat anonimiteit de openbare meningsvorming kan bevorderen. De publieke omroep werd gezien als een instrument ter bevordering van pluralisme; toegang voor minderheden werd bevorderd. Een breed cultuurbeleid waarborgde de instandhouding en toegankelijkheid van belangrijke informatiebronnen zoals openbare en wetenschappelijke bibliotheken. Uitgeverijen delen in deze voorrechten. Al deze intermediairs zijn in de loop van eeuwen in westerse landen vrijgemaakt van inhoudelijke overheidsbemoeienis.

Het internet heeft een nieuwe familie van belangrijke intermediairs gevormd, die deels de functie van de oude overnemen. De bescherming van de rol van deze intermediairs heeft zich nog niet vastgezet in recht en regelgeving. Voor zover het gaat om toegang tot het netwerk, de typische telecommunicatiefunctie, zijn er in de VS en de EU regels die de gelijke toegang voor dienstverleners en gebruikers beschermen. Dat gebeurt nu onder de vlag van het begrip netwerkneutraliteit. De internetdienstverleners die de informatie van en naar de gebruiker brengen, genieten in de EU een beperkte bescherming in de *cache*- en *hosting safe harbour*bepalingen in de E-commercerichtlijn.[48] Zij profiteren van dit elektronische communicatieregime doordat zij niet aansprakelijk gesteld kunnen worden voor de (illegale) inhoud van de informatie die zij in het kader van het transport kort opslaan of langer vasthouden om de opvraagbaarheid bij de gebruiker

48 Richtlijn 2000/31/EG.

te vergemakkelijken, mits zij maar op eerste aanmaning van een belanghebbende manifest onrechtmatige inhoud verwijderen, de zogenaamde *notice and take down*-procedure. De positie van de intermediairs die feiten en meningen produceren en doorgeven, zoals websites, is veel minder duidelijk, omdat zij zich tussen een pers- en telecommunicatieregime in bevinden. De positie van een belangrijke intermediair als de zoekmachine is nog het onduidelijkst. Enerzijds is deze ongebreideld verspreider en gebruiker van persoonsgegevens, anderzijds is deze steeds meer een essentiële schakel in het wereldwijd verschaffen van toegang tot informatiebronnen. Dat laatste maakt dat ze een eigen status moeten krijgen onder het statuut van de vrijheid van meningsuiting, maar zover is het echter nog lang niet.[49] Dit geldt ook voor alle intermediairs die zich erop toeleggen informatie systematisch te rangschikken en toegankelijk te maken, bijvoorbeeld door middel van hyperlinks, zoals gespecialiseerde zoekmachines, Wikipedia et cetera.

Bij de openbare media-uitingen en individuele uitingen op sociale media is het steeds moeilijker om de voor een uiting verantwoordelijke persoon te vinden, vanwege de fijnmazigheid en de voor de gemiddelde gebruikers ondoorzichtige organisatiestructuur van het internet. Dit brengt een verschuiving naar een collectieve verantwoordelijkheid van de intermediairs met zich mee, in die zin dat er een tendens is ze aansprakelijk te houden voor maatschappelijk ongewenste informatie die via hun platform wordt verspreid, of ze daar nu iets mee te maken hebben of niet.

Een andere ontwikkeling, die hiermee samenhangt, is dat er een nieuw type intermediair is ontstaan, namelijk de organisator van sociale media, die zich tussen de openbaarheid en het privégebruik bevindt. Voorbeelden zijn Facebook en YouTube. Ook hiervan is nog niet duidelijk of ze meer onder een telecommunicatieregime dan wel onder een mediaregime vallen. *Offline* blijkt niet één op één vertaalbaar naar *online*, dat eigen oplossingen vergt.

Deze nieuwe en machtige commerciële intermediairs zijn steeds meer functies van publieke media gaan overnemen, hetgeen ten koste gaat van pluriformiteit. De vormgeving van de publieke ruimte en het publieke debat is daardoor steeds meer geprivatiseerd. De publieke sfeer wordt bepaald door commercieel gedreven informatiepaden die door deze media worden getrokken, niet door de algemene belangen zoals die aan instellingen van publieke media ten grondslag liggen.

Van oudsher hebben massamedia ook een mobilisatiefunctie. Het internet en de daarop aangeboden sociale media hebben die versterkt en vele nieuwe dimensies gegeven. Iedere nieuwe ontwikkeling in de communicatietechnologie wordt ingezet voor emancipatoire doeleinden. Ten tijde van de val van de Muur was dat de fax. Later kwam de mobiele telefoon en e-mail. De demonstraties op de vrijheidspleinen in Europa (Occupy) en later in Turkije en het Midden-Oosten werden gedragen door de sociale media als Twitter en Facebook, vaak geflankeerd door daar handig op in spelende klassieke media zoals de Guardian en Al Jazeera. Deze nieuwe dimensie is ook zichtbaar bij de onthullingen van Assange en Snowden.

49 J. van Hoboken, Search Engine Freedom, On the implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, Alphen aan den Rijn, Wolters Kluwer Law & Business, 2012 (Information Law Series nr. 27). Zie ook de analyse van de Google-uitspraak in hoofdstuk V.3.1.

III.4 De relatie tussen rechtsbegrippen, techniek en soevereiniteit

Het internet (en de daarmee samenhangende ICT) confronteert ons met twee wezenlijke algemene vragen. In de eerste plaats de vraag of rechtsbegrippen en daarmee verbonden beschermingsnoties nog wel aansluiten op de onderliggende, door markt en informatietechnologie dynamisch voortgestuwde, werkelijkheid. In de tweede plaats de vraag wat de betekenis is van de soevereine natiestaat in de grenzeloze *cyberspace*.

III.4.1 Recht en techniek: communicatiegeheim, verkeersgegevens, beveiliging, intermediairs

Omvang communicatiegeheim

Deze vragen zijn onderliggende kwesties bij de Nederlandse worsteling met het communicatiegeheim. De Nederlandse regering heeft een voorstel tot wijziging van artikel 13 van de Grondwet (het brief- en telecommunicatiegeheim) naar de Tweede Kamer gestuurd op 16 juli 2014.[50] Dit voorstel wordt toegelicht met het argument dat het een hoognodige modernisering van deze bepaling brengt, zodat in de toekomst ook het e-mailgeheim wordt beschermd. Het telefoon- en telegraafgeheim wordt geschrapt en vervangen door de meer generieke term telecommunicatiegeheim, een begrip dat afwijkt van de EU-term elektronische communicatie. Met het gelijkstellen van het briefgeheim met het telecommunicatiegeheim verdwijnt echter ook het hoge beschermingsniveau van de klassieke brief. Deze was namelijk niet te openen door de inlichtingen- en veiligheidsdiensten zonder voorafgaande rechterlijke machtiging. Voor het bredere toepassingsbereik wordt het in de Grondwet gegarandeerde beschermingsniveau dus verlaagd. Dat betekent dat de grondwetgever er thans voor kiest het scheppen van waarborgen op het vlak van de rechtsbescherming en de proportionaliteit van de in te zetten middelen geheel te delegeren aan de wetgever.

Een verwant terugkerend discussiepunt in het kader van het telecommunicatiegeheim is of signalen die ongericht en onversleuteld worden verspreid, op hetzelfde beschermings niveau aanspraak kunnen maken als de communicatie over een afgebakend kanaal. De redenering is dat overal in de ether beschikbare signalen – die door iedereen kunnen worden opgevangen – op minder bescherming aanspraak kunnen maken omdat er bij het gebruik van dit medium geen *reasonable expectation of privacy* bestaat. Dit begrip is ontwikkeld door het Amerikaanse Hooggerechtshof, maar vormt in de VS steeds meer onderwerp van debat. Dit is de reden dat in de Nederlandse Wiv 2002 een lager beschermingsregime is opgenomen voor ongericht verspreide signalen. Het is de erfenis van de discussie over het Echelonproject – het door samenwerkende Angelsaksische inlichtingen- en veiligheidsdiensten volgen van open satellietverkeer op trefwoorden – dat aan het begin van de eeuw tot een publiek debat in Europa leidde.[51] De Nederlandse wetgever introduceerde daarnaast een zwaarder regime voor het afluisteren van kabelgebonden signalen, die mag alleen gericht worden afgeluisterd, dat wil zeggen dat de afzender bekend moet zijn. De commissie Dessens stelt voor dat onderscheid te laten vervallen. Deze aanpassing dreigt hetzelfde effect te hebben als bij het briefgeheim: de drempel voor het aftappen van de communicatie-infrastructuur wordt

50 Tweede Kamer der Staten-Generaal, 33 989, nrs. 1 en 2.

51 European Parliament, report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), 11 juli 2001.

verlaagd. In paragraaf V.2.2 wordt deze kwestie nader besproken.

In beide gevallen is dus sprake van een groter object van bescherming met een lager beschermingsniveau ten opzichte van het verouderde kleinere object van bescherming met het grotere beschermingsniveau. Drie voorbeelden kunnen duidelijk maken dat de technologie noopt tot herziening van de grondwettelijke en wettelijke normen.

Verkeersgegevens

Het eerste voorbeeld ziet op de status van verkeersgegevens, die in paragraaf III.1. bij het briefgeheim al ter sprake kwam. De uit 1984 daterende uitspraak van het EHRM (zie paragraaf III.1) is achterhaald omdat verkeersgegevens niet inhoudelijk neutraal zijn en veel over de 'kleur' van de contacten en de context (en daarmee de inhoud) van verzonden en ontvangen berichten kunnen vertellen, zeker als zij gecombineerd kunnen worden met informatie over bijvoorbeeld surfgedrag op het internet van de zender en de ontvanger van het bericht. Met het voortschrijden der techniek gingen de verkeersgegevens steeds meer vertellen over de verzenders en de ontvangers van de boodschap. Van oudsher vertelden zij iets over het tijdstip en de frequentie waarmee iemand met bepaalde personen contact zocht. In het tijdperk van de mobiele telefonie is daar de locatie van de verzender en ontvanger bijgekomen, omdat de ingeschakelde mobiele telefoon voortdurend contact legt met een fijnmazig systeem van zendmasten met specifieke ontvangstgebieden. In het internettijdperk is het aantal verkeersgegevens exponentieel toegenomen, die bovendien (tijdelijk) worden opgeslagen. En hier geldt de statistische *Big Data*-regel: hoe meer gegevens, hoe meer inzicht ze geven in de persoonlijke voorkeuren en aard van de activiteiten van de persoon en de aard van zijn of haar individuele contacten. Het onderscheid tussen de adressering en de inhoud vervaagt bij internetcommunicatie verder, omdat beide naadloos in elkaar overlopen zonder dat er een duidelijke beschermingswal (een dichtgeplakte enveloppe) tussen zit. Verkeersgegevens geven een indringend inzicht in iemands persoonlijke levenssfeer, ook als ze geen of weinig inzicht bieden in de inhoud van communicatie.[52] Niet alleen de verkeersgegevens laten sporen na op het internet waaruit persoonlijke gegevens zijn af te leiden, ook het internet-der-dingen zal leiden tot een toename van digitale gegevens die iets zeggen over de leefgewoonten en voorkeuren van internetgebruikers. Er zijn tal van andere metadata die van alles over personen kunnen zeggen.

Dit doet de vraag rijzen of en hoe dergelijke gegevens juridisch moeten worden beschermd. Het wetsontwerp tot wijziging van de Grondwet regelt dit probleem niet, maar laat het over aan de wetgever om invulling aan dit grondrecht te geven. Hoe men verkeersgegevens nu ook kwalificeert, een reden om ze op een relatief laag beschermingsniveau in te schalen is er niet.

Verwerking en beveiliging van persoonsgegevens

Het tweede voorbeeld ziet op de regeling van verwerking en beveiliging van persoonsgegevens. De dataprotectieregelingen zijn gebaseerd op het centrale begrip verwerking (*processing*). Hiervoor is betoogd dat het begrip persoonsgegeven steeds problematischer wordt omdat in de tijd van *Big Data* de persoon pas in beeld komt als

52 B.J. Koops en J.M. Smits, Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie, Wolf Legal Publishers, 2014.

het kwaad eigenlijk al is geschied. Een soortgelijk probleem doet zich voor bij het ruime begrip verwerking en de daarmee samenhangende beveiligingsplicht. Verwerking omvat in de gangbare juridische definitie computertechnisch ongelijksoortige grootheden, zoals verzamelen, opslag, en verspreiden, met daar tussenin alles dat de computer met de gegevens doet. Aanbieders van *cloud*diensten zijn verplicht om de gegevens bij hun dienstverlening adequaat te beveiligen, zodat hackers in beginsel geen toegang hebben tot de gegevens. Overheden kunnen gegevens uit de *cloud* opvragen en de dienstenaanbieder daarbij verplichten om gegevens te ontsleutelen. Gebruikers kunnen daar alleen iets tegen doen door zelf alle gegevens te versleutelen voordat ze naar de *cloud* gaan. Echter, weinig gebruikers doen dat, omdat ze vertrouwen op de beveiliging door de aanbieder, maar ook omdat het versleuteld opslaan in de *cloud* voor verschillende toepassingen inefficiënt is. Computers kunnen namelijk slecht rekenen met versleutelde gegevens, zodat de rekencapaciteit van de *cloud* niet meer gebruikt kan worden.[53]

De gaten in de beveiligingsplicht zijn wezenlijk, want het gaat om vitale belangen. De *cloud* wordt georganiseerd door overwegend Amerikaanse bedrijven en er bestaat een grote kans dat informatie die Nederlandse personen en instellingen aan de *cloud* toevertrouwen, zich in de Amerikaanse rechtssfeer bevindt. De gegevens zijn daarmee toegankelijk geworden voor Amerikaanse autoriteiten.[54] Daarbij zij aangetekend dat sinds de onthullingen van Snowden onzekerheid is ontstaan of inlichtingen- en veiligheidsdiensten achterdeurtjes in encryptietechnologie hebben ingebouwd. Een en ander betekent dat gebruikers de controle over gegevens dreigen te verliezen. Tijdens de Duitse bezetting werd een aanslag gepleegd op het Amsterdamse bevolkingsregister om de Duitsers te dwarsbomen bij het vervolgen en deporteren van leden van de Amsterdamse Joodse bevolking. Deze aanslag wordt in Nederland gezien als een eerste voorbeeld van een manier waarop burgers tegen de risico's van dataopslag in registers werden beschermd. Anno 2014 zou een dergelijke daad van verzet niet veel zin meer hebben, omdat ze via de *cloud* buiten het eigen territoir al voor een vreemde overheid toegankelijk zouden kunnen zijn.

Transport en inhoud

Het derde voorbeeld ziet op de begrippen van het mediarecht (wel verantwoordelijkheid voor de inhoud) en (tele)communicatierecht (geen verantwoordelijkheid voor de getransporteerde inhoud). In Nederland placht men te zeggen 'de PTT heeft geen boodschap aan de boodschap'. De technische werkelijkheid is echter complexer, omdat zij steeds meer is gebaseerd op de automatische ordening en agendering van inhoud, zonder dat degene die dat doet voor de inhoud van die boodschappen redactionele verantwoordelijkheid heeft. De zoekmachine doet meer dan transporteren, maar minder dan redigeren. Zij lijkt meer op een bibliotheek. Een wettelijke regeling die deze nieuwe intermediaire functie, die ligt tussen transport en redactie, niet erkent, legt verantwoordelijkheden waar zij niet horen en dreigt daardoor de essentiële functie die de

53 C. Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights. Note, European Parliament, 2013, p. 33.

54 Voor het eerst in Nederland in 2013 aan de orde gesteld door: J. van Hoboken, A. Arnbak en N. van Eijk, in: Obscured by the clouds. Zie: <http://www.ivir.nl/publications/vanhoboken/obscured_by_clouds.pdf>.

zoekmachine in het informatievoorzieningsproces heeft gekregen te schaden.[55]

Deze voorbeelden tonen aan dat het noodzakelijk is de relatie tussen de waarden die bescherming verdienen, te leggen naast de technische processen die plaatsvinden.

III.4.2 Nationale soevereiniteit: jurisdictie en grondrechtschendingen

Het internet legt in verhevigde mate een oud conflict in het internationale publiekrecht bloot, namelijk dat tussen de universele wereldgemeenschap van burgers en de (andere burgers uitsluitende) bescherming van eigen ingezetenen binnen het gezagsmonopolie van de natiestaat. Hoewel het internet in haar organisatie post-Westfaalse trekken vertoont, leert de Snowdenaffaire dat zij meer dan ooit tot een conflict tussen nationale en regionale rechtsgemeenschappen leidt.[56]

Op het internet is de productie, verspreiding en opslag van informatie niet meer aan plaats en tijd gebonden. De commerciële organisaties bedienen zich van wereldomspannende netwerken, waarin de beslissingen over waar wordt geproduceerd en over waar wordt opgeslagen door overwegingen van economische aard worden bepaald. De *cloud* is daarvan een voorbeeld. Bestuurlijke organisaties (zoals inlichtingen- en veiligheidsdiensten) gaan grensoverschrijdende samenwerkingsvormen aan waarin zij informatie met elkaar delen. Steeds vaker worden persoonsgegevensbestanden grensoverschrijdend gekoppeld. De wereldwijde opvraagbare webpagina's geven openbare media-uitingen een bereik dat zich uitstrekt tot ver buiten het nationale domein waarvoor ze oorspronkelijk veelal waren bedoeld. Daarnaast zijn internationaal georiënteerde elektronische internetmedia ontstaan.

In het algemeen opereren de nationale private dienstverleners in een duidelijk afgebakende nationale of regionale jurisdictie. Immers, de kantoren, fysieke infrastructuur en de ondersteunende diensten en apparatuur die de gebruiker met het internet verbinden, bevinden zich in een (of meer) specifieke jurisdictie(s). Dat bepaalt welke regels omtrent toegang, veiligheid en gebruik gelden voor een bepaalde gebruiker. Wereldwijde spelers, zoals Google, opereren in vele nationale markten, zodat niet altijd duidelijk is onder welk rechtsregime zij vallen. Dit alles leidt tot conflicten tussen verschillende nationale en regionale juridische en beleidsmatige beschermingsregimes van grondrechten, die nog niet zijn opgelost. Het Amerikaanse constitutionele recht is in tegenstelling tot het EVRM gebaseerd op bescherming van personen met de Amerikaanse nationaliteit (*we, the people*) en ingezetenen van de VS. Aangezien vele belangrijke intermediairs Amerikaans zijn en onder het Amerikaanse federale recht vallen, betekent dat dus dat informatie die door niet-Amerikaanse staatsburgers die geen ingezetenen zijn van de VS, in de *cloud* aan hen is toevertrouwd, geen aanspraak kunnen maken op bescherming onder het Amerikaanse recht. In de VS gaat de discussie rond de Snowdenaffaire dan ook voornamelijk over het feit dat Amerikaanse staatsburgers worden afgeluisterd en elektronisch werden gevolgd door de National Security Agency (NSA). Hoe dat met de uitspraken van het HvJ EU en het EHRM zal uitpakken, moet nog maar worden afgewacht. In hoofdstuk V.2.1 wordt het Amerikaanse recht ter zake nader toegelicht.

55 Zie ook III.3.

56 A. Linklater, The Transformation of political community. Ethical foundations of the post-Westphalian era, Oxford: Polity Press, 1998.

De vragen die hier opdoemen, zijn of burgers van andere nationaliteit binnen verschillende jurisdicties wel over een gelijkwaardige bescherming beschikken als waarover zij in eigen land of regio beschikken, in hoeverre nationale overheden maatregelen moeten nemen om het nationale of regionale beschermingsniveau ook buiten het eigen grondgebied te kunnen verzekeren, in hoeverre zij private dienstverleners in dat verband verplichtingen kunnen opleggen, en hoe dienstenaanbieders kunnen of moeten omgaan met tegenstrijdige of moeilijk verenigbare eisen vanuit verschillende jurisdicties ten aanzien van bepaalde groepen klanten. Een van de maatregelen die Europese overheden zouden kunnen treffen (Bondskanselier Merkel heeft het al geopperd) is dat vitale belangen worden beveiligd door mogelijkheden in te bouwen dat bepaalde informatie uitsluitend wordt verzonden via Europese infrastructuur en dat gegevens niet in een *cloud* worden opgeslagen die zich fysiek of rechtens buiten de Europese rechtssfeer bevindt. Het zijn interessante opties, maar technisch vermoedelijk niet of nauwelijks te realiseren. *Safe harbour*-overeenkomsten kunnen niet hetzelfde beschermingsniveau verzekeren om de hier en in de vorige paragraaf genoemde redenen. Ook het opleggen van verplichtingen aan bedrijven voor activiteiten die buiten de EU plaatsvinden is om die reden problematisch.

IV De belangrijkste juridische kaders

De grondrechtelijke waarden die hiervoor werden besproken krijgen gestalte in internationale en regionale verdragen, grondwetten en andere nationale wet- en regelgeving. Op mondiaal niveau zijn dat de VN-verdragen en -organen. Op Europees niveau zijn dat de verdragen en organen van de Raad van Europa en de EU. Alle lidstaten van de EU zijn ook lid van de Raad van Europa, maar de Raad van Europa bestrijkt veel meer landen (bijvoorbeeld Rusland en Turkije). Een organisatie die met niet-juridische instrumenten in Europa veel aan het internet doet is de Organisatie voor Veiligheid en Samenwerking in Europa, maar die blijft hier verder buiten beschouwing.[57]

IV.1 De VN

De Universele Verklaring van de Rechten van de Mens en de resoluties van de AVVN en de Mensenrechtenraad bevatten algemeen gedeelde normen en waarden. Het belangrijkste mondiale verdrag ten aanzien van internetvrijheid is het Internationaal Verdrag inzake burgerrechten en politieke rechten. Het speelt in de regio Europa minder een rol omdat de normen van dit verdrag ook zijn opgenomen in het EVRM en het Handvest van de grondrechten van de Europese Unie, die krachtiger handhavingsmechanismen kennen.

In juli 2012 heeft de Mensenrechtenraad een resolutie aangenomen *The promotion, protection and enjoyment of Human Rights on the Internet* (A/HRC/20/L.13), waarin het accent meer lag op de vrijheid van meningsuiting. De resolutie bevestigt onder andere dat mensen *online* dezelfde rechten hebben als *offline*, roept staten op toegang tot internet te bevorderen en verzoekt de Speciale Rapporteurs deze kwesties te betrekken bij de uitoefening van hun mandaten.

Ook in de VN zijn privacy en internet door de Snowdenaffaire hoger op de agenda gekomen. Op 18 december 2013 aanvaardde de AVVN unaniem de resolutie *The right to privacy in the digital age*,[58] die was ingediend door Brazilië en Duitsland. De resolutie bevestigt dat rechten *offline* ook *online* gelden, in het bijzonder privacy. In de resolutie worden staten opgeroepen om nationale wetgeving in lijn te brengen met internationale verplichtingen, een eind te maken aan illegale activiteiten en toezicht op inlichtingendiensten te versterken. Verder wordt de *UN High Commissioner for Human Rights* gevraagd een rapport voor te leggen aan de 69ste zitting van de AVVN (september-december 2014) over de bescherming van het recht op privacy in de context van nationaal en extraterritoriaal toezicht op communicatie, interceptie en verzameling van persoonlijke gegevens. Eind juni 2014 heeft de *UN High Commissioner for Human Rights* een rapport uitgebracht, waarin het internationaal recht ten aanzien van de bevordering en bescherming van het recht op privacy wordt uiteengezet. Het rapport heeft vooral binnen de internetgemeenschap grote aandacht getrokken, omdat daaruit blijkt dat veel landen niet voldoen aan de daarin ontwikkelde proportionaliteitsbeginselen. Het rapport concludeert in paragraaf 47 dat het internationaal recht ten aanzien van mensenrechten een duidelijk en universeel raamwerk biedt voor de bevordering en bescherming van het

57 Zie: <http://www.osce.org/what/media-freedom>.

58 A/C.3/68/L.45.

recht op privacy, ook in de context van binnenlandse en extraterritoriale surveillance, de onderschepping van digitale communicatie en de verzameling van persoonsgegevens. De praktijk in vele staten vertoont echter een gebrek aan adequate nationale wetgeving en/of afdwinging, zwakke procedurele waarborgen en ineffectief toezicht. Dat heeft bijgedragen aan een gebrek aan verantwoording voor arbitraire of onwettige inbreuken op het recht op privacy.[59]

In hoofdstuk II van dit advies is kort aangegeven welke activiteiten met betrekking tot het internet vanuit de VN-organisaties worden ondernomen. De ITU speelt steeds minder een rol van betekenis. Het IGF vervult daarentegen een belangrijke rol, die zich verder moet ontwikkelen.

IV.2 De Raad van Europa

IV.2.1 Het Comité van Ministers en de Parlementaire Assemblee

Zowel het Comité van Ministers als de Parlementaire Assemblee van de Raad van Europa hebben diverse verklaringen en aanbevelingen aangenomen inzake internetvrijheid.[60] In het algemeen kan worden opgemerkt dat deze de bijdrage van ICT aan de vrijheid van meningsuiting en het recht op informatie onderschrijven en wijzen op de keerzijde, namelijk dat ICT ook kan worden gebruikt voor censuur. Verder wordt gesteld dat het recht op vrijheid van meningsuiting, informatie en communicatie gelden onafhankelijk van het gekozen medium. Het maakt geen verschil of deze rechten worden uitgeoefend op digitale media of op andere media. Ook zijn bijvoorbeeld verklaringen en aanbevelingen aangenomen over openheid en toegankelijkheid en het gebruik van internetfilters. Vanzelfsprekend zijn deze politieke verklaringen en aanbevelingen van belang, zeker als ze neerslaan in verdragen en wetgeving. In het bestek van dit advies voert het echter te ver in te gaan op elke afzonderlijke verklaring of aanbeveling.

IV.2.2 Het Europees Hof voor de Rechten van de Mens

Het EHRM doet uitspraken over de interpretatie van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), die bindend zijn voor de lidstaten van de Raad van Europa. Hieronder worden enige zaken besproken met bijzondere relevantie voor internetvrijheid.

Artikel 10 EVRM

Het EHRM heeft op basis van een verdragsdynamische interpretatie artikel 8 en 10 EVRM naar de eisen van de tijd en de stand van de techniek uitgelegd. Daarbij spelen de resoluties en verklaringen van de Assemblee en de Raad van Ministers een rol. Deze uitspraken zijn ook leidend voor de interpretatie van het Handvestvan de grondrechten van de Europese Unie. Het EHRM heeft zich herhaaldelijk uitgelaten over de essentiële rol die de pers (daaronder begrepen de elektronische massamedia) voor de democratie spelen. Een aantal uitspraken vraagt daar de aandacht.

59 Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014.

60 Bijvoorbeeld de Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society (CM(2005)56 final of 13 May 2005), Recommendation CM/Rec(2007)16, Recommendation CM/Rec(2007)11, Recommendation CM/Rec(2008)6, Recommendation CM/Rec(2012)3.

Van belang is de zaak Yildirim (EHRM 18 december 2012, appl. 3111/10). Op 23 juni 2009 gaf de Turkse Denizli Strafrechtbank op grond van paragraaf 8 (1)(b) van de Turkse wet nr. 5651, die publicaties op het internet reguleert en internetdelicten beoogt te bestrijden, het bevel een site te blokkeren waarop publicaties waren te vinden die beledigend waren voor de nagedachtenis van Atatürk. Deze site werd gehost door sites.Google.com. Het bevel werd gegeven in het kader van een procedure tegen de eigenaar/exploitant van de site. Het Directoraat van de Telecommunicatie werd met de uitvoering van het bevel belast en dit blokkeerde de toegang in Turkije tot sites.Google.com, omdat dit de enige effectieve manier zou zijn om de toegang tot de voor wijlen Atatürk beledigende site onmogelijk te maken. Daarmee werd echter de toegang tot alle andere sites op sites.Google.com ook afgesneden in Turkije, waaronder die van de heer Yildirim. De Turkse rechters achtten dat de logische en daarom aanvaardbare consequentie van het doel van het oorspronkelijke bevel, namelijk het stoppen van verdere beledigingen van Atatürk op het internet.

Het Hof oordeelt dat de afsluiting, waardoor niemand meer bij de site van Yildirim kon (dus ook hij zelf niet), in strijd was met artikel 10 van het EVRM. Het Hof verwijst in het vonnis naar alle relevante Europese en VN verklaringen en resoluties over internetvrijheid. Hoewel daaruit als leidend beginsel naar voor komt dat *prior restraint* niet is toegestaan, houdt het Hof vast aan zijn opvatting dat de Conventie geen absoluut censuurverbod bevat. Overweging 64 luidt: '*The Court considers that such prior constraints are not necessarily incompatible with the Convention as a matter of principle. However, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power*.'

De klager in deze procedure die ten gevolge van deze maatregel geen toegang meer had tot zijn website, kreeg gelijk. Dit betekent dat het Hof de vrije toegang tot het internet onder de bescherming van artikel 10 heeft gebracht. Van bijzonder belang voor internetvrijheid is de overweging 67 waarin het Hof oordeelt dat het blokkeringsbevel in strijd is met paragraaf 1 van artikel 10 EVRM dat uitdrukkelijk zegt dat de vrijheid geldt ongeacht grenzen. Het Hof refereert daarbij aan overweging 62 in de Ekinzaak[61] waarin het Hof het verbieden van buitenlandse publicaties veroordeelde. Dat betekent dat de plaats van vestiging van de *hosting*dienst niet relevant is, maar wel de plaats waar de toegang tot het wereldwijde web effectief wordt geblokkeerd. Ligt die in een staat die lid is van de Raad van Europa, dan is het Verdrag van toepassing. Omgekeerd zal een ingezetene van een ander land niet kunnen klagen over uitingen in een land dat lid is van de Raad van Europa waartoe hij via het internet toegang heeft.[62] In een vonnis van 11 december 2006 in de zaak Ben El Mahi v. Denmark, (appl. 5853/06) betreffende een klacht van een Marokkaanse ingezetene tegen Denemarken werd de klacht niet-ontvankelijk verklaard omdat Denemarken geen rechtsmacht over de klager uitoefende. Dit vonnis betrof de kwestie in Denemarken rond de publicatie van cartoons met afbeeldingen van de profeet Mohammed. Op dit moment is nog onbeslist wat het geval is als de gevolgen van schendingen van grondrechten doorwerken in gebieden waarover de Raad van Europa rechtsmacht heeft, worden gepleegd in een land dat geen lid is van de Raad van Europa. Die vraag is door de Snowdenaffaire bijzonder actueel geworden.

61 Annotatie van E.J. Dommering bij de zaak Vereniging Ekin t. France, no. 39288/98, EHRM, 17 juli 2001, in: NJ 2002, 444.

62 N. Vajic en P. Voyatzis, The internet and freedom of expression and the ECHR's evolving case-law, in: Joseph Casadevall e.a. (red.), Freedom of Expression, Oisterwijk, Wolf Legal Publishers, 2013, p. 403.

Burgers in een land dat lid is van de Raad van Europa, die via het internet een schending van in het verdrag gegarandeerde rechten ondervinden, kunnen dus de bescherming van hun recht bij de nationale en Europese rechter inroepen. Als deze zich bevoegd acht en een schending constateert, is daarmee nog niet gezegd dat een dergelijke beslissing in een land dat geen lid is van de Raad van Europa (bijvoorbeeld de VS), zal worden erkend.

Op 6 juli 2014 hield de *Grand Chamber* een hoorzitting in de zaak Delphi/Estonia (appl. 64569/09) waarin het draait om de aansprakelijkheid van een *Internet Service Provider* voor de inhoud van de informatie die via het internet wordt aangeboden. Mogelijk dat het EHRM zich in die zaak in meer algemene zin zal uitlaten over de rol van het internet in de democratie.

Artikel 8 EVRM

Het EHRM heeft de procedurele waarborgen van het dataprotectierecht ontwikkeld vanuit artikel 8 (Recht op eerbiediging van privéleven, familie- en gezinsleven), door de in artikel 8 gelezen positieve verdragsverplichting tot nationale waarborgen tegen schending in het leven te roepen.[63] In paragraaf III.1 is besproken dat het Hof verkeersgegevens onder het bereik van artikel 8 heeft gebracht.[64] Later deed het dat ook met e-mail.[65] Verder is het Hof zeer expliciet dat het enkele verzamelen van gegevens is aan te merken als een privacy inbreuk.[66]

In het kader van *mass surveillance* wint de beslissing in de zaak Liberty aan actualiteit.[67] Deze zaak begon in de jaren negentig in het Verenigd Koninkrijk toen het Britse ministerie van Defensie alle telecommunicatie tussen Dublin en Londen begon af te tappen. De klacht betrof in het bijzonder dat de telefoongesprekken waren gefilterd volgens geheime filtercriteria en zonder dat er een behoorlijk afluisterbevel bestond. Deze klacht werd door het Hof gehonoreerd. Het afluisterproces ging in de volgende fasen in zijn werk. Eerst werd een afluisterbevel uitgevaardigd waarin de te onderscheppen verbindingen werden aangewezen. Dat kon heel breed zijn: bijvoorbeeld alle zeekabels die in het Verenigd Koninkrijk aan land komen. Daarna vaardigde de minister van

63 De zaak Gaskin, EHRM 7 juli 1989, Series A nr. 160, NJ 1991, 659 met annotatie van E.J Dommering. In 1981 kwam het Verdrag inzake de persoonsgegevensbescherming van de Raad van Europa tot stand dat de algemene beginselen van persoonsgegevensverwerking vastlegt: verzameling, opslag, verwerking, gebruik en verspreiding slechts met doelgebonden toestemming of een gerechtvaardigd doel, proportioneel (niet meer en niet langer dan noodzakelijk voor het doel waarvoor ze zijn verzameld), correct en transparant (inzage- en correctierecht). Dit verdrag heeft model gestaan voor veel nationale wetten in de Raad van Europalanden en de later door de EU opgestelde richtlijnen.

64 Malone t. Verenigd Koninkrijk, 2 augustus 1984, Series A, nr. 82, zie ook: NJ 1988, 534 met annotatie van E.J. Dommering.

65 Copland t. Verenigd Koninkrijk, 3 april 2007, nr. 62617/00, zie ook: NJ 2007, 617 met annotatie van E.J. Dommering.

66 S. en Marper t. Verenigd Koninkrijk, 4 december 2008, nrs. 30562/04 en 30566/04.

67 EHRM, 1 juli 2008, Liberty e.a. t. Verenigd Koninkrijk, nr. 58243/00. NJ 2010, 324, met annotatie van E.J. Dommering.

Binnenlandse Zaken een certificaat uit waarin omschreven werd welke categorieën informatie mochten worden onderschept via de aangewezen communicatiemiddelen. Vervolgens werden filtersystemen geïnstalleerd, zoekmachines die op vooraf ingestelde trefwoorden of combinaties daarvan de communicaties onderschepten. De volgende stap was het opschonen van de op trefwoorden gefilterde communicaties, zoals het verwijderen van namen of het verwijderen van details die buiten het opsporingsdoel vielen.

Zoals meestal in dit soort zaken, staat het Hof lang stil bij de vraag of de wettelijke regels en de praktijk wel voldoen aan het criterium dat de wet toegankelijk moet zijn en op voorzienbare wijze wordt toegepast, dat wil zeggen of de praktijk in overeenstemming met de wet is. De zaak spitst zich toe op de voorzienbaarheid van de wettelijke beperking (*in accordance with the law*). De criteria daarvoor heeft het Hof opgesomd in de paragrafen 93-95 van een ontvankelijkheidsbeslissing in de zaak Weber en Saravis, EHRM 29 juni 2006, appl. 54934/00, in welke zaak het eveneens ging om het onderscheppen van communicaties volgens een trefwoordensysteem.[68] In overweging 62 in deze zaak worden die overwegingen letterlijk geciteerd. Het Hof heeft de criteria ontwikkeld op basis van individuele communicatieonderscheppingen. Zij vormen een vijfstappentoets die er als volgt uit ziet:

1. Bestaat er een definitie van de categorieën van personen die mogen worden afgeluisterd?
2. Is de duur van het afluisteren beperkt?
3. Is er een vastgelegde procedure hoe gegevens mogen worden opgeslagen, gebruikt en onderzocht?
4. Liggen de voorzorgsmaatregelen vast die bij communicatie van de gegevens aan derden in acht moeten worden genomen?
5. Onder welke omstandigheden mogen of moeten de gegevens worden vernietigd?

Dit zijn algemene regels die het Hof heeft geformuleerd naar aanleiding van afluisteren, zodat zij niet onverkort op elke situatie kunnen worden toegepast. De situaties kunnen variëren van waarneming en opslag met elektronische middelen van de beeltenis van een persoon (bewakingscamera's in de cel),[69] opslaan van gegevens over iemands levenspatroon en sociale uitingen, de registers van de inlichtingen- en veiligheidsdiensten,[70] waarneming en opslag van iemands (elektronische) communicatiehandelingen (zowel de inhoud als waar en met wie).[71]

Het Hof beslist in de Liberty-zaak dat de vijfstappentoets ook van toepassing is op *strategic monitoring*: '*The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing*

68 Die regels zijn overigens ook reeds te vinden in de Huvig en Kruslin-arresten, maar waren toen toegespitst op individuele vormen van monitoring. Zie ook: NJ 1991, 523, met annotatie van E.J. Dommering.

69 Perry t. Verenigd Koninkrijk, nr. 63737/00, EHRM, 17 juli 2003 Zie ook: NJ 2006, 40, met annotatie van E.J. Dommering.

70 Segerstedt-Wiberg and others t. Zweden, nr. 62332/00, EHRM 6 juni 2006. Zie ook: NJ 2009, 449 met annotatie van E.J. Dommering.

71 Copland t. Verenigd Koninkrijk, 3 april 2007, nr. 62617/00, zie ook: NJ 2007, 617 met annotatie van E.J. Dommering.

the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.'

In september 2013 legden verschillende mensenrechtenorganisaties rechtstreeks aan het Europese Hof de vraag voor of de praktijk van de Britse geheime dienst toelaatbaar is om in het kader van de samenwerking met de NSA op grote schaal trans-Atlantisch verkeer te onderscheppen ten behoeve van de NSA of te doen onderscheppen door de NSA.[72] In deze zaak is het afwachten of het Hof de vijfstappentoets zal aanscherpen, door ook materiële onderbouwing van de noodzaak van een programma te verlangen.

IV.3 De Europese Unie

IV.3.1 Algemeen

De EU heeft op het gebied van internetvrijheid normen ontwikkeld, vanuit de in de Europese rechtsorde verzekerde vrijheid van goederen en diensten, de *acquis communautaire* van aan de nationale rechtsorden gemeenschappelijke constitutionele normen en waarden en, na de vaststelling en ratificatie daarvan, het Handvest van de grondrechten van de Europese Unie. Deze normen beogen nationale wetgeving van de EU-lidstaten te harmoniseren. Op grond van artikel 53 van het Handvest is de uitleg daarvan door het HvJ EU gekoppeld aan de rechtsontwikkeling binnen het EHRM. Kort gezegd kan worden vastgesteld dat de harmonisering op het gebied van vrijheid van meningsuiting gebrekkig en gefragmenteerd is. Op het gebied van techniek en privacy is dat in nog sterkere mate het geval.

De elektronische communicatie

De harmonisatie van de techniek heeft zich, na een klassieke start die geheel was gebaseerd op de telefonie (het *Open Network Provison*-kader), geleidelijk ontwikkeld tot een volledige harmonisatie van een pakket regels dat elektronische communicatie en communicatiediensten omvat, maar niet de diensten die op de inhoud betrekking hebben.[73] Dit pakket zal uiteindelijk ook een plaats moeten krijgen in een verordening.[74] Op het gebied van de privacy zijn twee richtlijnen vastgesteld, namelijk de richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[75] en de richtlijn betreffende privacy en elektronische communicatie.[76] Op de laatste is vervolgens een uitzondering gemaakt door langere opslagtermijnen toe te staan van verkeersgegevens die verband houden met orde en veiligheid. Deze gegevens moesten langer worden opgeslagen dan uit het doelbeginsel voortvloeit. Dat is vastgelegd in de dataretentierichtlijn. Deze is echter onverbindend verklaard in april 2014, zodat

72 De zaak Big Brother Watch and others, appl. 58170/13, zie: http://www.echr.coe.int/Documents/CLIN_2014_01_170_ENG.pdf.

73 Considerans 5 van de Kaderrichtlijn 2002/21/EG.

74 COM/2013/0627 (def)-2013/0309 (COD).

75 Richtlijn 95/46/EG, 24 oktober 1995.

76 Richtlijn 2002/58/EG, 12 juli 2002.

de hierop gebaseerde nationale dataretentiewetten moeten worden herzien.[77] Op basis van de toenmalige Derde Pijler is een Kaderbesluit vastgesteld dat ziet op de gegevensbescherming in het kader van de politiële en justitiële samenwerking in strafzaken. Dit pakket moet voor wat betreft de algemene dataprotectiebepalingen geharmoniseerd worden in een verordening. Het Kaderbesluit moet worden vervangen door een richtlijn.[78] Dit samenstel van regels heeft betekenis voor de internetvrijheid.

Een nieuw hoofdstuk vormt het Handvest van de grondrechten van de Europese Unie dat het HvJ EU immers verplicht de toepassing van primair en secundair Unierecht te toetsen aan de grondrechten van het Handvest en ook door lidstaten in acht moet worden genomen op terreinen binnen de werkingssfeer van het Unierecht. Een goed voorbeeld daarvan is de Scarlet/Sabambeslissing,[79] waarin het Hof de uitoefening van het verbodsrecht heeft gebaseerd op de auteursrechtrichtlijn in de informatiesamenleving.[80] In overweging 45 stelt het: 'de nationale autoriteiten en rechterlijke instanties moeten bij het vaststellen van maatregelen ter bescherming van auteursrechten een juist evenwicht verzekeren tussen de bescherming van deze rechten en de bescherming van de grondrechten van personen die door zulke maatregelen worden geraakt.' Deze afwegingen, die nauw raken aan de vrije toegankelijkheid van het internet, hadden een voorgeschiedenis in het wetgevende traject bij de lobby tegen het *Anti-Counterfeiting Trade Agreement* dat rechthebbenden vergaande bevoegdheden beoogde te geven om gebruikers van illegale inhoud de toegang tot het net te ontzeggen.

De vrijheid van meningsuiting

Op dit gebied is de regelgeving fragmentarisch omdat de EU te maken heeft met de zeer in nationale tradities gewortelde organisatie van de omroep. Vandaar dat de richtlijn audiovisuele mediadiensten niet verder komt dan het coördineren van een aantal regels op het gebied van de reclame.[81] Zij heeft bij de laatste wijziging nieuwe aan het internet gerelateerde ontwikkelingen proberen te ondervangen door naast het aanknopingspunt van de klassieke omroepmedia een begrippenpaar te introduceren dat de naam heeft gekregen van lineaire (klassieke massacommunicatie) en non-lineaire (een centraal geagendeerde dienst die interactief is met de gebruiker) mediadiensten. Dit is een voorbeeld van een juridische term die geen greep heeft op de onderliggende informatietechnologie, waarvan enige andere voorbeelden werden gegeven in paragraaf III.4.1.

Daarnaast is de E-Commercerichtlijn van betekenis, die van toepassing is op het gebied dat niet wordt bestreken door de communicatierichtlijnen en de richtlijn audiovisuele mediadiensten. Deze bevat een aantal bepalingen, die een intermediair vrijwaren van de aansprakelijkheid voor de doorgegeven inhoud, hetzij bij puur transport (*mere conduit*) hetzij als de inhoud enige tijd of langer wordt vastgehouden (*caching* en *hosting*). De in

77 Richtlijn 2006/24/EG, 15 maart 2006.

78 COM (2012)10 en COM (2012)11, beide van 25 januari 2012.

79 Zaak C-70/10, HvJ EU 24 november 2011), met noot E.J. Dommering, in: AMI 2012-2, pp. 49-53.

80 Richtlijn 2002/29/EG.

81 De Richtlijn Audiovisuele Mediadiensten 2010/13/EU.

deze richtlijn gehanteerde begrippen werden in paragraaf III.4.1 genoemd als voorbeeld van juridische begrippen die onvoldoende sporen met de onderliggende technische werkelijkheid. De voor dit advies belangrijkste onderdelen van deze richtlijn zijn de bepalingen die een voorafgaand verlof tot toegang van diensten verbieden en het verbod gebruikers van diensten generiek te monitoren.[82]

Regelgeving kan onbedoelde effecten hebben als regels toepassing krijgen in een gebied waarvoor zij niet zijn ontworpen. Dit is een ander aspect van het begrip verwerken dat in III.4.1 in verband met de *cloud* is besproken. Het HvJ EU is (daardoor min of meer door de ruime definitie van de wetgever gedwongen) het begrip verwerken van persoonsgegevens gaan toepassen op het redigeren van webpagina's. Dat gebeurde al betrekkelijk vroeg (in 2003) in het Lindqvist-arrest.[83] Daardoor is een begrippenapparaat en systematiek die oorspronkelijk zijn ontworpen voor databanken, ook van toepassing geworden op bijna elke webpublicatie, omdat daar vrijwel altijd enige verwerking van persoonsgegevens zal plaatsvinden.

IV.3.2 Het EU-privacydossier

Het normatieve kader van de privacyregulering heeft zich tot een aantal dossiers ontwikkeld die hier kort de revue passeren. Het gaat om de volgende kwesties: de vaststelling van de privacyverordening, de onderhandelingen met de VS naar aanleiding van de Snowdenaffaire en de grondrechtelijke toetsing door het HvJ EU.

De verordening

De bestaande grote verschillen in implementatie van de privacyrichtlijnen in de lidstaten van de EU verleiden organisaties ertoe zich te vestigen daar waar de implementatie voor hen het meest gunstig is. De vaststelling van een verordening beoogt voor de hele Unie een volledig geharmoniseerd kader vast te stellen waardoor *forum shopping* wordt tegengegaan. Zij gaat grotendeels uit van het bestaande begrippenkader, zodat de feilen die eerder werden gesignaleerd, blijven bestaan. Anderzijds worden de regels op tal van gebieden aangescherpt (bijvoorbeeld bij het maken van profielen, het plaatsen van *cookies* et cetera). Een heet hangijzer blijft de vraag of er Europees toezicht komt of Europees gecoördineerd landelijk toezicht (zoals in de sector elektronische communicatie). Het Amerikaanse perspectief komt hier in beeld omdat de verordening bij de gegevens-uitwisseling met niet-EU-landen nogal zwaar leunt op een zelfreguleringsmodel, in de verordening aangeduid als *binding corporate rules*, terwijl het hierbij vaak zal gaan om Amerikaanse bedrijven die staan onder Amerikaanse jurisdictie en al dan niet vrijwillig samenwerken met de NSA. Een punt van discussie blijft hoe in de uitwisseling van gegevens met derde landen een goede balans kan worden gevonden tussen adequate rechtsbescherming en soepele gegevensuitwisseling in een mondiale economie.

82 Zaak C-360/10, HvJ EU 16 februari 2012, (Sabam/Netlog).

83 Zaak C-101/01, HvJ EU 6 november 2003, Jur 2003, p. I-12971. Er zijn andere beslissingen aan voorafgegaan, zoals het Promusicae arrest van 28 januari 2008 (C-275/06, Jur 2008-I-00271). Daarin stelt het Hof dat de bescherming van een recht van intellectuele eigendom moet worden afgewogen tegen andere rechten.

De relatie met de VS

In de VS maakt de privacyregelgeving onderscheid tussen de private en publieke sector. De private sector wordt in de VS gereguleerd door de *Federal Trade Commission* (FTC). De FTC dwingt de naleving af van beginselen die niet erg afwijken van de Europese met sancties die vaak hoger zijn dan waarover de dataprotectie-autoriteiten in Europa beschikken.

De geldende Europese dataprotectierichtlijn verplicht de lidstaten overdracht van persoonsgegevens te verbieden naar derde landen die geen adequate bescherming bieden voor persoonsgegevens. Om export van persoonsgegevens naar de VS mogelijk te maken onder de richtlijn, is het *Safe Harbour Framework* overeengekomen. Dat biedt Amerikaanse bedrijven de mogelijkheid zich te registreren als een bedrijf met een adequaat beschermingsniveau. De procedure houdt in dat bedrijven zelf kunnen verklaren zich te zullen houden aan zeven principes. Bedrijven kunnen desgewenst externe deskundigen inschakelen om een onafhankelijk oordeel te vellen. De bedrijven moeten zich elk jaar registreren bij het ministerie van Handel, dat het bedrijf plaatst op een lijst van gecertificeerde bedrijven.

Naar aanleiding van het rapport van de Europarlementariër Claude Moraes begin 2014 over de Snowdenaffaire[84] wordt druk op de Commissie uitgeoefend om deze overeenkomst op te zeggen. Volgens het rapport van Moraes biedt het *Safe Harbour Agreement* onvoldoende bescherming voor Europese burgers en wordt het onvoldoende goed nageleefd. Bovendien zijn de uitzonderingen met betrekking tot nationale veiligheid te ruim gedefinieerd in dit verdrag. Over de mogelijke opzegging van het *Safe Habour Agreement* bestaat nog geen consensus. Het *Safe Harbour Agreement* kende altijd al zwak toezicht omdat zij slechts betrekking heeft op een deel van de uitgewisselde data, en zij grotendeels is gebaseerd op zelfcertificatie door bedrijven.[85] De Europese Commissie beslist over voortzetting of wijziging van de *Safe Harbour* overeenkomst. Nederland steunt de lijn van de Europese Commissie dat de *Safe Harbour* overeenkomst op onderdelen moet worden heronderhandeld en dat opzegging van de overeenkomst leidt tot een verslechtering van de positie van het bedrijfsleven.[86] Nederland beschikt echter over ruimschoots voldoende kennis van zaken om bij dit onderwerp meer een leidende rol te spelen.

Wat betreft trans-Atlantische data-uitwisseling in de publieke sector bestaat er al ten minste één voorbeeld van specifieke afspraken op dit gebied, namelijk de overeenkomst over de uitwisseling van gegevens inzake internationaal bankverkeer (SWIFT) met Amerikaanse autoriteiten (het *Terrorist Finance Tracking Programme*, TFTP-verdrag). Het Europees Parlement verlangt opschorting van dit verdrag omdat uit de onthullingen

84 Draft report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, Committee on Civil Liberties, Justice and Home Affairs, rapporteur: Claude Moraes, 2013/2188 (INI).

85 C. Connolly, EU/US Safe Harbor, Effectiveness of the Framework in relation to National Security Surveillance, Speaking / background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on Electronic mass surveillance of EU citizens, Strasbourg, October 7, 2013.

86 Tweede Kamer der Staten-Generaal, 32 317, nr. 226, pp. 12 en 13.

van Snowden zou zijn gebleken dat het verdrag is geschonden, hetgeen echter door de Europese Commissie wordt ontkend. Het verdrag kent echter grote tekortkomingen: de beschermingen die in dit verdrag zijn vastgelegd op het gebied van privacy, toegang tot, en correctie van individuele gegevens blijken in de praktijk vrijwel niet uitvoerbaar te zijn. Volgens het eerste rapport van de EU-VS-commissie die toezicht houdt op correcte naleving van het verdrag, kan geen gehoor worden gegeven aan individuele verzoeken om toegang tot en correctie van persoonlijke data. De reden hiervoor is dat die data ófwel niet kunnen worden opgevraagd binnen de grotere dataset omdat de autoriteiten in de VS alleen data met een nexus tot terrorisme(financiering) mogen opvragen; ófwel worden behandeld in het kader van vertrouwelijke terrorismegerelateerde onderzoeken, waarover geen mededelingen gedaan mogen worden. De juridische beschermingen in het TFTP-verdrag blijken dus in de praktijk ontoereikend.[87]

Er zijn thans onderhandelingen tussen de EU en de VS gaande om voor de publieke sector tot een *Umbrella Agreement* te komen. Een knelpunt is dat het Handvest van de grondrechten van de Europese Unie toezicht door een onafhankelijke data-autoriteit verlangt, een figuur die de VS niet kent. Verder stuit het ook af op de fundamentele kloof in het internationaal publiekrecht tussen de soevereine staat die alleen eigen burgers beschermt en het universaliteitsbeginsel dat wereldburgers overal dezelfde rechten geeft. De Amerikaanse overheid wil de Europese burgers bij de Amerikaanse rechter geen rechtsmiddel geven (zie paragraaf III.4.2). Over de uitgangspunten wat privacybescherming moet zijn bestaan geen grote verschillen van mening, maar over wat de uitzonderingen in het belang van de nationale veiligheid kunnen zijn wel, omdat de VS een veel ruimer begrip nationale veiligheid hanteert.

Grondrechtelijke toetsing

Ook in dit domein deed zich al vrij snel de werking van het Handvest van de grondrechten van de Europese Unie gevoelen. Het HvJ EU verklaarde de dataretentierichtlijn nietig, omdat zij geen enkele waarborg verschaft die uit de rechten van het Handvest van de grondrechten van de Europese Unie voortvloeien.[88] In dat arrest formuleerde het een aantal proportionaliteitseisen, waarin de richtlijn in het geheel niet voorzag. Deze uitspraak roept de vraag op wat de juridische status is van de wetten die in de lidstaten ter implementatie van de dataretentierichtlijn zijn vastgesteld. De Afdeling advisering van de Raad van State stelt dat de Wet bewaarplicht telecommunicatiegegevens geldig blijft, maar wel zal moeten worden aangepast aan de eisen die in het arrest zijn geformuleerd.[89] Duitsland heeft de richtlijn nooit geïmplementeerd en zal dat naar alle waarschijnlijkheid ook nooit doen, omdat het *Bundesverfassungsgericht* de implementatiewet in strijd met de grondwet heeft verklaard.

87 Commission report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Brussel, 16 maart 2011, pp. 16-17. Zie: http://ec.europa.eu/dgs/home-affairs/news/intro/docs/commission-report-on-the-joint-review-of-the-tftp.pdf; over dit onderwerp: M. de Goede, The SWIFT affair and the global politics of European security, in: *Journal of Common Market Studies*, 50(2), pp. 214-230.

88 Zaken C-293/2012 en C-594-12, HvJ EU, 8 april 2014.

89 Zie: <http://www.raadvanstate.nl/adviezen/samenvattingen/tekst-samenvatting.html?id=287&summary_only=>.

Op 13 mei 2014 heeft het HvJ EU in de Google Spain-zaak een verstrekkende uitspraak over de privacyaspecten van zoekmachines gedaan.[90] Een Spaans dagblad had in 1998 een bericht gepubliceerd waaruit bleek dat de klager in deze zaak (die met name in het bericht werd genoemd) schulden had gemaakt en in betalingsmoeilijkheden was gekomen. Dat bericht was op zich juist. De papieren versie van de krant was later op het internet gezet. De Spaanse Google geeft zestien jaar later bij het intikken van de naam van de betrokkene het bericht vrij hoog in de zoekresultaten weer. De betrokkene beriep zich bij de Spaanse rechter op zijn recht om vergeten te worden. Hij wendde zich tot Google en niet tot de krant. De krant had geen maatregelen genomen om het bericht van de krant voor zoekmachines niet opvraagbaar te maken, hetgeen technisch kan.

Het draait in deze zaak om de toepassing van de competentiebepalingen van de privacyrichtlijn en de regel dat de betrokkene zich om zwaarwegende redenen tegen (verdere) verwerking van persoonsgegevens kan verzetten. De huidige voorziening van het vernietigingsrecht (*right to erasure*) in de richtlijn kan in deze context worden opgevat als een *right to be forgotten*. Het Amerikaanse hoofdkantoor van Google en de Spaanse dochteronderneming van Google hadden aangevoerd dat deze niet kon worden toegepast, omdat de verwerking van persoonsgegevens (het vinden en indexeren van zoekresultaten) niet in Europa, maar in de VS plaatsvindt. Het Hof vindt dat echter niet beslissend. Het economische exploitatiemodel van de zoekmachine is gebaseerd op het koppelen van advertenties aan zoekresultaten. De advertenties worden toegesneden op de nationale markt waarin de Spaanse dochteronderneming van Google opereert. In dit geval verkocht de Spaanse Google de advertenties in de Spaanse markt en dat was voldoende om te beslissen dat de richtlijn van toepassing was. De verwerking van de persoonsgegevens vond plaats in het kader van de activiteiten van de dochteronderneming, zoals de richtlijn het zegt. Dit deel van de uitspraak is belangrijk omdat het aantoont dat Amerikaanse bedrijven en instellingen zich niet zo gemakkelijk aan de Europese privacywetgeving kunnen onttrekken als zij binnen de EU opereren. Op dit punt bestaat er geen verschil van mening over de fundamentele betekenis van de uitspraak. Meer discussie is er over het feit dat de zoekmachine de persoonsgegevens zou moeten verwijderen als deze verwijzen naar een historische stand van zaken die het moeilijk op juistheid of relevantie kan controleren. Het HvJ EU betrekt hierbij in ieder geval niet de beslissing van het EHRM uit 2009 in de Times Inc.-zaak in het kader van artikel 10 EVRM over het belang dat elektronische archieven op het internet correct zijn.[91] Het uitwissen van de vindbaarheid in de zoekmachine beperkt de toegankelijkheid van op het internet beschikbare historische bronnen. De uitspraak heeft veel discussie opgeroepen omdat volgens critici bij de toepassing van de regels van de privacyrichtlijn in combinatie met de betreffende normen van het Handvest een onvoldoende afweging heeft plaatsgevonden tussen privacy en andere in het Handvest beschermde rechten, namelijk de vrijheid van meningsuiting en de ondernemersvrijheid.

Afgezien van deze vragen blijven er ook moeilijkheden bij de toepassing van de uitspraak, bijvoorbeeld hoeveel zoekresultaten uit welke domeinen moeten worden verwijderd. Een onafhankelijk adviserend orgaan van de Europese Commissie, de Artikel 29 Werkgroep, heeft hierover in juli 2014 gesproken met de bedrijven die de grootste zoekmachines

90 Zaak C-131/2012, HvJ EU, 13 mei 2014.

91 Times Newspapers Ltd. (no's. 1 and 2) t. Verenigd Koninkrijk, no's. 3002/03 en 23676/03. Zie ook: Nederlands Juristenblad 2010, 109, met notaties van E.J. Dommering.

exploiteren.[92] Inmiddels heeft de Nederlandse voorzieningenrechter over dit probleem een uitspraak gedaan, waarin een afweging wordt gemaakt tussen het *right to be forgotten* en de noodzaak historische informatiebronnen toegankelijk te houden.[93]

92 Zie: <http://www.cbpweb.nl/Pages/pb_20140725_privacy-toezichthouders-zoekmachines-recht-om-vergeten-te-worden.aspx>.

93 Rechtbank Amsterdam 18 september 2014, ECLI: NL: RBAMS: 2014: 6118.

V Vier typen van problemen

In dit hoofdstuk beschrijven wij vier typen van problemen die karakteristiek zijn voor de hiervoor besproken vragen. 1. Hoe zal het *multistakeholder*model van ICANN zich verder ontwikkelen? 2. De dilemma's van de liberale democratieën als de VS en Nederland, die enerzijds de vrijheid van het internet voorstaan, maar anderzijds voor bepaalde doelen vergaande controle toestaan van burgers die zich op het internet bewegen 3. De autoritaire staten in het internettijdperk en 4. De rol van internationaal opererende bedrijven. De analyse van deze casus moet binnen het bestek van dit rapport kort blijven.

V.1 Het *multistakeholder*model en de rollen die staten, bedrijven en niet-gouvernementele organisaties kunnen spelen in *internetgovernance*

Het multistakeholdermodel

Dit model kan op brede steun rekenen, zoals hieronder zal blijken en ook bleek tijdens de NETmundial-bijeenkomst in Sao Paulo in april 2014, een bijeenkomst die de Braziliaanse regering buiten de bestaande fora om had georganiseerd.[94]

Er zitten verschillende haken en ogen aan de *multistakeholder*benadering.[95] Het begrip impliceert dat alle betrokkenen kunnen deelnemen aan de besluitvorming op voet van gelijkwaardigheid. Het is echter een illusie te veronderstellen dat staten en andere betrokkenen op voet van gelijkheid kunnen deelnemen aan de besluitvorming. Staten beschikken nu eenmaal over andere middelen dan andere betrokkenen. Anderzijds kunnen staten in een vrije discussie nauwelijks openlijk standpunten innemen zonder de indruk te wekken dat het gaat om een officieel standpunt. Bedrijven en niet-gouvernementele organisaties (NGO's) hebben daarin meer vrijheid.

In de praktijk worden vaak brede categorieën belanghebbenden gehanteerd, zoals het bedrijfsleven, staten en niet-gouvernementele organisaties. Binnen deze categorieën kunnen de opvattingen sterk uiteenlopen, zodat het aanwijzen van vertegenwoordigers op zich een politiek proces wordt. Procedures om vast te stellen wie de legitieme vertegenwoordigers van een categorie betrokkenen zijn, kunnen gemakkelijk worden gemanipuleerd.

Als derde punt betekent de *multistakeholder*benadering niet meer of minder dan het horen van groeperingen die worden geraakt door te nemen besluiten. In een nationale context geschiedt dat binnen duidelijke institutionele kaders door burgers die duidelijke rechten en plichten hebben. Zo bereidt het ministerie van Economische Zaken de vergaderingen van de GAC binnen ICANN zorgvuldig voor met alle belanghebbenden in Nederland. Dat berust op een bestuurlijke praktijk van het ministerie en niet op een inspraakrecht van de betrokkenen. In een internationale context is dat veel gecompliceerder. Wie de belanghebbenden zijn, wat hun rechten en plichten zijn, wie

94 Zie: <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>, geraadpleegd op 26 juni 2014.

95 M. Mueller, Network and States, Cambridge, Londen, MIT Press 2010, pp. 264-266.

vertegenwoordigers aanwijst zijn belangrijke vragen. Een *multistakeholder*benadering vergt dus een minimum aan institutionalisering.

Aanvankelijk daagde de internetgemeenschap de gevestigde macht van multilaterale organisaties en staten uit, maar inmiddels zijn deze organisaties zelf onderdeel van de gevestigde orde en verdedigen zij hun eigen belangen en voorrechten, zoals riante salarissen.[96] Het gebrek aan formele structuur betekent aan de andere kant weer dat er beleidsconcurrentie bestaat tussen de verschillende groepen, zodat er binnen ICANN een discussie over machtenscheiding à la Montesquieu op gang is gekomen.

Desondanks blijft het *multistakeholder*model grote aantrekkingskracht houden vanwege de solidariteit van de internetgemeenschap en de bindende factor van interconnectiviteit.[97] Staten, bedrijven en NGO's blijven echter naar hun aard principieel verschillende entiteiten. Derhalve verschillen hun rollen en functies, hoewel die dikwijls ook door elkaar lopen.[98] Dit wordt hieronder toegelicht.

Democratische rechtsstaten bieden burgers waarborgen, die zij meestal ook bepleiten in internationale organisaties. Daarnaast moeten staten verschillende belangen zorgvuldig tegen elkaar afwegen; bedrijven en NGO's doen dat niet. Het internet kent geen grenzen, terwijl de jurisdictie van een staat beperkt is tot zijn territorium. Voor dat deel van het internet kunnen staten nationale belangen veilig stellen, maar dat heeft beperkingen door het grensoverschrijdende karakter van vrijwel al het internetverkeer.

Bedrijven beschikken in vele gevallen over technische kennis die niet aanwezig is bij andere partijen, omdat die niet over de middelen en de drijfveer beschikken om aanzienlijke investeringen te plegen in de ontwikkeling van technische kennis. De ontwikkeling en actualisering van antivirussoftware is daarvan een voorbeeld. Deze taak kan goed worden overgelaten aan commerciële partijen. Als er concurrentie is tussen aanbieders van vergelijkbare diensten, heeft de consument keuzevrijheid die bedrijven aanspoort een optimaal product te leveren. Het nadeel is dat zij dominante posities op vitale onderdelen van het internet kunnen gaan bezetten en een proces van toe-eigening in de open *end-to-end*-omgeving proberen te forceren.

NGO's kunnen belangrijke functies vervullen, zoals de ontwikkeling van normen. Zo worden zij vaak gezien als een drijvende kracht achter de totstandkoming van het Ottawaverdrag, dat tot doel heeft de productie, handel, opslag en het gebruik van anti-personeelmijnen wereldwijd uit te bannen. NGO's voeren vaak campagnes om bekendheid te geven aan misstanden of om kwesties op de politieke agenda te zetten. Er zijn NGO's die opkomen voor algemene belangen, maar ook NGO's die de specifieke belangen van hun achterban (vaak leden) behartigen. Evenals bedrijven ontberen NGO's een democratische legitimiteit, al kunnen zij waarden of belangen vertegenwoordigen die brede aanhang genieten. Bovendien zijn de meeste NGO's gevestigd in westerse

96 Idem, pp. 217-219.

97 Zie ook: Laura DeNardis, The global war for internet governance, New Haven en London: Yale University Press, 2014, pp. 226-227.

98 Over de rollen die bedrijven en NGO's kunnen vervullen, zie ook: AIV, De rol van NGO's en bedrijven in internationale organisaties, advies nummer 51, Den Haag, oktober 2006, pp. 7-10.

landen.[99] Verder komt het steeds meer voor dat NGO's in ontwikkelingslanden die financiering ontvangen uit westerse landen, door de regering in hun eigen land verdacht worden gemaakt, worden gehinderd in hun activiteiten of zelfs worden verboden.

In paragraaf II.2 is vermeld dat de WGIG een definitie heeft geformuleerd van *internetgovernance*. Deze luidt als volgt: '*Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*'[100] Landen die een greep op de inhoud van de communicaties hebben, hebben de neiging dit begrip te ruim te interpreteren, als zou het ook om de inhoud van communicatie gaan. De enge opvatting is dat het niet over de inhoud gaat. Anderzijds kan het begrip ook weer te eng worden uitgelegd. Van Eeten en Mueller[101] wijzen erop dat het begrip *internetgovernance* in de wetenschappelijke literatuur vaak te eng wordt geïnterpreteerd, namelijk met een sterke focus op ICANN en op de invloed van staten. Maar *internetgovernance* omvat ook in de enge opvatting meer dan dat. Ook telecommunicatiebeleid is relevant voor *internetgovernance*, omdat dit onder andere de regulering van het internet, mededingingsbeleid en regulering van interconnectiviteit betreft. Verder heeft het adresseersysteem met domeinnamen een belangrijke commerciële wervingsfunctie gekregen en moet dit ook worden gezien als onderdeel van *internetgovernance*. Ook is de economische benadering van veiligheid van het internet van belang, naast de technische benadering. De economische benadering bestudeert de prikkels voor actoren om al dan niet maatregelen te nemen om de veiligheid van het net te vergroten. Dat kan gevolgen hebben voor *cybercrime*bestrijding en voor nationale veiligheid. Van Eeten en Mueller benadrukken dat *internetgovernance* plaatsvindt in een omgeving die wordt gekarakteriseerd door lage formalisering, heterogene organisaties, zeer veel actoren en een diffuus verdeelde beslissingsmacht. Besluitvorming vindt niet zozeer plaats in een formeel centraal proces, maar via de markt, in netwerken gebaseerd op vertrouwen, reputaties en wederkerigheid, via *peer production* (vrijwillige bijdragen van vele autonome actoren) en *crowd sourcing*.[102] Zo wijzen zij erop dat dienstverleners die toegang tot het internet bieden, ook een rol zijn gaan spelen in de beveiliging van het netwerk en van de apparatuur van klanten, op grond van economische overwegingen. Tot op heden heeft deze mix van organisatievormen goed gefunctioneerd.

De toekomst van ICANN

Er blijft veel kritiek op de beheersstructuur van ICANN bestaan. Omdat ICANN een monopoliepositie heeft en onder toezicht staat van het Amerikaans ministerie van Handel, heeft de Amerikaanse overheid potentieel een grotere invloed dan andere landen op een belangrijk element van het internet. Hoewel ICANN een *Governmental*

99 Idem, pp. 30-31.

100 Report of the Working Group on Internet Governance, June 2005, p. 4, punt 10. Zie: <http://www.wgig.org/docs/WGIGREPORT.pdf>, geraadpleegd op 24 juli 2014.

101 M. van Eeten en Milton L. Mueller, Where is the governance in Internet governance?, New Media & Society, 15 (5), August 2013, pp. 720-736.

102 L.B. Solum, Models of internet governance, zie: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1136825>, geraadpleegd op 6 juni 2014.

Advisory Committee (GAC) kent, dat openstaat voor alle staten, vinden vele landen dat ze onvoldoende zeggenschap hebben over ICANN.

De Amerikaanse overheid heeft in maart 2014 bekend gemaakt dat zij de verantwoordelijkheid voor de coördinatie van domeinnamen wil overdragen aan de *multistakeholder*internetgemeenschap en zij heeft ICANN verzocht een publieke consultatie over de wenselijke toekomstige structuur te houden.[103] Het ministerie heeft daarbij de hoop uitgesproken dat ICANN andere belangrijke internetorganisaties van het eerste uur zal betrekken, zoals de *Internet Engineering Task Force* (IETF), *Internet Architecture Board* (IAB) en ISOC. Ook heeft het ministerie van Handel randvoorwaarden gesteld aan de uitkomst van de consultatie. Het voorstel voor de overdracht van verantwoordelijkheden moet kunnen rekenen op brede steun en de volgende uitgangspunten respecteren: het *multistakeholder*model, behoud van de veiligheid, stabiliteit en veerkracht van het internetdomeinsysteem, voldoen aan de behoeften van internetgebruikers en de openheid van het internet bewaren. Verder heeft het ministerie aangegeven dat de verantwoordelijkheden niet zullen worden overgedragen aan een regeringsgeleide of intergouvernementele organisatie.

In de Montevideo Verklaring over de Toekomst van Internetsamenwerking (7 oktober 2013) spraken de leiders van de belangrijkste internetorganisaties zich uit voor een spoedige mondialisering van de ICANN en IANA-functies naar een omgeving waarin alle belanghebbenden, inclusief regeringen, kunnen deelnemen op voet van gelijkheid. Deze verklaring is onder andere ondertekend door de leiders van IAB, ICANN, IETF, ISOC, W3C.[104]

De wijze waarop en aan wie een geherstructureerd ICANN of een nieuwe organisatie verantwoording zal gaan afleggen, is daarbij een van de lastigste vragen. Het is nog niet duidelijk op welke termijn dit voornemen daadwerkelijk tot veranderingen zal leiden. De situatie waarin ICANN zich bevindt lijkt wel wat op die van de 17de eeuwse Republiek van de Verenigde Nederlanden: toen zij zich had losgemaakt van de absolute macht van de Spaanse Koning, moest zij op zoek naar een nieuwe soeverein. De AIV signaleert dat de toekomstige structuur van ICANN een belangrijk aandachtspunt van de regering moet zijn. Op de bijeenkomst van ICANN in oktober 2014 is een *High Level Team* samengesteld met vertegenwoordigers van alle belanghebbenden, dat een oplossing moet uitwerken. Bezien zal worden of twee van de drie taken van ICANN (namelijk protocollen en IP-adressen) kunnen worden afgestoten en ICANN uitsluitend verantwoordelijk te maken voor het beheer van domeinnamen. Een mogelijke toekomstige plaats van vestiging is Genève, maar alles is nog in discussie. Het is een onderwerp dat naar het oordeel van de AIV de aandacht van de regering vergt.

Het belang van technische organisaties voor internetvrijheid

Zoals hierboven is aangegeven is de opname van een domeinnaam in de *root* een noodzakelijke voorwaarde om dat internetadres te kunnen bereiken, tenzij men het IP-adres van een website rechtstreeks kent. ICANN neemt in beginsel alle domeinnamen op. Een domeinnaam kan worden verwijderd in gevallen waarin legitieme belangen van

103 Zie: <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>, geraadpleegd op 25 juni 2014.

104 Zie: <https://www.icann.org/news/announcement-2013-10-07-en>, geraadpleegd op 25 juni 2014.

derden zich verzetten tegen continuering van de registratie. Indien autoritaire staten de opname van domeinnamen in de *root* zouden kunnen tegenhouden, dan zouden zij niet alleen in eigen land censuur kunnen toepassen, maar wereldwijd. Informatie die deze regimes onwelgevallig zou zijn, zou onder een andere domeinnaam alsnog kunnen worden gepubliceerd, maar dat zou die domeinnaam eveneens blootstellen aan het risico op verwijdering uit de *root*. Informatie die deze regimes onwelgevallig zou zijn, zou daardoor moeilijk te vinden zijn op het internet. Het blokkeren van een domeinnaam kan daardoor onderdeel worden van een bredere campagne de toegang tot bepaalde websites te hinderen of onmogelijk te maken. Het is daarom van belang dat de controle over de *root* in neutrale handen blijft.

Eén van de meest privacygevoelige aspecten van ICANN is het beleid ten aanzien van de WHOIS databases voor de algemene topdomeinnamen. Elke internetgebruiker kan via een dergelijke WHOIS nagaan wie een domeinnaam heeft geregistreerd en wat de contactgegevens zijn van dat bedrijf of die persoon. Uit deze database kunnen dus persoonsgegevens worden opgevraagd. De *Expert Working Group* doet onderzoek naar methoden om enerzijds bijvoorbeeld informatie aan opsporingsdiensten te kunnen verstrekken en intellectuele eigendomsrechten te kunnen beschermen en anderzijds privacy beter te waarborgen dan in het huidige systeem. Sommige beheerders van landendomeinen zijn al aan deze bezwaren tegemoet gekomen, met name in Europa. Zij tonen minder persoonsgegevens aan het publiek.[105] De WHOIS van de Stichting Internet Domeinregistratie Nederland, die de domeinnamen voor het domein .nl registreert, toont geen adresgegevens van de domeinnaamhouder. Gerechtsdeurwaarders en advocaten kunnen die wel opvragen. Nederland zou een dergelijke oplossing ook internationaal kunnen uitdragen.

Open standaarden (*open source software*) kunnen bijdragen aan de bescherming van de rechten van internetgebruikers, omdat het mogelijk is te controleren of achterdeurtjes zijn ingebouwd die het verkeer aftappen en controleren. Maar er zijn ook lobby's die dat willen voorkomen. Het nieuwe internetprotocol versie 6 (IPv6-protocol) voor de langere IP-adressen bevatte een privacybeveiliging, die er later weer is uitgehaald.

De activiteiten van W3C hebben een grote invloed op de privacy van gebruikers. Het *world wide web* en zoekmachines maakten het mogelijk informatie op het internet te vinden. Bij het begin van de toepassing van het *world wide web* sloegen websites en de computer van de gebruiker niet op welke pagina's eerder waren bezocht. Het protocol voor websites bevatte geen mogelijkheid om na te gaan vanaf welke computer (vanaf welk IP-adres) de website werd benaderd. Om de commerciële mogelijkheden van het internet te vergroten, werd het protocol aangepast.[106] Zo moet een gebruiker kunnen wisselen tussen de websites van de winkel en die van de bank om een bestelling te kunnen plaatsen via een website, zonder dat de website van de winkel de bestelling kwijtraakt. Dit is het begin geweest van de *behavioural targeting*-industrie. Door bij het ontwerpen van technische specificaties rekening te houden met privacyaspecten,

105 Lee A. Bygrave c.s., The naming game: governance of the Domain Name System, in: Lee. A. Bygrave en Jon Bing, Internet Governance, infrastructure and institutions, Oxford: Oxford University Press, 2009, p. 164.

106 Lawrence Lessig, Code version 2.0, New York: Basic Books, 2006, pp. 47-49. Zie ook: <http://codev2.cc/download+remix/Lessig-Codev2.pdf>, geraadpleegd op 16 juni 2014.

kunnen de genoemde organisaties een belangrijke rol spelen bij de bescherming van internetvrijheid.[107]

W3C heeft enkele initiatieven genomen ter bescherming van de privacy van gebruikers.[108] W3C heeft het *Platform for Privacy Preferences Project* uitgevoerd, dat tot een protocol leidde waardoor websites aan de browser van computergebruikers laten weten welke gegevens over de gebruiker worden verzameld. Dit protocol wordt echter nauwelijks toegepast. Daarnaast heeft W3C een voorstel gepubliceerd om gebruikers in staat te stellen zelf te bepalen welke gegevens bedrijven kunnen verzamelen over hun gedrag op het internet. Het is gewenst dat de VS, als land van vestiging van de grootste internetbedrijven, de EU en andere westerse landen overleg voeren met W3C over de wijze waarop het gebruik van dergelijke protocollen kan worden bevorderd en welke rol regeringen en W3C daarin kunnen spelen.

Het Internet Governance Forum

Het IGF vervult een nuttige functie maar kampt met een gebrek aan menskracht en fondsen, waardoor de voorbereiding van de bijeenkomsten niet optimaal is. De agenda wordt daardoor in belangrijke mate bepaald door landen, bedrijven en instellingen die wel geld geven. Het lijdt ook onder de conflicterende waarden, die sterke gemeenschappelijke normstelling bemoeilijkt (zie hoofdstuk II). Bovendien zijn grote partijen als Google en Facebook er niet vertegenwoordigd. De AIV beveelt aan dat de participatie van Nederland aan dit forum versterkt wordt door middel van een institutionele voorbereiding van IGF-bijeenkomsten met het veld en door een hoger budget ter beschikking te stellen.

V.2 De dilemma's van de westerse democratische staten: de Verenigde Staten en Nederland

De hierna te schetsen dilemma's zien op het feit dat de westerse constitutionele democratieën enerzijds een zeer grote openbare- en privécommunicatievrijheid voorstaan en realiseren, maar anderzijds – vanwege de permanente terreurdreiging en gefaciliteerd door de bijna onbegrensde technische controlemogelijkheden – steeds meer gegevens gaan verzamelen. Dat maakt meer toezicht op het privéleven en communicatie mogelijk, waardoor het recht op privéleven en de onbevangen communicatie in het gedrang dreigen te komen. Als democratieën die twee aspecten niet met elkaar verbinden in een rechtsstatelijk kader, dreigen het Janusgezichten te worden die tegengestelde werelden laten zien, al naar gelang hoe men ernaar kijkt. Vanwege verschillen in de rechtsorden van de VS en van Nederland, gaan deze landen anders om met deze dilemma's. Ter illustratie wordt hieronder besproken hoe deze dilemma's in de VS en Nederland worden behandeld binnen hun specifieke rechtsorde. De situatie in de Verenigde Staten is ook voor Nederlanders van belang, omdat de grootste internetbedrijven (met sociale media, zoekmachines en *clouds*) zijn gevestigd in de Verenigde Staten.

107 Laura DeNardis, The global war for internet governance, New Haven and London: Yale University Press, 2014, pp. 78-79.

108 Idem, p. 79.

V.2.1 De Verenigde Staten

Internetvrijheid

In paragraaf IV.1 is verwezen naar het Internationaal Verdrag inzake burgerrechten en politieke rechten, dat in de artikelen 17 en 19 respectievelijk het recht op privacy en op vrijheid van meningsuiting vastlegt. De VS interpreteren artikel 2 van dit verdrag[109] als zouden de rechten genoemd in het verdrag alleen toekomen aan personen die zich zowel binnen het territoir van de VS als onder de jurisdictie van de VS bevinden.[110] Dit uitgangspunt wordt nog steeds gehanteerd, omdat bij de ratificatie van het verdrag het voorbehoud gemaakt is dat de bepalingen van het verdrag niet *self executing* zijn. Over het beginsel dat de bescherming van de Grondwet alleen aan Amerikaanse burgers en ingezetenen van de VS toekomt, is de laatste jaren een discussie gaande over de universele waarde van de in de Constitutie gegarandeerde rechten.[111] Ook onder invloed van de Snowdenaffaire is er beweging in dit standpunt te constateren. De President heeft initiatieven op dit vlak aangekondigd.[112]

De Verenigde Staten hebben op basis van het Eerste Amendement altijd een voortrekkersrol in de wereld gespeeld ten aanzien van de vrijheid van meningsuiting, ook bij het internet. Al vrij snel heeft de VS het internet als een voor de vrijheid van meningsuiting belangwekkend medium erkend. In een reeks beslissingen, te beginnen bij *Reno vs ACLU,*[113] werden de beginselen van de ruime bescherming van de persvrijheid op het internet toegepast en werden filtermaatregelen in de meeste gevallen veroordeeld. In contrast met deze traditie staan de maatregelen die de VS in het belang van de nationale veiligheid toelaatbaar achten. De Snowdenaffaire heeft dat duidelijker dan ooit aan het licht gebracht.

De Amerikaanse grondwet kent geen zelfstandig recht op privacy. Dit recht is voornamelijk afgeleid van het Vierde Amendement, dat burgers beschermt tegen onredelijke doorzoekingen en inbeslagname. Deze oorsprong verhindert toepassing op de particuliere sector. Er is wel een *Privacy Act*, die alleen van toepassing is op de overheid. Gegevens die vrijwillig bekend zijn gemaakt aan bedrijven, mogen door deze bedrijven voor andere doelen worden gebruikt zonder toestemming van de betrokkene. Daarnaast zijn in diverse wetten privacybepalingen opgenomen. Privacybepalingen kunnen vanwege nationale veiligheid terzijde worden geschoven. Er zijn geen dataretentieregels die bedrijven verplichten data te bewaren.

109 'Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'

110 CCPR/C/USA/4, 30 December 2011, pp. 142-143.

111 David Cole, Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?, T. Jefferson Law Review, no. 25, 2003, pp. 367-388.

112 Presidential Policy Directive, Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435, January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy directive-signals-intelligence-activities, geraadpleegd op 16 juni 2014.

113 521 US 844 (1997).

De VS heeft een systeem voor dataprotectie dat sterk afwijkt van de systemen die de EU en veel andere landen kennen. De VS kent namelijk geen algemene wet voor de bescherming van gegevens door bedrijven, maar veel sectorale wetgeving. Niet alle sectoren kennen wetgeving, zodat er lacunes zijn. Er is geen dataprotectie-autoriteit die toeziet op de naleving van de wetgeving.[114] Slechts een klein aantal wetten limiteert de hoeveelheid gegevens die bedrijven mogen verzamelen. In de ongereguleerde sectoren kunnen bedrijven persoonsgegevens bovendien voor allerlei doelen gebruiken zonder toestemming van de klant. Bedrijven hoeven dan de klant niet te informeren over dit gebruik en geen mogelijkheid te bieden zich daaraan te onttrekken. De regelgeving van de Europese Unie daarentegen bindt voor alle sectoren de verzameling, de verwerking en het gebruik van gegevens aan een vooraf gespecificeerd doel en geeft de burger meer zeggenschap over de gegevens nadat hij die heeft verstrekt. De verschillen tussen de VS en de EU leveren spanningen op bij de trans-Atlantische uitwisseling van gegevens, waarbij de EU eisen stelt aan het beschermingsniveau die in de VS moeilijk gerealiseerd kunnen worden (zie pargraaf IV.3.2).

Privacy en inlichtingen- en veiligheidsdiensten: Snowden

In 2002 werd door de *Defense Advanced Research Projects Agency*, uit wiens schoot ooit het internet is geboren, de *Information Awareness Office* opgericht met als doelstelling om de wereld van de *Total Information Awareness* (TIA) te bereiken. Als gevolg van 9/11 werd het TIA-programma gewijzigd in een programma voor een contraterrorisme-informatie-infrastructuur. Hiervoor ontbrak iedere wettelijke basis, hetgeen een reden was voor de Senaat (en later het Huis van Afgevaardigden) de ontwikkeling van TIA in 2003 stil te leggen. TIA krijgt dan ook geen financiering meer. Na het stilleggen van het TIA-programma zijn de ontwikkelingen onder een andere naam verdergegaan. In 2007 heeft de NSA het project ondergebracht bij een al sinds 1970 actieve *Special Source Operation* onder de naam PRISM, waarin door de NSA wordt samengewerkt met een honderdtal Amerikaanse *trusted companies*.

Snowden onthulde onder andere dat de NSA permanent massaal verkeersgegevens van telefoongesprekken van Amerikanen verzamelde en opsloeg. Dit gebeurde vanaf 2006 op basis van section 215 van de *USA PATRIOT Act* (2001) en met jaarlijks hernieuwde toestemming van de *Foreign Intelligence Surveillance Court* (FISC). De FISC verbood de NSA dataminingtechnieken toe te passen op de verkeersgegevens, er mocht alleen gericht in worden gezocht. Daarnaast verzamelde de NSA de inhoud van communicatie, waaronder telefoongesprekken en e-mails, van personen waarvan werd aangenomen dat zij buitenlander zijn en niet in de VS verblijven. De juridische basis daarvoor is *section* 702 van de *FISA Amendments Act* (2008).

Naar aanleiding van de onthullingen door Snowden heeft de Amerikaanse president een commissie ingesteld, de *President's Review Group on Intelligence and Communications Technologies*, die in december 2013 verslag uitbracht aan de president.[115] Daarnaast heeft de Amerikaanse *Privacy & Civil Liberties Oversight Board* (PCLOB) twee rapporten

114 Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalisation of Convention 108?, University of Edinburg School of Law, Research Paper Series no. 2012/12, pp. 3-6.

115 Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 2013.

uitgebracht, één over *section* 215 en één over *section* 702.[116] De rapporten gaan niet in op andere NSA-programma's die volgens Snowden zouden bestaan, waaronder de beschuldigingen dat de NSA versleuteling van berichten brak (Bullrun) en zwakheden in programma's van bedrijven kende of zelfs liet inbouwen, waardoor de NSA kon inbreken in computers.[117]

De vraag naar de (juridische) toelaatbaarheid van de activiteiten van de NSA wordt in deze rapporten beoordeeld vanuit het perspectief van de Amerikaanse grondwet en wetgeving. De *Presidential Review Group* maakt slechts een korte opmerking over mensenrechten.[118] Het rapport van de *Presidential Review Group* en het rapport van de PCLOB over *section* 702 beschrijven in detail de juridische kaders van de onderschepping van communicatie van buitenlanders die buiten de VS verblijven. Er zijn daarbij belangrijke verschillen met onderschepping van communicatie van Amerikanen en personen die legaal in de VS verblijven. Amerikanen en personen die legaal in de VS verblijven worden beschermd door het Vierde Amendement op de grondwet.[119] Als het gaat om deze groep, dan heeft de regering een *probable cause* nodig en een individueel bevel (*warrant*, rechterlijke machtiging) om gericht onderzoek te mogen doen. Voor buitenlanders buiten de VS gelden beide voorwaarden niet, zelfs niet als de onderschepping van de communicatie binnen de VS plaatsvindt. In plaats van een *probable cause* moet er slechts een *reasonable belief* zijn dat een e-mailadres of telefoonnummer wordt gebruikt voor internationaal terrorisme, nucleaire proliferatie, vijandige *cyber*activiteiten en dergelijke.[120] Het voorgaande betekent dat de vertrouwelijkheid van communicatie en de privacy van buitenlanders buiten de VS aanzienlijk minder bescherming geniet dan die van Amerikanen en buitenlanders die in de VS verblijven. De *Presidential Review Group* stelt voor buitenlanders dezelfde rechten toe te kennen (inzagerecht, correctierecht, juridische remedies) als Amerikanen en ingezetenen hebben onder de *Privacy Act*, ook ten aanzien van inlichtingen- en veiligheidsdiensten, tenzij er dwingende redenen zijn dat niet te doen. Daarmee zou de praktijk van het *Department of Homeland Security* worden geformaliseerd.[121] *Attorney General* Holder heeft op 25 juni 2014 toegezegd aan de Europese ministers van Justitie en Binnenlandse Zaken dat de Amerikaanse regering een wetsontwerp aan het Congres zal voorleggen waarin de werking van de *Privacy Act* wordt uitgebreid tot burgers van

116 Privacy & Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, January 2014, alsmede Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 July, 2014.

117 Zie: <https://www.eff.org/nsa-spying>.

118 Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 2013, p. 155.

119 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

120 Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 2013, pp. 152-153.

121 Idem, p. 157, recommendation 14.

de EU.[122] Europese burgers zouden dan bijvoorbeeld dezelfde rechten krijgen als Amerikanen om genoegdoening te verkrijgen als beschermde informatie zonder legitieme grondslag wordt gedeeld met anderen. Kennelijk zou de voorgenomen uitbreiding van de werking van de *Privacy Act* niet gelden voor andere buitenlanders. Zoals hierboven aangegeven is het niveau van bescherming van privacy in de VS in diverse opzichten aanzienlijk lager dan in de EU.[123]

De rapporten van de *Presidential Review Group* en van de PCLOB over *section* 215 gaan in op de vraag in hoeverre het ongericht verzamelen van verkeersgegevens van communicatie van Amerikanen legaal is volgens de Amerikaanse grondwet en het Amerikaanse recht. Daarover blijken de meningen te verschillen. Volgens de commissie moet een afweging worden gemaakt tussen de additionele veiligheid die ongerichte verzameling en opslag genereert en de offers in termen van individuele privacy, persoonlijke vrijheid en publiek vertrouwen.[124]

De rapporten gaan in op de vraag in hoeverre deze programma's effectief waren. Zowel de PCLOB als de *Presidential Review Group* concluderen dat de ongerichte verzameling van verkeersgegevens onder *section* 215 niet effectief was in het voorkomen van terroristische aanslagen. Voor zover wel relevante informatie beschikbaar kwam, had deze ook kunnen worden verkregen met methoden die minder inbreuk maken op de privacy.[125] De PCLOB wijst erop dat het niet denkbeeldig is dat de overheid misbruik maakt van de opgeslagen informatie, gezien de recente geschiedenis van de VS. Bovendien kan het verzamelen en opslaan van metadata door de overheid burgers terughoudend maken vrij hun mening te uiten, omdat de vertrouwelijkheid van communicatie niet is gewaarborgd.[126] Een lid van de PCLOB meende dat het programma wel effectief was.[127]

V.2.2 Nederland

Ook Nederland loopt voorop als het gaat om het uitdragen van internetvrijheid. De adviesaanvraag vermeldt dat ons land de *Freedom Online Coalition* heeft opgericht. Deze heeft succesvol geopereerd in Dubai bij het tegenhouden van de wijziging van de *International Telecommunications Regulations* die beoogde de overheidscontrole op de

122 The Guardian, 25 juni 2014. Zie: <http://www.theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe>, geraadpleegd op 26 juni 2014.

123 Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalisation of Convention 108?, University of Edinburg School of Law, Research Paper Series no. 2012/12, pp. 3-6.

124 Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 2013, pp. 108-114.

125 Privacy & Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, January 2014, p. 146 en: Liberty and security in a changing world, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 2013, p. 104.

126 Privacy & Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, January 2014, pp. 155-164.

127 Idem, Annex B.

inhoud van de uitingen te vergroten (zie paragraaf II.3). Nederland speelt actief in op het Groenboek van de Europese Commissie 'Voorbereiding op een volledig geconvergeerde audiovisuele wereld, groei en creatie van waarden'.[128]

In Nederland hebben zich belangrijke economische activiteiten rond internet ontwikkeld. In Amsterdam bevindt zich de grootste internet exchange ter wereld (AMS-IX met ruim 600 aangesloten netwerken). De digitale infrastructuursector heeft een omzet van circa 1,5 miljard euro en faciliteert naar schatting een derde van de Europese omzet in *e-commerce*. Het gaat om een belangrijke groeisector.[129]

Evenals in de VS zijn ook in Nederland voorbeelden te vinden waarin het dilemma zichtbaar is tussen enerzijds een zeer grote openbare- en privé communicatievrijheid en anderzijds toegenomen verzameling van gegevens die zijn gerelateerd aan het privéleven en de onbevangen communicatie. Ook hier is er een worsteling privacy en veiligheid met elkaar in balans te brengen binnen rechtsstatelijke kaders.

In paragraaf III.4.1 is toegelicht dat uit de metadata over een individu veel is af te leiden over zijn of haar gedrag en voorkeuren. Het onderscheid tussen inhoud en metadata is niet scherp. Deze kwestie is onder meer van belang bij de herziening van artikel 13 van de Grondwet. Uit de memorie van toelichting en uit het nader rapport (in reactie op het advies van de Raad van State) blijkt dat het kabinet wel erkent dat het onderscheid is vervaagd, maar het kabinet is van mening dat dit niet betekent dat alle verkeersgegevens hetzelfde niveau van grondwettelijke bescherming moeten krijgen als de communicatie-inhoud. In de toelichting bij het wetsvoorstel tot wijziging van artikel 13 van de Grondwet worden grensgevallen genoemd tussen inhoud en verkeersgegevens en is de keuze gemaakt om verkeersgegevens die de inhoud van de communicatie betreffen, onder het telecommunicatiegeheim te brengen. De wetgever en de rechtsspraak zullen dat nader vorm moeten geven.

De Europese dataretentierichtlijn is in april 2014 ongeldig verklaard en op 17 november 2014 zond de minister van Veiligheid en Justitie zijn reactie aan de Tweede Kamer der Staten-Generaal,[130] na advies te hebben ingewonnen bij de Afdeling advisering van de Raad van State. De minister en de Afdeling advisering concluderen dat de ongeldigverklaring van de dataretentierichtlijn niet betekent dat de Nederlandse wetgeving ongeldig is. De minister stelt dat de relevante wetgeving op een aantal punten moet worden aangepast, zodat de wetgeving in overeenstemming wordt gebracht met de eisen die het HvJ EU stelt aan dataretentie. Het gaat om voorafgaande toestemming door de rechter-commissaris bij vordering van telecommunicatiegegevens, differentiatie van toegang tot gegevens naar gelang de ernst van het misdrijf, mogelijke versleuteling van opgeslagen gegevens, verplichte opslag op het grondgebied van de Europese Unie en uitbreiding van de bevoegdheden van de Agentschap Telecom voor sterker toezicht.

128 Groenboek, Voorbereiding op een volledig geconvergeerde audiovisuele wereld: Groei, creatie en waarden, Brussel, 24 april 2013, COM(2013) 231 final. Zie voor de Nederlandse conceptreactie Tweede Kamer der Staten-Generaal 22112 nr. 1659 met bijlage.

129 Cijfers ontleend aan *The.nlyst*, nr. 15, Q3 2014, een uitgave van de Stichting Internet Domeinnamen Nederland.

130 Tweede Kamer der Staten-Generaal, 33 542, nr. 16.

De AIV is van oordeel dat ongerichte verzameling van metadata niet toelaatbaar is, omdat deze ingrijpt in het recht op privacy, tenzij daarvoor wettelijke normering bestaat die beantwoordt aan de voorwaarden van de betreffende fundamentele rechten. Het HvJ EU heeft in zijn arrest over de vernietiging van de dataretentierichtlijn aangegeven aan welke voorwaarden de opslag van metadata moet voldoen. De minister van Veiligheid en Justitie heeft in zijn brief aan de Tweede Kamer der Staten-Generaal naar aanleiding van de ongeldigverklaring van de dataretentierichtlijn, namens het kabinet toegezegd dit arrest te betrekken bij de herziening van de Wiv 2002.[131]

In rapport 38 van de CTIVD constateert dit orgaan dat de technologische ontwikkelingen wijzen van inzet van bevoegdheden mogelijk maken die niet door de wetgever waren voorzien. Voor die wijzen van inzet van middelen bestaan onvoldoende waarborgen, al wordt de Wiv 2002 strikt genomen niet overschreden. Dat geldt bijvoorbeeld voor de analyse van metadata. De CTIVD adviseert in de wet een specifieke regeling op te nemen voor de analyse van metadata, omdat deze voor een deel zijn aan te merken als persoonsgegevens. Ook adviseert de CTIVD in de herziene wet op de inlichtingen en veiligheidsdiensten een maximumtermijn vast te leggen voor de bewaring van ruwe gegevens. Het kabinet heeft beide aanbevelingen overgenomen.[132]

Op 21 november 2014 informeerde het kabinet de Tweede Kamer over zijn standpunt over de herziening van het interceptiestelsel Wiv 2002. Het kabinet volgt het advies van de commissie Dessens om het onderscheid tussen kabelgebonden en niet-kabelgebonden communicatie te laten vervallen en daarbij aanvullende waarborgen in de wet op te nemen.[133] De artikelen 26 (verkenning van communicatie) en 27 (ongerichte interceptie) van de Wiv 2002 zullen worden gewijzigd, zodat de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden uitgebreid tot kabelgebonden communicatie. De feitelijke verwerking zal in drie fasen plaatsvinden, waarbij in elke fase waarborgen zullen worden ingebouwd. Het kabinet geeft in algemene zin aan waaruit deze waarborgen zullen bestaan, maar specifieke informatie daarover ontbreekt. De brief verwijst niet naar het arrest van het HvJ EU, waarin de dataretentierichtlijn werd vernietigd en dat de eisen vermeld waaraan opslag van gegevens moet voldoen. Voor kabelgebonden en niet-kabelgebonden interceptie zullen dezelfde waarborgen gaan gelden, zodat het beschermingsniveau voor niet-kabelgebonden interceptie wordt verhoogd.

Het kabinet heeft de aanbeveling van de Commissie Dessens dat het externe toezicht op de veiligheidsdiensten tijdig bindende aanwijzingen moet kunnen geven over de rechtmatigheid van de controle- en onderzoekswerkzaamheden, niet overgenomen. De CTIVD heeft deze aanbeveling van de commissie Dessens ondersteund. Het kabinet merkt op dat de minister te allen tijde volledig verantwoordelijk is voor de operationele activiteiten van de diensten en daarvoor ook ten volle verantwoording aflegt aan de beide Kamers der Staten-Generaal. Als de CTIVD stuit op activiteiten die naar het oordeel van de CTIVD onmiddellijk stopgezet zouden moeten worden, dan kan de CTIVD de minister informeren. Het advies van de CTIVD wordt openbaar en kan zodoende

131 Idem, p. 14.

132 Tweede Kamer der Staten-Generaal, 29 924, nr. 105.

133 Tweede Kamer der Staten-Generaal, 33 820, nr. 4.

onderwerp worden van politieke verantwoording door de verantwoordelijke minister.[134]

Een aantal burgerrechtenorganisaties heeft over de samenwerking tussen de Nederlandse diensten en de NSA een procedure bij de rechter aangespannen, die door eisers op feitelijke gronden is verloren. De eisers hebben hoger beroep ingesteld.[135] Het ministerie van Veiligheid en Justitie maakt jaarlijks het aantal telefoon- en internettaps openbaar en heeft een werkgroep in het leven geroepen die bestudeert of en hoe de transparantie over taps vergroot kan worden.[136]

Voorts valt te wijzen op het binnenkort in te dienen wetsvoorstel computercriminaliteit III.[137] Blijkens het in consultatie gebrachte voorontwerp introduceert dit voorstel vergaande bevoegdheden om de bestrijding van computercriminaliteit te bevorderen, waarbij in dit verband vooral het voorstel om de politie de bevoegdheid te geven computers op afstand te doorzoeken (het 'hackvoorstel') relevant is. Het voorstel komt neer op het plaatsen van *malware* (afluistersoftware) op de computer of *smartphone* van een verdachte, waarbij heimelijk de harde schijf kan worden doorzocht, toetsaanslagen kunnen worden doorgegeven en de camera en microfoon op afstand kunnen worden aangezet. Het voorstel is kritisch ontvangen,[138] niet alleen vanwege de vele mogelijkheden om de hele handel en wandel van een verdachte op afstand in beeld te krijgen, maar ook vanwege het voorstel om de bevoegdheid grensoverschrijdend te kunnen inzetten. Dit laatste zou kunnen wanneer de plaats van opslag van gegevens niet bekend is (wat bij *cloud computing* al snel het geval kan zijn), maar het voorstel sluit niet uit dat wanneer de opslagplaats wel bekend is, gegevens vanuit Nederland heimelijk kunnen worden doorzocht en eventueel zelfs ontoegankelijk worden gemaakt, zonder voorafgaande toestemming van de andere staat. De niet-onderbouwde uitspraak in de memorie van toelichting bij het consultatievoorstel[139] dat dit in overeenstemming zou zijn met het volkenrecht, is aanvechtbaar; de AIV acht het grensoverschrijdend doorzoeken van computers zonder toestemming van de staat waarin de gegevens zijn opgeslagen, niet geoorloofd naar het huidige internationale recht.[140] Dat dit onbevredigend is gezien de noodzaak van effectieve *cyber*opsporing, waarbij veelal

134 Idem, 33 820, nr. 2, p. 6.

135 Rechtbank Den Haag, 23 juli 2014. Zie: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:8966.

136 Zie: <http://over.vodafone.nl/nieuwscentrum/nieuws/actueel-nieuws?page=5>, geraadpleegd op 12 november 2014.

137 Zie: <http://www.internetconsultatie.nl/computercriminaliteit>.

138 C. Conings en J.J. Oerlemans, Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?, Computerrecht, 2013, nr. 1, pp. 23-32.

139 Wetsontwerp computercriminaliteit III, memorie van toelichting, p. 36, beschikbaar op: <http://www.internetconsultatie.nl/computercriminaliteit>.

140 Een uitzondering geldt voor staten die partij zijn bij het Cybercrime-verdrag van de Raad van Europa in gevallen waarin artikel 32(b) van dat verdrag voorziet, namelijk wanneer er vrijwillige toestemming is van de rechthebbende van de gegevens of van de internetaanbieder die rechtmatig kan beschikken over de opgeslagen gegevens.

de koninklijke weg van wederzijdse rechtshulp te lang duurt om vluchtige gegevens veilig te stellen, moge duidelijk zijn, maar dat doet niet af aan de juridische grenzen die het internationale recht momenteel trekt. Het voorstel zou in deze vorm ook negatieve gevolgen kunnen hebben voor de status van Nederland in de internationale gemeenschap als voorvechter van internetvrijheden en bovendien als gevolg hebben dat Nederland internationaalrechtelijk niet meer zou mogen klagen als buitenlandse staten in Nederlandse computers zouden inbreken om gegevens van bedrijven te kopiëren. In plaats van unilateraal een grensoverschrijdende bevoegdheid in te voeren, kan Nederland beter het initiatief voor een aanvullend protocol bij het *Cybercrime*-verdrag betreffende grensoverschrijdende opsporingstoegang tot data afwachten en actief ondersteunen, iets waar het ministerie van Veiligheid en Justitie zich al actief voor inzet.

Naast de grensoverschrijdende dimensie, moet ook worden gesignaleerd dat het hackvoorstel een bijzonder vergaande inbreuk op de privacy oplevert – een inbreuk die aanzienlijk verder gaat dan de concept-Memorie van Toelichting erkent. Een doorzoeking op afstand van een computer of *smartphone* geeft namelijk nog veel meer inzicht in de persoonlijke levenssfeer dan een klassieke doorzoeking. Zoals het Amerikaanse Hooggerechtshof in een recente mijlpaalzaak over het onderzoek van mobiele telefoons heeft geformuleerd: '*a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form. (…) With all they contain and all they may reveal, they hold for many Americans 'the privacies of life'*.'[141] Een hackbevoegdheid voor de politie is daarom alleen verenigbaar met het recht op privacy als het wordt omkleed met strikte proportionaliteits- en subsidiariteitswaarborgen, die nog strakker moeten zijn dan de bevoegdheid om communicatie te onderscheppen.

De AIV brengt onder de aandacht van de regering dat bij de hierboven beschreven beleidskwesties betrokken moeten worden de in juli 2012 in de Mensenrechtenraad aangenomen resolutie '*The promotion, protection and enjoyment of Human Rights on the Internet*' (A/HRC/20/L.13) en de voorbeeldfunctie die Nederland met name op het gebied van de mensenrechten wil vervullen. Daarbij gaat het er immers niet alleen om of en hoe lang mindere vormen van bescherming van grondrechten binnen de internationale rechtsorde verdedigbaar zijn, maar ook of Nederland gangmaker wil zijn in de gewenste ontwikkelingsrichting van die rechtsorde.

V.3 Internetcensuur, controle en de mobilisatiefunctie van het internet

China en Rusland worden hier als voorbeeld genomen voor censurering en controle van het internet, maar zouden met vele andere voorbeelden kunnen worden aangevuld. In verschillende varianten valt te constateren dat deze landen beogen van het internet een in*tra*net te maken (in China: een digitale Chinese Muur), waarvan het inkomende en uitgaande verkeer via centrale servers wordt geleid en het nationale verkeer in vergaande mate wordt gecensureerd op inhoud en bijgehouden op gedrag en communicaties van de gebruikers.

Aan de hand van de door *Freedom House* ontwikkelde criteria die in hoofdstuk I zijn geciteerd zijn de volgende opmerkingen te maken.

141 Riley v. California, 573 U.S. _ (2014), te vinden op: <http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf>.

China[142] *en Rusland*[143]

China heeft het Internationaal Verdrag inzake burgerrechten en politieke rechten niet geratificeerd, maar wel ondertekend en moet zich dus onthouden van handelingen die het verdrag zijn voorwerp en zijn doel zouden ontnemen. De Russische Federatie heeft het Internationaal Verdrag inzake burgerrechten en politieke rechten wel geratificeerd. Bovendien is ze lid van de Raad van Europa en dus onderworpen aan de bepalingen van het EVRM en de uitspraken van het EHRM.

In beide landen garandeert de grondwet de vrijheid van meningsuiting, maar in de praktijk zijn de burgerlijke en politieke vrijheden begrensd. Juridisch worden de inperkingen meestal gerechtvaardigd met een beroep op de staatsveiligheid of de wet op de staatsgeheimen (China) of wetgeving over extremisme (Rusland). Deze wetgeving is vaag geformuleerd, zodat de overheid veel ruimte heeft in de toepassing en de burgers weinig rechtszekerheid hebben. De regering zet onder andere propaganda en censuur in om de positie van de regerende partij te waarborgen, ook op het internet. Al bij het begin van de ontwikkeling van het internet in China in 2001 verklaarde haar toenmalige president Jiang Zemin dat het internet een 'politiek, cultureel en ideologisch slagveld' was.[144]

De belangrijkste methode voor censuur is automatische technische filtering van data, maar ook wordt informatie handmatig van het internet verwijderd. In beide landen stellen overheidsorganisaties lijsten op van websites die internetdienstverleners moeten blokkeren, zonder rechterlijke toetsing vooraf of achteraf. In China kunnen internetdienstverleners aansprakelijk worden gesteld voor de verspreiding van informatie die de overheid onwelgevallig is. Zij passen daarom zelf censuur toe. Niettemin lukt het de overheid niet altijd om onwelgevallige informatie te blokkeren of te verwijderen voordat deze wijd verspreid is. Internationale internetdienstverleners werken daaraan niet altijd mee. Zo heeft Google in 2010 geprobeerd de censuur te ontwijken door internetgebruikers in China te verwijzen naar de ongecensureerde zoekmachine die op servers in Hong Kong draait. Overigens wordt ook niet alle politieke kritiek gecensureerd; de nadruk ligt op censuur van uitingen die oproepen of kunnen leiden tot mobilisatie van groepen of andere collectieve acties.[145]

Verder zijn in Rusland eind 2011 nieuwe regels in werking getreden voor registratie

142 Freedom House, Freedom of the Press 2013, pp. 120-127. Zie: <http://www.freedomhouse.org/sites/default/files/FOTP%202013%20Full%20Report.pdf>, Freedom House, Freedom in the World 2014, <http://www.freedomhouse.org/report/freedom-world/2014/china-0 en Freedom House>, Freedom on the Net 2013, <http://www.freedomhouse.org/report/freedom-net/2013/china>, alle geraadpleegd op 10 juli 2014.

143 Freedom House, Freedom on the Net 2013, pp. 588-600, Freedom House, Freedom of the Press 2013, pp. 315-319, <http://www.freedomhouse.org/sites/default/files/FOTP%202013%20Full%20Report.pdf en Freedom House, Freedom in the World 2014, http://www.freedomhouse.org/report/freedom-world/2014/russia-0>, alle geraadpleegd op 10 juli 2014.

144 Evan Osnos, Age of Ambition, Chasing Fortune,Truth and Faith in the New China, London: The Bodley Head 2014, p. 30.

145 Gary King e.a., How Censorship in China Allows Government Criticism but Silences Collective Expression, American Political Science Review, May 2013.

van domeinnamen onder het domein.ru. Bepaalde opsporingsautoriteiten hebben de bevoegdheid schriftelijk opdracht te geven de registratie van specifieke domeinnamen te beëindigen, waarmee deze feitelijk niet meer bestaan. Een andere methode om de toegang tot inhoud te verhinderen is door *Distributed Denial of Service*aanvallen op websites uit te voeren. Sinds mei 2014 geldt de registratieplicht voor bloggers die meer dan 3000 volgers trekken. Sociale media worden aan steeds scherpere (informele) controle onderworpen.

Vanaf 2016 geldt voor de opslag van persoonsgegevens een datalokalisatieplicht in Rusland.[146]

Daarnaast manipuleert de overheid in beide landen de inhoud op het internet door bloggers te betalen voor het plaatsen van positieve commentaren op overheidsfunctionarissen, de partij en het beleid. Deze zogenaamde Russische 'trollen' beginnen steeds meer op te vallen.

De bescherming van de privacy is in China beperkt. Er is geen relevante grondwetsbepaling en er is geen privacywet. Er is wel een grondwetsbepaling over privacy van correspondentie, maar daarop bestaan vele uitzonderingen.[147] China kent geen algemene wet voor dataprotectie.[148]

In China is de toegang tot buitenlandse internetdiensten zoals Facebook, Twitter en YouTube geblokkeerd. Filters belemmeren toegang tot deze diensten vanuit China. Chinese bedrijven hebben nationale varianten van deze diensten opgezet en deze zijn zeer populair.

Diverse technische middelen kunnen helpen om censuur te ontlopen, zoals verzending van verboden informatie via *peer-to-peer* netwerken of *virtual private network*s. Een andere methode is het gebruik van homoniemen. Daarbij wordt gebruik gemaakt van het feit dat Chinese woorden een totaal andere betekenis kunnen krijgen als ze iets anders worden uitgesproken. Het Bureau Internet Zaken in Beijing voert met een enorme mankracht een voortdurende, maar schier hopeloze strijd om de vrijheid van meningsuiting op internet te beperken.[149]

Het tekort aan internetvrijheid in autoritair geregeerde landen is een aspect van het bredere tekort aan democratie en rechtsstaat. De censuur op het internet wordt dan ook aangevuld met repressieve maatregelen, zoals detentie van populaire bloggers. Steeds vaker worden administratieve of fiscale maatregelen gebruikt tegen mensenrechtenverdedigers om hen het zwijgen op te leggen.

146 Gegevens over de toenemende internetrepressie in de opinie van Tanya Loksjina, directeur Human Rights Watch Moskou, Volkskrant, 2 augustus 2014.

147 UNESCO, Global survey on internet privacy and freedom of expression, 2012, pp. 74-78. Zie: <http://unesdoc.unesco.org/images/0021/002182/218273e.pdf>.

148 Graham Greenleaf, The influence of European data privacy standards outside Europe: implications for globalisation of Convention 108?, University of Edinburg School of Law, Research Paper Series no. 2012/12, p. 6.

149 Evan Osnos, Age of Ambition, Chasing Fortune,Truth and Faith in the New China, London: The Bodley Head 2014, pp. 199-203.

De mobilisatiefunctie van het internet

Tijdens de omwentelingen in de Arabische wereld is veel geschreven over de rol van sociale media. Werkloosheid, armoede en politieke uitsluiting waren belangrijke redenen voor de relatief jonge, beter opgeleide en mondiger bevolking om in opstand te komen.[150] Sociale media hebben een belangrijke rol vervuld in de politieke ontwikkelingen in de Arabische regio,[151] omdat zij hebben bijgedragen aan snelle verspreiding van informatie, het politieke bewustzijn hebben verhoogd en een platform waren voor netwerken en mobilisatie.

Sociale media kunnen tegenwicht bieden aan propaganda van de regering, vooral in situaties waarin de regering controle heeft over andere media. Via sociale media kunnen gemakkelijker alternatieve *narratives* ontstaan, mits deze niet onder controle staan van de regering. Ze kunnen een platform zijn voor discussie, maar ook worden gebruikt om misinformatie en propaganda te verspreiden.

Voordat het internet bestond werden diverse misstanden alleen lokaal of nationaal bekend. Nu kan één incident via sociale media snel wereldwijde bekendheid krijgen en de aanleiding zijn voor grootschalig maatschappelijk protest tegen de autoriteiten. Voorbeelden zijn de Facebookcampagne naar aanleiding van de dood van Egyptenaar Khalil Said als gevolg van politiegeweld in juni 2010 en de zelfverbranding van de Tunesische straatverkoper Mohammed Bouazizi in december 2010. Sociale media bieden ook de mogelijkheid belangrijke gebeurtenissen wereldkundig te maken terwijl ze gebeuren. Zo was een artilleriebombardement op de stad Homs via het internet te volgen terwijl het plaatsvond.

Omdat via sociale media veel mensen tegelijk zijn te bereiken, zijn zij een goed middel om mensen te mobiliseren, ook als zij geografisch ver van elkaar zijn verwijderd. In een oogwenk kan een oproep tot een demonstratie worden verzonden aan veel mensen. In de Russische Federatie gebruikte oppositieleider Aleksey Navalny sociale media om geld in te zamelen voor zijn beweging en stemmen te winnen voor de verkiezingen voor de burgemeester van Moskou in september 2013.[152] Sociale media kunnen mobilisatie weliswaar bevorderen, maar er moet ook aan andere voorwaarden zijn voldaan om mensen te bewegen politiek actief te worden.[153]

In landen waar de vrijheid van meningsuiting onder druk staat, vreest de regering de mogelijkheden tot mobilisatie van sociale media. Overheden proberen greep te krijgen op deze media door wettelijke beperkingen op te leggen aan gebruikers en bedrijven, door de bedrijven onder druk te zetten, te verplichten mee te werken aan censuur. De meeste staten slagen er niet in alle ongewenste inhoud tegen te houden, er wordt teveel gepubliceerd. Als de dreiging te groot wordt, sluit de overheid soms het internet

150 AIV, De Arabische Regio, een onzekere toekomst, advies nummer 79, Den Haag, mei 2012.

151 Paul Aarts e.a, From resilience to revolt, making sense of the Arab spring, Universiteit van Amsterdam, juni 2012, pp. 45-47.

152 Freedom House, Freedom in the World 2014, Russia, p. 1.

153 Paul Aarts e.a, From resilience to revolt, making sense of the Arab spring, Universiteit van Amsterdam, juni 2012, pp. 34-38 en pp. 45-47.

af voor een korte periode. Maar in vrijwel alle landen is het internet te belangrijk voor de economie om langdurig af te sluiten. De Chinese Amazon, Alibaba, zorgde in de VS in september 2014 voor een van de grootste beursgangen uit de geschiedenis.

Globaal zijn er twee sporen om de vrijheid van meningsuiting op het internet te bevorderen. Het eerste spoor is aandringen op betere naleving van bestaande normen en het tweede spoor betreft technische mogelijkheden creëren voor mensenrechten-verdedigers om censuur en andere belemmeringen te ontwijken. De geraadpleegde deskundigen stelden dat voldoende technieken beschikbaar zijn, maar deze zouden meer gebruiksvriendelijk moeten worden gemaakt. De Nederlandse regering steunt diverse activiteiten op deze terreinen, zoals trainen van bloggers en *online* journalisten over het ontwijken van censuur, over veiligheid op en buiten het internet. In 2011 was Nederland een van de oprichters van de *Freedom Online Coalitie*.

V.4 De rol van bedrijven

In paragraaf III.3 is gewezen op de rol van intermediairs, die in democratische rechtsstaten bescherming genieten tegen overheidsbemoeienis. Ook werd geconstateerd dat de bescherming van de rol van de nieuwe intermediairs van het internet zich nog niet heeft vastgezet in recht en regelgeving. Zowel voor gebruikers als voor bedrijven moeten rechtsstatelijke beginselen in acht worden genomen als de overheid wil ingrijpen op de vrijheid op het internet. Bedrijven voeren in verschillende mate actief beleid ten aanzien van internetvrijheid. Sommige kennen procedures en beleid voor verwijderen van inhoud. Ze verzetten zich al dan niet tegen verzoeken van de overheid om inhoud te verwijderen of informatie over te dragen aan de overheid. Momenteel loopt een procedure voor Amerikaanse rechters waarin Microsoft de competentie betwist van Amerikaanse federale autoriteiten om Microsoft te gelasten de inhoud van een e-mail over te dragen die op een server in Ierland wordt bewaard. Microsoft wordt daarin gesteund door andere grote Amerikaanse internetbedrijven.

Verder hebben bedrijven eigen opvattingen over wat al dan niet toelaatbaar is, bijvoorbeeld over zedelijkheid. Bedrijven zijn in verschillende mate transparant over de mate waarin zij inhoud filteren. Twitter informeert gebruikers over blokkades, maar Facebook doet dat niet. De vergaande samenwerking tussen de bedrijven en de NSA in het kader van PRISM is zeer ondoorzichtig, omdat bedrijven gedwongen worden de (verplichte) medewerking geheim te houden. Internetapparatuur en -diensten bevatten meestal geheime broncodes, zodat ondoorzichtig is in hoeverre er technische lekken zijn die de privacy en veiligheid van gebruikers kunnen bedreigen.

In minder democratische landen zetten overheden bedrijven vaak onder druk om websites onvindbaar te maken, inhoud te filteren, *tweets* te verwijderen, informatie te verstrekken over de identiteit van bloggers en dergelijke. Ook internationale bedrijven kunnen onder druk komen te staan en moeten dan – vanwege het ontbreken van rechtsmiddelen – een afweging maken tussen hun commerciële belangen en mensenrechten. Ook als internationale bedrijven ervoor kiezen actief te blijven in landen met een gebrekkige internetvrijheid, dan kunnen zij transparantie nastreven over de mate waarin zij (moeten) meewerken aan censuur. Zo kunnen zij statistieken publiceren over het aantal en de aard van opdrachten die zij van de overheid kregen. Zij kunnen gebruikers informeren die worden getroffen. Dat laatste kan echter worden verboden; sommige bedrijven sturen hun klanten in dat licht '*warrant canaries*': een (wel toegestane) mededeling dat de

aanbieder (nog) géén bevel van de overheid heeft gehad om gegevens over de klant te verstrekken.[154]

Internationale internetbedrijven reageren op verschillende wijzen op verzoeken van autoriteiten om inhoud te filteren of te manipuleren.[155] Zo laat Google sinds kort andere grenzen van de Oekraïne zien, afhankelijk van de plaats waar de internetgebruiker zich bevindt. Google besloot geen zaken meer te doen in China, nadat het opdracht had gekregen resultaten te filteren. Twitter honoreert verzoeken van autoriteiten om *tweets* te verwijderen, maar blokkeert de *tweet* alleen voor het betrokken land. In andere landen blijft de *tweet* zichtbaar. Door resultaten lokaal aan te passen kan een bedrijf actief blijven in landen waar de vrijheid van meningsuiting wordt beperkt, maar werkt zo wel mee aan censuur. Dit doet de functie van het internet als platform voor discussie tekort. Aangezien de inhoud in de rest van de wereld wel zichtbaar blijft, worden internetgebruikers in andere landen wel geïnformeerd.

In deze aaneenschakeling van conflicterende posities is het moeilijk om bedrijven tot instrument te maken van een door de regering voorgestaan mensenrechtenbeleid. Op dit gebied gebeurt al veel, zoals de Ruggie *framework principles* van de VN laten zien.[156] De bijzondere urgentie in het domein van de communicatie is dat de wereldwijde openbare en privécommunicatiekanalen en diensten in handen zijn van deze ondernemingen. Een beleid ten aanzien van deze communicatieondernemingen heeft slechts kans van slagen als er coalities worden gevormd op internationale fora. Een voorbeeld is de Snowdenzaak, waar zich een Europese consensus aftekent dat het PRISM-programma niet in deze vorm kan worden voortgezet, omdat het de rechten van Europese burgers schendt. Niettemin acht de AIV het gewenst dat Nederland een beleid uitdraagt waarin in Nederland werkzame bedrijven worden aangespoord het Nederlandse mensenrechtenbeleid te respecteren. Niet goed valt in te zien waarom Nederland met autoritair geregeerde landen een mensenrechtendialoog onderhoudt, maar niet met bedrijven die voor de handhaving van privacy en vrijheid van communicatie in de wereld essentieel zijn.

154 Zie: <http://en.wikipedia.org/wiki/Warrant_canary>.

155 Zie: <http://gigaom.com/2014/05/21/twitters-selective-censorship-of-tweets-may-be-the-best-option-but-its-still-censorship/>.

156 A/HRC/17/31.

VI Samenvatting, conclusies en aanbevelingen

Samenvatting en conclusies

In hoofdstuk II is uiteengezet dat het internet zich vanuit de internetgemeenschap heeft losgemaakt van een klassieke internationaalrechtelijke structuur van een verdrag (waarin de mondiale afspraken over telecommunicatie vastlagen), een internationale organisatie (de Internationale Telecommunicatie Unie) en daarin samenwerkende nationale staten. Daarvoor in de plaats is een semi-privaatrechtelijk *multistakeholder*model gekomen, bestaande uit ICANN (namen en adressering) en een verzameling technische groepen, die over de standaarden en protocollen van het internet gaan. Dit ging gepaard met een technische omwenteling in de wijze van het versturen van data en een sociale omwenteling in de wijze van communiceren. ICANN is formeel nog opgehangen aan het Amerikaanse ministerie van Handel. Na de Snowdenaffaire is het algemene gevoelen dat deze band niet langer kan worden gehandhaafd. Gezocht wordt naar een nieuwe structuur, gebaseerd op het *multistakeholder*model.

Deze vorm van *governance* beperkt zich tot de technische lagen van het internet, al bestaat er ook over deze enge opvatting van *governance* binnen de internetgemeenschap geen consensus (zie hoofdstuk V.2). Naast deze nieuwe internetstructuur blijft de oude organisatie ITU actief proberen haar invloedssfeer uit te breiden, recent in een poging de *International Telecommunications Regulations* op de *World Conference on International Telecommunications* in Dubai aan te passen, tot op heden zonder succes. Binnen de ITU proberen staten als Rusland en China een grotere greep op internetcommunicatie te krijgen, ook op de inhoud. Vanuit de VN is echter ook een nieuwe ontwikkeling gestart met het *Internet Governance Forum*. In dit mondiale platform proberen staten in samenwerking met andere belanghebbenden consensus over het begrip *internetgovernance* te bereiken. Tot op heden met gedeeltelijk succes, omdat het – buiten de meer technische zaken – heel moeilijk is consensus te bereiken over onderwerpen waarbij verschillende waardeopvattingen zijn betrokken. Tegen deze achtergrond zijn de vragen van de regering beantwoord.

De eerste vraag van de regering was: hoe kan zij zorgdragen voor een zo effectief mogelijke verankering en verdere operationalisering van internetvrijheid in Nederlands binnenlands en buitenlands beleid? In hoofdstuk III is deze vraag op conceptueel niveau besproken. Ten eerste wordt uiteengezet dat het bestaande grondrechtelijke communicatie- en privacykader niet meer past bij de huidige stand van de techniek. Tegelijkertijd blijkt dat het met beraad en voorzichtigheid moet worden aangepast, omdat een aanpassing kan leiden tot een verlaging van het beschermingsniveau. Dit wordt onder meer gedemonstreerd aan de hand van het communicatiegeheim en verkeersgegevens. Het communicatiegeheim is in een netwerksamenleving niet langer een statisch gegeven, maar een bescherming voor hoe en in welk verband een individu vrij kan communiceren. Een tweede belangrijk punt is dat juridische begrippen òf voor een andere technische werkelijkheid dan het huidige internet zijn ontworpen (bijvoorbeeld het begrip verwerken uit het dataprotectierecht) òf uitgaan van een situatie waarin een duidelijk onderscheid te maken valt tussen het transport van de boodschap en het uiten van de boodschap (uit het media- en telecommunicatierecht). Twee andere belangrijke met elkaar verweven vragen zijn internationale jurisdictie en universaliteit versus nationale soevereiniteit. Deze tegenstelling openbaart zich vooral in de moeizame onderhandelingen van de EU met de VS over de *safe harbour*-beginselen

bij dataprotectie. Verder is een belangrijk punt van aandacht de voortschrijdende erosie van het begrip persoonsgegevens, als gevolg van ontwikkelingen zoals *Big Data* en *mass* of *targeted surveillance* van burgers. Velen veronderstellen ten onrechte dat verkeersgegevens per definitie geen persoonsgegevens zijn, terwijl uit een verzameling verkeersgegevens (individuele) profielen kunnen worden samengesteld. De veronderstelling dat anonieme gegevens op grote schaal verzameld mogen worden zonder effectief toezicht, is dan ook onjuist.

Verder wordt geconstateerd dat veiligheid moet worden geplaatst in de context van de rechtsstaat. Het nastreven van het onbereikbare ideaal van *precluded event security* kan leiden tot maatregelen die disproportioneel zijn en de rechtsstatelijke balans aantasten.

Daarnaast is in dit advies gewezen op de strijd die gaande is rond de verbreding van het begrip *governance* van het internet; ook deze is belangrijk voor de verankering van internetvrijheid. Deze strijd speelt zich onder andere af in de ITU (paragraaf II.3). Ook het debat rond de nieuwe organisatie die in de plaats zal komen van ICANN, is van groot belang omdat controle over de *root* kritisch is voor internetvrijheid en omdat ICANN de spin in het web is van *internetgovernance* (paragraaf V.1). Het *Internet Governance Forum* lijkt een geschikt forum om kwesties rondom de operationalisering van internetvrijheid te bespreken, maar het secretariaat van dit forum lijdt onder een gebrek aan personele en financiële middelen.

Bovendien kan de regering een bijdrage leveren aan de bevordering van internetvrijheid door dezelfde normatieve uitgangspunten te hanteren in binnenlandse beleidsdiscussies als die zij uitdraagt in het buitenland. Hier dreigt het risico dat op zichzelf vrije constitutionele democratieën een Janusgezicht ontwikkelen van rechtsstatelijk gewaarborgde vrijheid gecombineerd met onvoldoende rechtsstatelijk gewaarborgde beperking van de vrijheid, zoals is uiteengezet in paragraaf V.2. Dat gaat op dit moment in de VS ten koste van de geloofwaardigheid van de VS, hetgeen in de studie *Foreign Policy begins at home* van Richard Haass, president van de Council on Foreign Relations, werd bekritiseerd.[157]

De tweede vraag was of de Nederlandse jurisdictie ten aanzien van internetvrijheid zich alleen uitstrekt over het eigen grondgebied, of dat dit door de toegenomen technische mogelijkheden ook op situaties buiten het eigen grondgebied ziet. Indien de jurisdictie niet zover strekt: op welke wijze kan de Nederlandse overheid buiten de eigen grenzen effectief aan bewaking van internetvrijheid bijdragen? Op het internet is de productie, opslag en verspreiding van informatie niet meer aan plaats en tijd gebonden. Het internet kent geen nationale grenzen. De technische mogelijkheden zijn weliswaar toegenomen, maar dit impliceert niet dat bevoegdheden ook ruimer zijn. In paragraaf V.2.2 is deze vraag toegespitst op het in consultatie gebrachte concept voor een wetsvoorstel computercriminaliteit III. Naar de mening van de AIV voorziet dit conceptwetsvoorstel in ruimere bevoegdheden dan het volkenrecht toelaat.

Niettemin blijven de nationale staten een belangrijke rol vervullen omdat de fysieke infrastructuur van het internet begint en eindigt binnen een gebied waarover zij feitelijke en juridische rechtsmacht hebben. De vragen ten aanzien van toegang en vrije en niet gecontroleerde communicatie concentreren zich dus nog steeds binnen de nationale

157 Richard N. Haass, Foreign Policy begins at home. The Case for Putting America's House in Order, New York: Basic Books 2014.

rechtssfeer. De hoofdstukken III en V, waarin toegangs-, surveillance- en censuurvragen aan de orde komen, laten zien dat het gaat om nationale beslissingen die getoetst worden aan internationale (of regionale: EVRM en EU) verdragen. In paragraaf V.4 is daarentegen toegelicht dat de grote internationale ondernemingen, die een grote rol spelen bij de toegang en het vrije gebruik van het internet, slechts voor een beperkt deel onder de Nederlandse invloedssfeer vallen, namelijk alleen als het handelingen betreft die binnen de Nederlandse rechtssfeer worden verricht. Bovendien is er regelmatig discussie over wanneer dat bij internetdiensten precies het geval is. Het Google Spanje-arrest van het HvJ EU brengt op dit punt een doorbraak.

De derde vraag was in hoeverre bedrijven verantwoordelijk zijn voor de bescherming van internetvrijheid van burgers in de landen waar ze actief zijn en hoe de Nederlandse overheid, zelfstandig en samen met andere landen bedrijven kan oproepen die verantwoordelijkheid op te pakken. In dit advies is uiteengezet dat de organisatie van de moderne elektronische communicatie sterk verschilt van de periode waarin vaste telefoon en telex de belangrijkste communicatiemiddelen waren. In de plaats van staatsmonopolies in een internationaal publiekrechtelijk kader is een systeem gekomen van vele spelers. In dit systeem is de rol van bedrijven groot; dit is op verschillende plaatsen in dit advies besproken, met name in hoofdstuk II en in paragraaf V.4. Bedrijven hebben een belangrijke rol in de *governance* van het internet en zijn de aanbieders van diverse diensten zoals zoekmachines, *cloud* (paragraaf III.4.1 en IV.3.2) en e-mail. Soms worden bedrijven gedwongen op te treden als verlengstuk van de overheid, zoals bij dataretentie (paragraaf III.2) of censuur, waartegen zij zich al dan niet verzetten (paragraaf V.3). Bedrijven hebben zodoende een aanzienlijke invloed op de internetvrijheid.

Geconstateerd kan worden dat de positie van internetbedrijven juridisch niet altijd helder is. Zo is in Nederland voor sociale media niet duidelijk of zij vallen onder het telecommunicatierecht of onder het mediarecht. Het antwoord op die vraag heeft belangrijke gevolgen voor de mate waarin dergelijke bedrijven kunnen worden aangesproken op de inhoud van communicaties en publicaties. Verder kunnen bedrijven klem komen te zitten tussen nationale jurisdicties met verschillende rechtsregimes. Voor bedrijven zijn commerciële overwegingen gewoonlijk doorslaggevend, ook waar het gaat om de verzameling, verwerking en opslag van gegevens van internetgebruikers. Het antwoord op de vraag in hoeverre bedrijven verantwoordelijk zijn voor de bescherming van internetvrijheid is juridisch nog niet te geven. Deze vraag moet worden geplaatst binnen de bredere context van het maatschappelijk verantwoord ondernemen. Daarvoor is het Ruggie-raamwerk opgesteld, dat onderwerp is van internationaal overleg, maar dat in dit domein wel bijzondere relevantie krijgt.

Aanbevelingen

Aanbeveling 1
In paragrafen III.2, III.4 en IV.3.2 is uiteengezet dat gegevens van Nederlandse internetgebruikers tegenwoordig vaak worden opgeslagen op computerservers die zich veelal buiten de Nederlandse rechtssfeer bevinden. De staten waar die servers zich bevinden, zijn meestal bevoegd onder bepaalde omstandigheden toegang tot die gegevens te eisen. Omdat computers slecht kunnen rekenen met versleutelde gegevens en de servers waarop deze gegevens zijn opgeslagen zich vaak bevinden in jurisdicties waar Nederlanders geen rechtsbescherming hebben, is de *cloud* potentieel zo lek als een mandje. *Safe Harbour*-overeenkomsten zijn daartegen geen afdoende beveiliging, omdat ze ontoereikend zijn, slecht of niet afdwingbaar zijn en te grote uitzonderingen

met betrekking tot nationale veiligheid kennen. Deze risico's verdienen de volle aandacht van het kabinet.

De Nederlandse regering voert een beleid om zoveel mogelijk alle relaties tot de burgers in het binnenland via *cyberspace* te laten plaatsvinden: overheidsdossiers, registers en overheidstransacties moeten in 2017 allemaal elektronisch worden in het kader van Nederland Digitaal. Naar het oordeel van de AIV is het urgent na te gaan of bij de opslag en verwerking van gegevens het risico bestaat dat deze buiten de Nederlandse rechtssfeer terechtkomen, waar ze technisch en juridisch niet voldoende zijn te beveiligen. Er dienen beleidsmatige en wettelijke maatregelen te worden genomen om dat te voorkomen, althans juridische waarborgen te scheppen om toegankelijkheid van bestanden aan dezelfde rechtswaarborgen te binden als die hier gelden (zie paragrafen III.5.1 en III.5.2). Verder is van belang dat ook de rechtsbescherming voldoende is gewaarborgd.

Aanbeveling 2
Nederland heeft economisch een goede uitgangspositie op de internetmarkt. Het kan deze positie verbeteren door een positief vestigingsbeleid te creëren in de vorm van een in alle opzichten optimale bescherming van de internetvrijheid in alle facetten die in dit advies zijn belicht. Het organiseren van internationale conferenties en instituten heeft een positieve *spin-off*, maar dat blijft vluchtig als het niet wordt verankerd in de Nederlandse internetgemeenschap. Als onderdeel van het internationaal bevorderen van optimale internetvrijheid zou Nederland een positief vestigingsklimaat in Nederland voor internetbedrijven kunnen creëren en concentratie van internetspecialisten in innovatieve wetenschapscentra binnen de universiteiten kunnen stimuleren. Het zou voorts binnen het ministerie van Economische Zaken, dat hierin een sleutelrol vervult, tot een betere coördinatie kunnen komen tussen de directies die met internet hebben te maken.

Aanbeveling 3
Het vertrekpunt van het mensenrechtenbeleid (een van de hoekstenen van het buitenlandbeleid) is dat Nederland zelf, zonder perfectie te pretenderen, een voorbeeld wil stellen, vooral in de zin van openheid en toetsbaarheid: democratie en vrijheid in eigen huis is de maatstaf. Dit impliceert dat Nederland ook nationaal bij de hiervoor aangesneden internetkwesties het hoge beschermingsniveau moet nastreven dat het internationaal uitdraagt. Dit is een verantwoordelijkheid van alle ministeries, met name ook van die ministeries bij welke thans de internetdossiers berusten.

Bij de aanhangige grondwetswijziging, de voorziene aanpassing van de Wiv 2002 en het concept voor een wetsvoorstel computercriminaliteit III dat in consultatie is gebracht, moet een punt van bijzondere aandacht zijn of Nederland een beleid voert en/of een regeling maakt waarmee het internationaal voor de dag kan komen.

Aanbeveling 4
Het verzekeren van effectief en onafhankelijk toezicht op inlichtingen- en veiligheidsdiensten heeft in de VS na de Snowdenaffaire veel aandacht gekregen en is ook in Nederland door de evaluatie van de Wiv 2002 aan de orde gesteld, onder andere in de door het CDA ingediende motie in de Eerste Kamer der Staten-Generaal, die werd aanvaard op 7 oktober 2014 (Eerste Kamer der Staten-Generaal, vergaderjaar 2014-2015, CVIII, D). De in juli 2012 door de Mensenrechtenraad van de Verenigde Naties aangenomen resolutie '*The promotion, protection and enjoyment of Human Rights on the Internet*', volgens welke mensen *online* dezelfde rechten hebben als *offline*, moet maatgevend zijn voor het Nederlandse beleid. Indien, vanwege de permanente terreurdreiging, middelen worden ingezet tegen (categorieën van) personen tegen wie geen gerichte

verdenking bestaat, dan is dit rechtsstatelijk alleen te rechtvaardigen als er effectief en onafhankelijk toezicht bestaat. Het versterken van effectief en onafhankelijk toezicht door het College bescherming persoonsgegevens en de CTIVD op de rechtmatigheid en proportionaliteit van opsporings- en preventiemaatregelen, acht de AIV bij de huidige stand van de techniek en de gewijzigde internationale verhoudingen van groot belang voor de internetvrijheid, zoals deze in dit advies is gedefinieerd.

Aanbeveling 5
Nederland zal in 2014 ongeveer 53,5 miljoen aan het mensenrechtenbeleid (inclusief Wereldomroep) besteden. Een deel daarvan wordt uitgegeven ter bevordering van internetvrijheid. Nederland ondersteunt diverse belangrijke projecten met menskracht en geld op het gebied van internetvrijheid. Echter, een coherente visie ten aanzien van het internet en de verschillende facetten die daarbij moeten worden onderscheiden en geaccentueerd, valt niet waar te nemen. Aan keuzes ten aanzien van de ondersteuning van dergelijke activiteiten zou een algemene onderbouwing en prioritering moeten voorafgaan, gericht op de ook voor Nederland relevante facetten van de internetproblematiek. Daarbij zou de regering in overleg met het veld gericht maatregelen kunnen ontwikkelen die vrijheid en beveiliging van het internet bevorderen, zoals het ontwikkelen en beschikbaar stellen van *open source software*. De AIV beschouwt het als een duidelijke leemte dat er weinig aandacht is voor de verbetering van internationale beleidsvorming (zoals het *Internet Governance Forum* en de reorganisatie van ICANN).

Aanbeveling 6
Ook in de EU-dossiers is veel aan de hand. Nederland neemt een afwachtende houding aan over het al dan niet voortzetten van het *Safe Harbour agreement* en de onderhandelingen over het *Umbrella agreement*. Nederland beschikt over ruimschoots voldoende kennis van zaken om bij deze onderwerpen een meer leidende rol te spelen. Nederland moet het standpunt innemen dat voortzetting van de *Safe Harbour*-overeenkomst zonder ingrijpende verbeteringen niet meer kan dienen als basis voor gegevensuitwisseling met de VS in de particuliere sector. Nederland kan het voorzitterschap van de Europese Unie in 2016 benutten om voorstellen voor de EU te ontwikkelen met als doel de bestaande verouderde wetgeving die effecten heeft op internetvrijheden, te actualiseren.

Aanbeveling 7
Een punt van bijzondere aandacht is de uitwisseling van gegevens tussen nationale inlichtingen- en veiligheidsdiensten binnen Europa en daarbuiten van betere waarborgen te voorzien dan momenteel het geval is. Bij de herziening van de Wiv 2002 moet de uitwisseling van gegevens tussen Nederlandse en buitenlandse inlichtingen- en veiligheidsdiensten wettelijk worden geregeld, waarbij voldoende waarborgen voor de burger worden geboden, zoals uiteengezet in paragraaf III.2.

Aanbeveling 8
De activiteiten van bedrijven en internetorganisaties waarin bedrijven dominant zijn, kunnen een aanzienlijke invloed uitoefenen op de internetvrijheid. Bedrijven worden primair geleid door het winstoogmerk en hebben met uiteenlopende nationale en internationale wettelijke kaders te maken. Het is de rol van de overheid om te monitoren of nieuwe software, protocollen en dergelijke inbreuk maken op de Europese interpretatie van de vrijheid van meningsuiting, privacy en dataprotectie. NGO's kunnen daarbij een signalerende rol spelen.

De vraag hoe internationaal opererende bedrijven bij de uitvoering van het Nederlandse mensenrechtenbeleid betrokken kunnen worden, staat al lang op de agenda. In het kader van dit advies is zij wel zeer urgent omdat een klein aantal internationale ondernemingen verantwoordelijk is voor de internationale vertrouwelijke en openbare communicatie en de waarborgen waarmee deze moeten worden omgeven. De regering moet daarom de verantwoordelijkheid van deze bedrijven op internationale fora aan de orde stellen en met deze bedrijven een mensenrechtendialoog aangaan, zoals zij dat ook bij buitenlandse regeringen pleegt te doen.

Aanbeveling 9
Vragen die met internetvrijheid verbonden zijn, zo blijkt op tal van plaatsen uit dit advies, zijn departementsoverstijgende vragen en bovendien steeds meer verbonden met verantwoordelijkheden die door het bedrijfsleven en andere belanghebbenden moeten worden gedragen. De departementsoverstijgende zaken maken de uitvoering van het Nederlandse mensenrechtenbeleid, bij uitstek in dit domein, tot een gedeelde verantwoordelijkheid. De AIV beveelt daarom aan dat coördinatie en gedeelde verantwoordelijkheid wordt nagestreefd bij de beleidsvoorbereiding en -vorming in de internetdossiers.

Aanbeveling 10
Nederland moet een consistenter beleid voeren ten aanzien van de vraag op welke internationale fora en in welke coalities zij diverse internetstandpunten wil vertolken. Het ministerie moet meer geld en mankracht investeren in het *Internet Governance Forum*. Voorts zou het binnen ICANN en andere internetorganisaties privacybevorderende maatregelen kunnen uitdragen. Een voorbeeld daarvan werd gegeven in pararagraaf V.1: de WHOIS van de Stichting Internet Domeinregistratie Nederland, die de domeinnamen voor het domein .nl registreert, toont geen adresgegevens van de domeinnaamhouder; gerechtsdeurwaarders en advocaten kunnen die wel opvragen. Nederland zou een dergelijke oplossing ook internationaal kunnen uitdragen.

Aanbeveling 11
Bij de beleidsvorming ten aanzien van internetvrijheid zijn diverse ministeries betrokken: de ministeries van Buitenlandse Zaken, van Veiligheid en Justitie, van Economische Zaken, van Binnenlandse Zaken en Koninkrijksrelaties en van Defensie. Het ministerie van Economische Zaken voert ter voorbereiding op internationale bijeenkomsten regelmatig overleg met Nederlandse belanghebbenden. Dit is een voorbeeld dat andere ministeries kunnen volgen. Uit gesprekken met deskundigen is de indruk ontstaan dat het ministerie van Buitenlandse Zaken weinig aansluiting heeft met de Nederlandse internetgemeenschap. Het is wenselijk dat het ministerie van Buitenlandse Zaken meer personele capaciteit beschikbaar maakt voor het op peil brengen en houden van de kennis met betrekking tot het internet en voor het versterken van de contacten met de internetgemeenschap in binnen- en buitenland, ook ten aanzien van de EU.

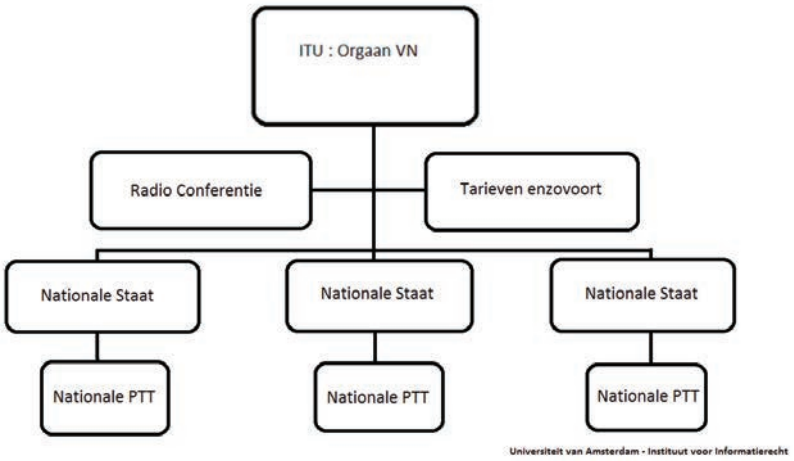
Bijlagen

Aanvullende informatie bij de voorgeschiedenis van de huidige telecommunicatie

Technische infrastructuur: van telefoon naar het internet

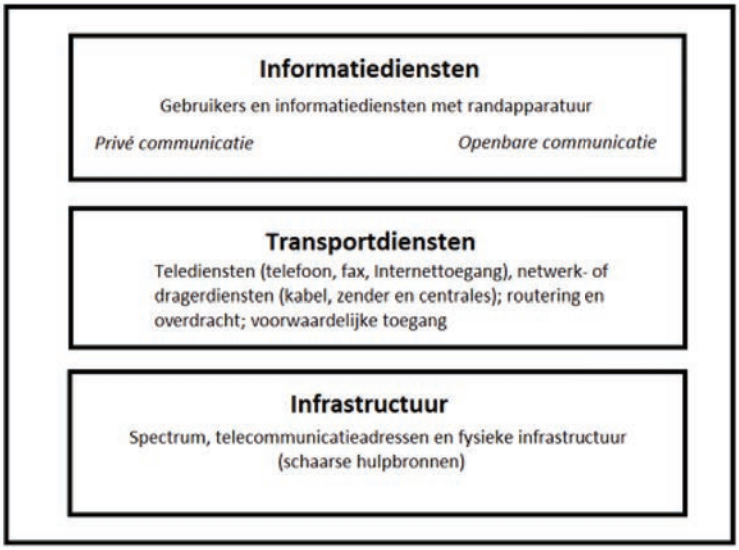
In paragraaf II.1 is uiteengezet dat het internationale telefoonverkeer en het eenduidige gebruik van frequenties een stabiel internationaal juridisch kader en een overlegstructuur vergden. De kenmerken van de toenmalige internationale telecommunicatiestructuur zijn als volgt schematisch voor te stellen.

De organisatie van de telefonie



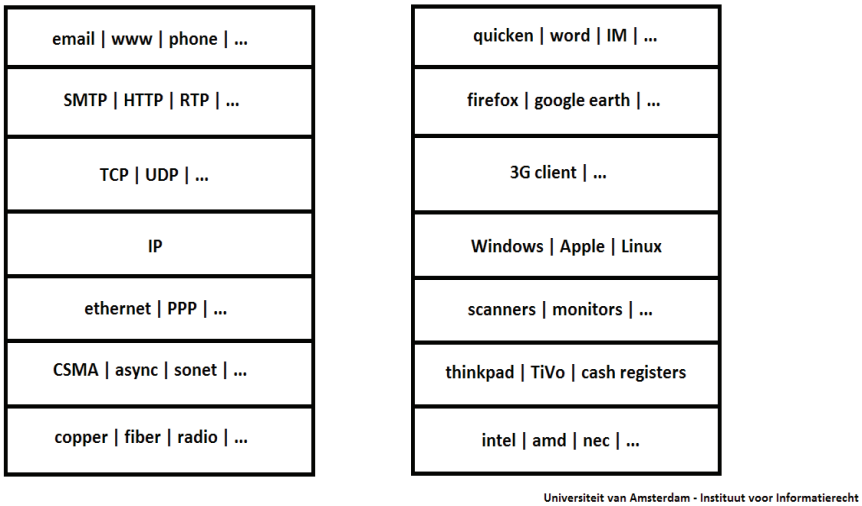
Binnen dit organisatiemodel ontwikkelden de nationale PTT's een lagenmodel waarin het gehele communicatiekanaal technisch werd vormgegeven, het zogenaamde *Open System Interconnection* model (OSI-model). In de onderste laag bevindt zich de fysieke infrastructuur (de kabels, frequenties en centrales), daarboven op elkaar gestapelde diensten voor de omzetting van menselijke taal naar machinetaal, voor routering, voor beveiliging, voor adressering et cetera. Die diensten communiceerden met elkaar volgens vaste standaarden. Een belangrijke eigenschap van dit model is dat de typische menselijke communicatie (inhoud) en de technische telecommunicatie (de gegevens die nodig zijn om de communicatie op het juiste adres te krijgen, de verkeersgegevens) nauwkeurig van elkaar zijn gescheiden. De PTT's gingen alleen over het laatste volgens het adagium 'geen boodschap aan de boodschap'. Schematisch kan dit lagenmodel als volgt worden voorgesteld:

Diensten, transport en infrastructuur



In het schematische lagenmodel kan de loskoppeling van diensten en toepassingen van de infrastructuur als volgt worden weergegeven, links het netwerk, rechts de computer.[158] De verschillende afkortingen staan voor de op elkaar gestapelde met elkaar samenwerkende protocollen en software applicaties die respectievelijk op het internet en een PC anno 2014 met elkaar samenwerken. De onderste laag vormt de fysieke laag. De bovenste lagen van de applicaties op de PC zijn de lagen die met het internet communiceren of daarop draaiende diensten.

Ontbundeling van het lagenmodel in telecommunicatie en computers



158 Bron: Jonathan Zittrain, The Future of the Internet and How to Stop It, New Haven/London: Yale University Press 2008, pp. 68-70.

De concurrentie op alle niveaus van het communicatiekanaal en de steeds grotere en snellere bandbreedten en media (glas, licht, digitale frequenties, digitale geheugenopslag) en het andere communicatiepatroon van het publiek (van telefoneren naar het verzenden van multimediale berichten) hebben ertoe geleid dat het internet aan het eind van de 20ste eeuw een even grote communicatierevolutie is als telefonie en radio waren aan het eind van de 19de eeuw. Maar het maakt nog steeds gebruik van die toen gelegde infrastructuur.

Het internet heeft een soortgelijke hiërarchische structuur als het OSI-model. Het kent ook een duidelijke fysieke laag. Het verschil met het OSI-model is dat de scheiding tussen inhoud en transport lastiger te maken is. Het verschil met de telefonie is dat het pakketgeschakeld is. Dat wil zeggen dat voor een communicatie geen unieke verbinding nodig is. Bovendien kent het geen centrales waar al het verkeer door moet. Naast een diversiteit van diensten voor korte berichten (van e-mail tot twitter) kent het internet door het *world wide web* (www) krachtige toepassingen van verkenners- en zoekmachines die het hele net afgrazen en documenten, beeld en geluid wereldwijd toegankelijk maken (bijvoorbeeld door Google en YouTube).

Organisaties rondom het ontstaan van het internet

De *Internet Activities Board* (IAB) dateert uit 1983 en is de voorloper van de huidige *Internet Architecture Board*. Het was de eerste poging de *governance* van het internet te formaliseren. Zij is sterk verbonden gebleven met de *Internet Engineering Task Force* (IETF), van begin af aan een informele club waar over open standaarden werd gesproken. Zij vormde een soort anti-OSI-beweging. De OSI-overlegorganen, bevolkt door PTT-ingenieurs, werden gezien als formeel, op staatsgezag en eigendom gebaseerd en het tegendeel van wat de internetgemeenschap voorstond: een horizontale organisatie gebaseerd op open standaarden.

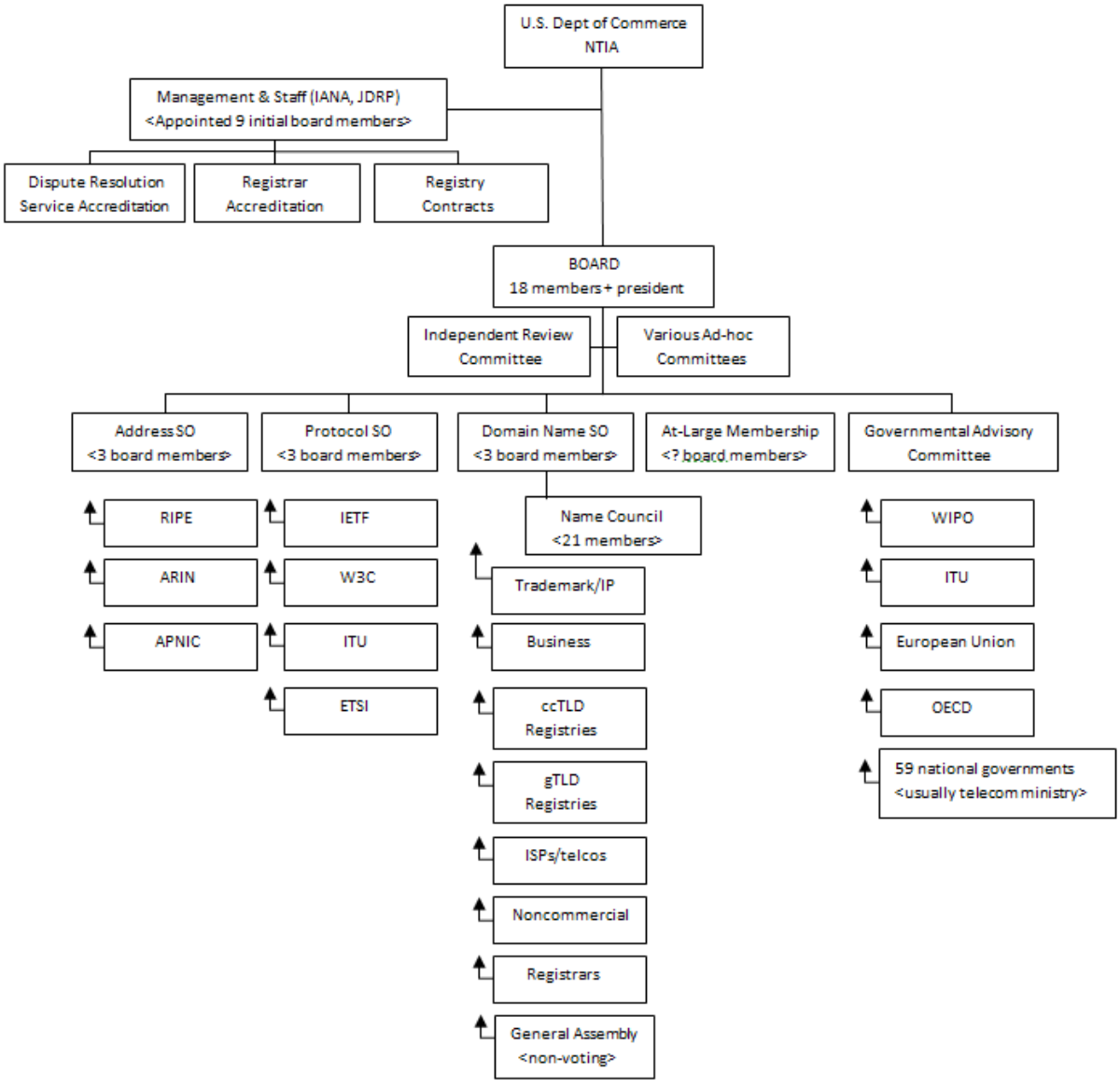
De IETF formuleert nog steeds protocollen, standaarden en specificaties voor het internet. De IETF heeft geen instrumenten om naleving daarvan af te dwingen. Dat is ook niet nodig, omdat de protocollen, standaarden en specificaties nog steeds (conform het oorspronkelijke ideaal) vrijwillig worden nageleefd. Indien een bedrijf of individu dat niet zou doen, dan zou dat bedrijf of dat individu bovendien moeizaam of geen toegang krijgen tot het internet. Het belang van interconnectiviteit en gemeenschappelijke normen en waarden (zie de analyse van Nye in hoofdstuk I) bevorderen de naleving van de norm. Iedereen kan deelnemen aan het werk van de IETF. De protocollen, standaarden en specificaties komen tot stand op basis van consensus binnen werkgroepen. De IETF is geen rechtspersoon, maar opereert nu onder de vlag van de *Internet Society*.

De *Internet Assigned Numbers Authority* (IANA) ontstond in 1988. IANA werkte op basis van een contract met DARPA, een agentschap van het Amerikaanse ministerie van Defensie dat aan de basis heeft gestaan van de ontwikkeling van het internet. In dit contract werd een sleutelfiguur in de ontwikkeling van het internet, Jon Postel, min of meer aangewezen als de autoriteit *'the IANA'*. IANA ging zich bezighouden met de ontwikkeling van de IP-adressen en daarmee verbonden activiteiten. Ook hier hetzelfde beeld: een 'autonome ontwikkeling'. Milton Mueller formuleert het als volgt:[159] '*Explicit claims on the right to manage name and address assignment were being made by an*

159 Milton Mueller, Ruling the Root, Massachusetts: Massachusetts Institute for Technology, 2002, p. 93.

authority (…) that lacked any basis in formal law or state action. The authority claims nevertheless had significant legitimacy within the technical community.'

In onderstaand schema is de organisatiestructuur van ICANN bij de stichting weergegeven.[160] Onder het bestuur van ICANN hangen diverse adviserende organen: de *Address Supporting Organization*, de *Protocol Supporting Organization*, de *Domain Name Supporting Organization*, de *At Large Membership* en het *Governmental Advisory Committee*. Deze adviserende organen bestaan uit vertegenwoordigers van de organisaties die in het schema staan vermeld in de kolom onder de respectievelijke adviserende organen. De *Supporting Organizations* hebben onder andere tot taak consensus te creëren binnen het deel van de internetgemeenschap dat zij vertegenwoordigen.



160 Idem, p. 173, figuur 8.1.

Kort samengevat gaat het over adressen (uiterste linker kolom), protocollen en standaarden (tweede kolom links) en namen (middelste kolom). De meest rechter kolom vertegenwoordigt de oude belanghebbenden en staatsbelangen. De tweede kolom van rechts (*at large*) vertegenwoordigt NGO's die niet in de andere kolommen passen. In het schema is ISOC niet opgenomen, maar ISOC onderhoudt banden met verschillende organisaties, die worden genoemd in het schema. Inmiddels is de *Protocol Supporting Organization,* de technische poot (tweede kolom links), opgeheven. ICANN is de spin in het web. Het Amerikaanse ministerie van Handel stuurt via de *National Telecommunications and Information Administration* deze optocht van oude en nieuwe vertegenwoordigers van de wereldtelecommunicatie.

In deze gremia is jarenlang overleg gepleegd over de overgang van de IPv4-nummers naar de langere IPv6-nummers, om de schaarste op te heffen die bij de kortere nummers dreigde. De invoering daarvan vindt nu geleidelijk plaats. Binnen ICANN is de belangrijkste beleidsdiscussie de invoering en toekenning van nieuwe *Toplevel* domeinen (gTLD's). Dit is een vrij heftige discussie tussen de belanghebbenden voor merken en geografische herkomstaanduidingen en de invoering van generieke namen (voorbeeld: nieuwe gTLD's als '.wine', '.amazon', '.patagonia'). Voor de nieuwe domeinen zijn thans tenderprocedures gaande.

ICANN heeft een *Joint Project Agreement* en een contract met het Amerikaanse ministerie van Handel voor de toewijzing van internetadressen en het beheer van gTLD's. Dit contract draagt de volgende taken op aan ICANN:
- ontwikkeling van beleid voor de toewijzing van blokken van IP-adressen;
- toezicht op het systeem van *root servers*;
- toezicht op het beleid voor toevoegingen aan de *root* (nieuwe domeinen);
- coördinatie van andere technische parameters teneinde de universele connectiviteit van het internet in stand te houden;
- andere activiteiten die noodzakelijk zijn voor het beheer van het systeem van domeinen, zoals overeengekomen tussen het ministerie en ICANN.

Het *Joint Project Agreement* is herhaaldelijk verlengd en gewijzigd, waarbij de autonomie van ICANN geleidelijk is vergroot, al houdt het ministerie van Handel een toezichthoudende rol.[161] In de *Affirmation of Commitments* tussen het ministerie van Handel en ICANN van 30 september 2009 is het *Joint Project Agreement* voor onbepaalde tijd verlengd.[162] Het *National Telecommunications and Information Administration* van het ministerie van Handel heeft zich ontwikkeld tot een soort procesbewaker. Alle betrokkenen konden daarmee leven, maar de band tussen ICANN en de VS is door de Snowdenaffaire onhoudbaar geworden.

ICANN wordt bestuurd door een *board of directors*. Daarin is een aantal groepen vertegenwoordigd. De *board* bestaat uit 20 personen, waarvan 16 stemrecht hebben. De helft van de stemgerechtigde leden wordt voorgedragen aan de *board* door het *Nominating Committee*. De anderen worden gekozen door organen van ICANN, onder andere de *country-code Names Supporting Organization* (waarvan organisaties lid kunnen

161 Lee A. Bygrave e.a., The naming game: governance of the Domain Name System, in: Lee. A. Bygrave and Jon Bing, Internet Governance, infrastructure and institutions, Oxford, Oxford University Press, 2009, pp. 151-153.

162 Zie: <http://www.ntia.doc.gov/page/docicann-agreements>, geraadpleegd op 5 juni 2014.

worden die landenspecifieke topdomeinen beheren), de *generic Names Supporting Organization* (waarvan organisaties lid kunnen worden die algemene topdomeinen beheren) en de *at large* leden. Verder kent de *board* vijf adviserende leden, waaronder vertegenwoordigers van de *Governmental Advisory Committee*, waarvan elke staat lid kan worden) en de *Internet Engineering Task Force*. Het *Nominating Committee* is eveneens samengesteld uit vertegenwoordigers van diverse belanghebbende groepen. Verder moeten de *board of directors* onder andere culturele en geografische diversiteit weerspiegelen.[163] Er zijn echter vele kruisverbanden tussen de hiervoor genoemde organisaties en organen, waardoor de structuur van ICANN ondoorzichtig is. Zo is een aantal organisaties dat lid is van de *board*, ook vertegenwoordigd in het *Nominating Comittee.* De inkomsten van ICANN bestaan onder andere uit de jaarlijkse afdrachten voor het gebruik van toplevel domeinnamen. Dat is een aanzienlijk bedrag aangezien er nu alleen al 125 miljoen .com domeinnamen zijn geregistreerd en er nog vele andere algemene topdomeinen zullen komen. Er bestaan strikte interne controleregels voor de financiën, maar toch heeft de *Chief Executive Officer* van ICANN nog vrij vergaande discretionaire bevoegdheden voor de besteding van gelden aan onder meer goede doelen. Dit past in de rechtsvorm van een goede doelen vennootschap naar Californisch recht, want zo moet men ICANN uiteindelijk juridisch kwalificeren.

WGIG slaagde erin een definitie van *internetgovernance* te formuleren (zie paragraaf V.1), maar bleef vaag over de reikwijdte van dit begrip. Verder identificeerde WGIG beleidsvraagstukken die relevant zijn voor de *governance* van het internet, maar kon niet tot inhoudelijke aanbevelingen komen. WGIG constateerde dat er geen internationaal forum is waar de geïdentificeerde beleidskwesties kunnen worden besproken en adviseerde dan ook een mondiaal *multistakeholder*forum in te stellen. Over de institutionele vormgeving voor de *governance* van het internet kon WGIG geen overeenstemming bereiken en daarom bevat het rapport vier modellen voor de institutionele *governance* van het internet. Een van de elementen daarin was de rol van ICANN. In één van de modellen zou ICANN komen te vallen onder een orgaan van de VN. Verder stelde WGIG dat geen enkele regering een geprivilegeerde rol in *internetgovernance* mocht hebben, een aanbeveling die expliciet gericht was tegen de dominante positie van de VS in het beheer van domeinnamen.

163 Zie: <https://www.icann.org/resources/pages/bylaws-2012-02-25-en#/II>, geraadpleegd op 5 juni 2014.

Bijlage IIa

Adviesaanvraag

Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de Adviesraad Internationale Vraagstukken
Mr. J.G. de Hoop Scheffer
Postbus 20061
2500 EB DEN HAAG

Postbus 20061
2500 EB Den Haag
Nederland
www.rijksoverheid.nl

Contactpersoon
Simone Halink

T +31 70 348 4777

Onze referentie
MINBUZA-2014.80946

Datum 20 februari 2014
Betreft Aanvraag voor AIV-advies over internetvrijheid

Geachte voorzitter,

Binnen het Nederlandse buitenlandse mensenrechtenbeleid is het thema 'internetvrijheid' een belangrijk speerpunt. Uitgangspunt bij 'internetvrijheid' is dat fundamentele rechten offline in beginsel ook online gelden, waarbij in het bijzonder het recht op privacy, gegevensbescherming en het communicatiegeheim, en het recht op vrijheid van meningsuiting in het oog springen.[1] De VN-resolutie over het recht op privacy in het digitale tijdperk, die door Nederland mede is gesponsord, heeft dit recent helder verwoord.[2] Nederland ontplooit zelfstandig en samen met anderen initiatieven om dit uitgangspunt kracht bij te zetten. Zo heeft Nederland twee jaar geleden de Freedom Online Coalition (FOC) opgericht. De FOC telt inmiddels 22 landen en zet zich in voor internetvrijheid wereldwijd. Hiertoe organiseert de coalitie onder meer een jaarlijkse multi-stakeholder conferentie en verleent zij via het Digital Defenders Partnership financiële steun aan bloggers en cyberactivisten in nood.

De FOC, maar ook de International Conference on Cyberspace die in 2015 in Nederland zal plaatsvinden, laten zien dat Nederland internationaal een voortrekkersrol heeft op het gebied van internetvrijheid. Er is echter sprake van een groeiend aantal landen dat meer controle wenst over (de inrichting van) het internet en daartoe initiatieven ontplooit. Ook zien regeringen, waaronder de Nederlandse regering, zich voor de uitdaging gesteld om per context een goede afweging te maken tussen vrijheid en veiligheid, waarbij het recht op privacy van burgers wordt gerespecteerd. Door deze ontwikkelingen staat internetvrijheid onder druk.

De recente onthullingen rondom de Amerikaanse National Security Agency (NSA) hebben de discussie over beveiliging en internetvrijheid op scherp gesteld. Onderwerp is onder meer de manier waarop rechten die ook online gelden op een zo effectief mogelijke manier in (inter)nationale wetgeving en beleid kunnen worden verankerd. Leidraad voor die discussie is – onder meer - de hiervoor genoemde VN-resolutie over het recht op privacy en ook de zogenaamde *necessary and proportionate principles*[3] kunnen als inspiratie dienen.[4] Deze 13 principes, die op initiatief van het maatschappelijk middenveld

---

[1] Zie respectievelijk artikelen 10, 13 en 7 Grondwet, artikelen 8 en 10 EVRM en artikelen 17 en 19 van het IVBPR.
[2] Resolutie van de Algemene Vergadering van de Verenigde Naties van 1 november 2013 (A/C.3/68/L.45).
[3] Andere voorbeelden zijn het EVRM en resoluties van de Raad van Europa.
[4] Ook kan worden aangesloten bij het EVRM en resoluties van de Raad van Europa.

zijn opgesteld, beschrijven welke beginselen volgens de initiatiefnemers van toepassing zouden moeten zijn op moderne vormen van surveillance.[5]

Een advies van de Adviesraad Internationale Vraagstukken (AIV) kan de discussie, die in Nederland, zoals bekend, ook intens wordt gevoerd, voeden en verhelderen.

Het kabinet wil daarom de volgende vragen aan de AIV voorleggen:

1. Hoe kan de Nederlandse regering zorgdragen voor een zo effectief mogelijke verankering en verdere operationalisering van internetvrijheid[6] in Nederlands binnenlands en buitenlands beleid – tegen de achtergrond van:

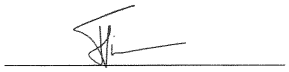
a) de uitdaging waar regeringen, waaronder de Nederlandse regering, zich voor gesteld zien voor het afwegen van het recht op privacy – zoals geformuleerd in de VN-resolutie over het recht op privacy[7] – met andere door de overheid te beschermen belangen bij het zoeken naar oplossingen voor vragen die de digitale wereld oproept;
b) de vooraanstaande rol die Nederland speelt in het buitenlands beleid ten aanzien van internetvrijheid, getuige de FOC, en de kansen die NL heeft om het internationale debat te beïnvloeden, waaronder de International Conference on Cyberspace in het voorjaar van 2015;
c) een internationaal speelveld waarbij een groeiend aantal landen meer controle wenst over (de inrichting van) het internet en hiertoe ook initiatieven ontplooit;
d) het recht op bescherming van persoonsgegevens, dat op verschillende wijzen wordt geadresseerd binnen de VN, de Raad van Europa en de EU.

2. Strekt de Nederlandse jurisdictie ten aanzien van internetvrijheid zich alleen uit over het eigen grondgebied, of ziet dit door de toegenomen technische mogelijkheden ook op situaties buiten het eigen grondgebied?[8] Indien de jurisdictie niet zover strekt: op welke wijze kan de Nederlandse overheid buiten de eigen grenzen effectief aan bewaking van internetvrijheid bijdragen?

3. In hoeverre zijn bedrijven verantwoordelijk voor de bescherming van internetvrijheid van burgers in de landen waar ze actief zijn en hoe kan de Nederlandse overheid, zelfstandig en samen met andere landen bedrijven oproepen die verantwoordelijkheid op te pakken?[9]

Ik zie uw advies met veel belangstelling tegemoet.

Frans Timmermans
Minister van Buitenlandse Zaken



[5] Zie: https://necessaryandproportionate.org/text. Deze principes zijn wereldwijd inmiddels door meer dan 350 organisaties en meer dan 50 onafhankelijke experts onderschreven. Ook Zweden heeft 7 van deze principes omarmt: https://www.privacyinternational.org/blog/swedens-foreign-minister-declares-his-support-for-principles to-protect-privacy-in-the-face-of.
[6] Zie voetnoot 1.
[7] Zie voetnoot 2.
[8] Zie aanhef, tiende alinea van de VN-resolutie genoemd in voetnoot 2.
[9] Bijvoorbeeld via de Freedom Online Coalition en de Raad van Europa.

United Nations A/C.3/68/L.45

General Assembly

Distr.: Limited
1 November 2013

Original: English

Sixty-eighth session
Third Committee
Agenda item 69 (b)
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Brazil and Germany: draft resolution

The right to privacy in the digital age

The General Assembly,

Reaffirming the purposes and principles of the Charter of the United Nations,

Reaffirming also the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,

Reaffirming further the Vienna Declaration and Programme of Action,

Noting that the rapid pace of technological development enables individuals in all regions to use new information and communication technologies and at the same time enhances the capacity of Governments, companies and individuals for surveillance, interception and data collection, which may violate human rights, in particular the right to privacy, as enshrined in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and is therefore an issue of increasing concern,

Reaffirming the human right of individuals to privacy and not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and the right to enjoy protection of the law against such interferences and attacks, and recognizing that the exercise of the right to privacy is an essential requirement for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society,

Stressing the importance of the full respect for the freedom to seek, receive and impart information, including the fundamental importance of access to information and democratic participation,

Welcoming the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,[1] submitted to the Human Rights Council at its twenty-third session, concerning the implications of States' surveillance of communications and the interception of personal data for the exercise of the human right to privacy,

Emphasizing that illegal surveillance of communications, their interception and the illegal collection of personal data constitute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society,

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, States must ensure full compliance with their obligations under international human rights law,

Deeply concerned at human rights violations and abuses that may result from the conduct of any surveillance of communications, including extraterritorial surveillance of communications, their interception and the collection of personal data, in particular massive surveillance, interception and data collection,

Recalling that States must ensure that measures taken to counter terrorism comply with international law, in particular international human rights, refugee and humanitarian law,

1. *Reaffirms* the rights contained in the International Covenant on Civil and Political Rights, in particular the right to privacy and not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence, and the right to enjoy protection of the law against such interference or attacks, in accordance with article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights;

2. *Recognizes* the rapid advancement in information and communications technologies, including the global and open nature of the Internet, as a driving force in accelerating progress towards development in its various forms;

3. *Affirms* that the same rights that people have offline must also be protected online, in particular the right to privacy;

4. *Calls upon* all States:

(a) To respect and protect the rights referred to in paragraph 1 above, including in the context of digital communication;

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection, with a view to upholding the right to privacy and ensuring the full and effective implementation of all their obligations under international human rights law;

---

[1] A/HRC/23/40 and Corr.1.

(d) To establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data;

5. *Requests* the United Nations High Commissioner for Human Rights to submit an interim report on the protection of the right to privacy in the context of domestic and extraterritorial surveillance of communications, their interception and collection of personal data, including massive surveillance, interception and collection of personal data, to the General Assembly at its sixty-ninth session, and a final report at its seventieth session, with views and recommendations, to be considered by Member States, with the purpose of identifying and clarifying principles, standards and best practices on how to address security concerns in a manner consistent with States' obligations under international human rights law and with full respect for human rights, in particular with respect to surveillance of digital communications and the use of other intelligence technologies that may violate the human right to privacy and freedom of expression and of opinion;

6. *Decides* to examine the question on a priority basis at its sixty-ninth session, under the sub-item entitled "Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms" of the item entitled "Promotion and protection of human rights".

International Principles on the Application of Human Rights to Communications Surveillance

FINAL VERSION 10 JULY 2013

As technologies that facilitate State surveillance of communications advance, States are failing to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. This document attempts to explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These principles can provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Preamble

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law.[1] Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, they are necessary to achieve a legitimate aim, and are proportionate to the aim pursued.[2]

Before public adoption of the Internet, well-established legal principles and logistical burdens inherent in monitoring communications created limits to State communications surveillance. In recent decades, those logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear. The explosion of digital communications content and information about communications, or "communications metadata" – information about an individual's communications or use of electronic devices – the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make State surveillance possible at an unprecedented scale.[3] Meanwhile, conceptualisations of existing human rights law have not kept up with the modern and changing communications surveillance capabilities of the State, the ability of the State to combine and organize information gained from different surveillance techniques, or the increased sensitivity of the information available to be accessed.

The frequency with which States are seeking access to both communications content and communications metadata is rising dramatically, without adequate scrutiny.[4] When accessed and analysed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.[5] Despite the vast potential for intrusion into an individual's life and the chilling effect on political and other associations, legislative and policy instruments often afford communications metadata a lower level of protection and do not place sufficient restrictions on how they can be subsequently used by agencies, including how they are data-mined, shared, and retained.

In order for States to actually meet their international human rights obligations in relation to communications surveillance, they must comply with the principles set out below. These principles apply to surveillance conducted within a State or extraterritorially. The principles also apply regardless of the purpose for the surveillance – law enforcement, national security or any other regulatory purpose. They also apply both to the State's obligation to respect and fulfil individuals' rights, and also to the obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.[6] The private sector bears equal responsibility for respecting human rights, particularly given the key role it plays in designing, developing and disseminating technologies; enabling and providing communications; and - where required - cooperating with State surveillance activities. Nevertheless, the scope of the present Principles is limited to the obligations of the State.

Changing technology and definitions

"Communications surveillance" in the modern environment encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects, arises from or is about a person's communications in the past, present or future. "Communications" include activities, interactions and transactions transmitted through electronic mediums, such as content of communications, the identity of the parties to the communications, location-tracking information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.

Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content", "subscriber information" or "metadata", stored data or in transit data, data held in the home or in the possession of a third party service provider.[7] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, color, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,[8] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

When adopting a new communications surveillance technique or expanding the scope of an existing technique, the State should ascertain whether the information likely to be procured falls within the ambit of "protected information" before seeking it, and should submit to the scrutiny of the judiciary or other democratic oversight mechanism. In considering whether information obtained through communications surveillance rises to the level of "protected information", the form as well as the scope and duration of the surveillance are relevant factors. Because pervasive or systematic monitoring has the capacity to reveal private information far in excess of its constituent parts, it can elevate surveillance of non-protected information to a level of invasiveness that demands strong protection.[9]

The determination of whether the State may conduct communications surveillance that interferes with protected information must be consistent with the following principles.

The Principles

LEGALITY: Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

LEGITIMATE AIM: Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

NECESSITY: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. Communications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

ADEQUACY: Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

PROPORTIONALITY: Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests, and should involve a consideration of the sensitivity of the information and the severity of the infringement on the right to privacy.

Specifically, this requires that, if a State seeks access to or use of protected information obtained through communications surveillance in the context of a criminal investigation, it must establish to the competent, independent, and impartial judicial authority that:

1. there is a high degree of probability that a serious crime has been or will be committed;
2. evidence of such a crime would be obtained by accessing the protected information sought;
3. other available less invasive investigative techniques have been exhausted;

4. information accessed will be confined to that reasonably relevant to the crime alleged and any excess information collected will be promptly destroyed or returned; and
5. information is accessed only by the specified authority and used for the purpose for which authorisation was given.

If the State seeks access to protected information through communication surveillance for a purpose that will not place a person at risk of criminal prosecution, investigation, discrimination or infringement of human rights, the State must establish to an independent, impartial, and competent authority:

1. other available less invasive investigative techniques have been considered;
2. information accessed will be confined to what is reasonably relevant and any excess information collected will be promptly destroyed or returned to the impacted individual; and
3. information is accessed only by the specified authority and used for the purpose for which was authorisation was given.

COMPETENT JUDICIAL AUTHORITY: Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:

1. separate from the authorities conducting communications surveillance;
2. conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights; and
3. have adequate resources in exercising the functions assigned to them.

DUE PROCESS: Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public. Specifically, in the determination on his or her human rights, everyone is entitled to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law,[10] except in cases of emergency when there is imminent risk of danger to human life. In such instances, retroactive authorisation must be sought within a reasonably practicable time period. Mere risk of flight or destruction of evidence shall never be considered as sufficient to justify retroactive authorisation.

USER NOTIFICATION: Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation. Delay in notification is only justified in the following circumstances:

1. Notification would seriously jeopardize the purpose for which the surveillance is authorised, or there is an imminent risk of danger to human life; or
2. Authorisation to delay notification is granted by the competent judicial authority at the time that authorisation for surveillance is granted; and
3. The individual affected is notified as soon as the risk is lifted or within a reasonably practicable time period, whichever is sooner, and in any event by the time the communications surveillance has been completed. The obligation to give notice rests with the State, but in the event the State fails to give notice, communications service providers shall be free to notify individuals of the communications surveillance, voluntarily or upon request.

TRANSPARENCY: States should be transparent about the use and scope of communications surveillance techniques and powers. They should publish, at a minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation type and purpose. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance, adhere to those procedures, and publish records of State communications surveillance.

PUBLIC OVERSIGHT: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.[11] Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information; to assess whether the State is making legitimate use of its lawful capabilities; to evaluate whether the State has been transparently and accurately publishing information about the use and scope of communications surveillance techniques and powers; and to publish periodic reports and other information relevant to communications surveillance. Independent oversight mechanisms should be established in addition to any oversight already provided through another branch of government.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS: In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes. *A priori* data retention or collection should never be required of service providers. Individuals have the right to express themselves anonymously; States should therefore refrain from compelling the identification of users as a precondition for service provision.[12]

SAFEGUARDS FOR INTERNATIONAL COOPERATION: In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. Where States seek assistance for law enforcement purposes, the principle of dual criminality should be applied. States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance. Mutual legal assistance processes and other agreements should be clearly documented, publicly available, and subject to guarantees of procedural fairness.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS: States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. Laws should stipulate that any information obtained in a manner that is inconsistent with these principles is inadmissible as evidence in any proceeding, as is any evidence derivative of such information. States should also enact laws providing that, after material obtained through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

[1] Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

[2] Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

[3] Communications metadata may include information about our identities (subscriber information, device information), interactions (origins and destinations of communications, especially those showing websites visited, books and other materials read, people interacted with, friends, family, acquaintances, searches conducted, resources used), and location (places and times, proximities to others); in sum, metadata provides a window into nearly every action in modern life, our mental states, interests, intentions, and our innermost thoughts.

[4] For example, in the United Kingdom alone, there are now approximately 500,000 requests for communications metadata every year, currently under a self-authorising regime for law enforcement agencies who are able to authorise their own requests for access to information held by service providers. Meanwhile, data provided by Google's Transparency reports shows that requests for user data from the U.S. alone rose from 8888 in 2010 to 12,271 in 2011. In Korea, there were about 6 million subscriber/poster information requests every year and about 30 million requests for other forms of communications metadata every year in 2011-2012, almost of all of which were granted and executed. 2012 data available at <http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586>.

[5] See as examples, a review of Sandy Petland's work, 'Reality Mining', in MIT's Technology Review, 2008, available at <http://www2.technologyreview.com/article/409598/tr10-reality-mining/> and also see Alberto Escudero-Pascual and Gus Hosein, 'Questioning lawful access to traffic data', Communications of the ACM, Volume 47 Issue 3, March 2004, pages 77-82.

[6] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, May 16 2011, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf>.

[7] "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[8] "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." United States v. Jones, 565 U.S., 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

[9] "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." U.S. v. Maynard, 615 F.3d 544 (U.S., D.C. Circ., C.A.) p. 562; U.S. v. Jones, 565 U.S. __, (2012), Alito, J., concurring. "Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past…In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention." (Rotaru v. Romania, [2000] ECHR 28341/95, paras. 43-44.

[10] The term "due process" can be used interchangeably with "procedural fairness" and "natural justice", and is well articulated in the European Convention for Human Rights Article 6(1) and Article 8 of the American Convention on Human Rights.

[11] The UK Interception of Communications Commissioner is an example of such an independent oversight mechanism. The ICO publishes a report that includes some aggregate data but it does not provide sufficient data to scrutinise the types of requests, the extent of each access request, the purpose of the requests, and the scrutiny applied to them. See <http://www.iocco-uk.info/sections.asp?sectionID=2&type=top>.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, para 84.

Lijst van gebruikte afkortingen

AIV	Adviesraad Internationale Vraagstukken
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AVVN	Algemene Vergadering van de Verenigde Naties
CMR	Commissie Mensenrechten
CTIVD	Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten
CVV	Commissie Vrede en Veiligheid
DNS	Domeinnamen systeem
DTP	Datafile Transfer Protocol
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
FISC	Foreign Intelligence Surveillance Court
FTC	Federal Trade Commission
GAC	Governmental Advisory Committee
gTLD	algemene toplevel domeinen
HvJ EU	Hof van Justitie van de Europese Unie
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Informatie- en communicatietechnologie
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internetprotocol
ISOC	Internet Society
ITR	International Telecommunications Regulations
ITU	Internationale Telecommunicatie Unie
NGO	niet-gouvernementele organisatie
NSA	National Security Agency
OSI-model	Open System Interconnection model
PCLOB	Privacy & Civil Liberties Oversight Board
PTT	Post, telefoon en telegrafie
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIA	Total Information Awareness
TCP	Transmission Control Protocol
TFTP	Terrorist Finance Tracking Programme
VN	Verenigde Naties
VS	Verenigde Staten
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
Wiv 2002	Wet op de inlichtingen- en veiligheidsdiensten 2002
WODC	Wetenschappelijk Onderzoek en Documentatie Centrum
WSIS	World Summit on the Information Society
www	world wide web

Lijst van geconsulteerde deskundigen

C. Bowden	Onafhankelijk privacy onderzoeker
Mw. mr.dr. Q. Eijkman	Hoofd politieke zaken en persvoorlichting van Amnesty International Nederland
Mr. H. Hijmans	Afdelingshoofd Policy & Consultation bij de European Data Protection Supervisor (op sabbatical)
Prof. E. Huizer	CTO van SURFnet en hoogleraar internettoepassingen aan de Universiteit Utrecht
Prof. M.L. Mueller	Hoogleraar Syracuse University School of Information Studies, Syracuse, New York, Verenigde Staten
Ir. R. Zenger	Onderzoeker Bits of Freedom
H. de Zwart	Directeur Bits of Freedom

Door de Adviesraad Internationale Vraagstukken uitgebrachte adviezen*

1 EUROPA INCLUSIEF, *oktober 1997*
2 CONVENTIONELE WAPENBEHEERSING: dringende noodzaak, beperkte mogelijkheden, *april 1998*
3 DE DOODSTRAF EN DE RECHTEN VAN DE MENS: recente ontwikkelingen, *april 1998*
4 UNIVERSALITEIT VAN DE RECHTEN VAN DE MENS EN CULTURELE VERSCHEIDENHEID, *juni 1998*
5 EUROPA INCLUSIEF II, *november 1998*
6 HUMANITAIRE HULP: naar een nieuwe begrenzing, *november 1998*
7 COMMENTAAR OP DE CRITERIA VOOR STRUCTURELE BILATERALE HULP, *november 1998*
8 ASIELINFORMATIE EN DE EUROPESE UNIE, *juli 1999*
9 NAAR RUSTIGER VAARWATER: een advies over betrekkingen tussen Turkije en de Europese Unie, *juli 1999*
10 DE ONTWIKKELINGEN IN DE INTERNATIONALE VEILIGHEIDSSITUATIE IN DE JAREN NEGENTIG: van onveilige zekerheid naar onzekere veiligheid, *september 1999*
11 HET FUNCTIONEREN VAN DE VN-COMMISSIE VOOR DE RECHTEN VAN DE MENS, *september 1999*
12 DE IGC 2000 EN DAARNA: op weg naar een Europese Unie van dertig lidstaten, *januari 2000*
13 HUMANITAIRE INTERVENTIE, *april 2000***
14 ENKELE LESSEN UIT DE FINANCIËLE CRISES VAN 1997 EN 1998, *mei 2000*
15 EEN EUROPEES HANDVEST VOOR GRONDRECHTEN?, *mei 2000*
16 DEFENSIE-ONDERZOEK EN PARLEMENTAIRE CONTROLE, *december 2000*
17 DE WORSTELING VAN AFRIKA: veiligheid, stabiliteit en ontwikkeling, *januari 2001*
18 GEWELD TEGEN VROUWEN: enkele rechtsontwikkelingen, *februari 2001*
19 EEN GELAAGD EUROPA: de verhouding tussen de Europese Unie en subnationale overheden, *april 2001*
20 EUROPESE MILITAIR-INDUSTRIËLE SAMENWERKING*, mei 2001*
21 REGISTRATIE VAN GEMEENSCHAPPEN OP HET GEBIED VAN GODSDIENST OF OVERTUIGING*, juni 2001*
22 DE WERELDCONFERENTIE TEGEN RACISME EN DE PROBLEMATIEK VAN RECHTSHERSTEL*, juni 2001*
23 COMMENTAAR OP DE NOTITIE MENSENRECHTEN 2001, *september 2001*
24 EEN CONVENTIE OF EEN CONVENTIONELE VOORBEREIDING: de Europese Unie en de IGC 2004, *november 2001*
25 INTEGRATIE VAN GENDERGELIJKHEID: een zaak van verantwoordelijkheid, inzet en kwaliteit, *januari 2002*
26 NEDERLAND EN DE ORGANISATIE VOOR VEILIGHEID EN SAMENWERKING IN EUROPA IN 2003: rol en richting, *mei 2002*
27 EEN BRUG TUSSEN BURGERS EN BRUSSEL: naar meer legitimiteit en slagvaardigheid voor de Europese Unie, *mei 2002*
28 DE AMERIKAANSE PLANNEN VOOR RAKETVERDEDIGING NADER BEKEKEN: voors en tegens van bouwen aan onkwetsbaarheid, *augustus 2002*
29 PRO-POOR GROWTH IN DE BILATERALE PARTNERLANDEN IN SUB-SAHARA AFRIKA: een analyse van strategieën tegen armoede, *januari 2003*
30 EEN MENSENRECHTENBENADERING VAN ONTWIKKELINGSSAMENWERKING, *april 2003*
31 MILITAIRE SAMENWERKING IN EUROPA: mogelijkheden en beperkingen, *april 2003*
32 *Vervolgadvies* EEN BRUG TUSSEN BURGERS EN BRUSSEL: naar meer legitimiteit en slagvaardigheid voor de Europese Unie, *april 2003*
33 DE RAAD VAN EUROPA: minder en (nog) beter, *oktober 2003*
34 NEDERLAND EN CRISISBEHEERSING: drie actuele aspecten, *maart 2004*
35 FALENDE STATEN: een wereldwijde verantwoordelijkheid, *mei 2004***
36 PREËMPTIEF OPTREDEN, *juli 2004***
37 TURKIJE: de weg naar het lidmaatschap van de Europese Unie, *juli 2004*
38 DE VERENIGDE NATIES EN DE RECHTEN VAN DE MENS, *september 2004*
39 DIENSTENLIBERALISERING EN ONTWIKKELINGSLANDEN: leidt openstelling tot achterstelling?, *september 2004*

40 DE PARLEMENTAIRE ASSEMBLEE VAN DE RAAD VAN EUROPA, *februari 2005*
41 DE HERVORMINGEN VAN DE VERENIGDE NATIES: het rapport Annan nader beschouwd, *mei 2005*
42 DE INVLOED VAN CULTUUR EN RELIGIE OP ONTWIKKELING: stimulans of stagnatie?, *juni 2005*
43 MIGRATIE EN ONTWIKKELINGSSAMENWERKING: de samenhang tussen twee beleidsterreinen, *juni 2005*
44 DE NIEUWE OOSTELIJKE BUURLANDEN VAN DE EUROPESE UNIE, *juli 2005*
45 NEDERLAND IN DE VERANDERENDE EU, NAVO EN VN, *juli 2005*
46 ENERGIEK BUITENLANDS BELEID: energievoorzieningszekerheid als nieuwe hoofddoelstelling, *december 2005****
47 HET NUCLEAIRE NON-PROLIFERATIEREGIME: het belang van een geïntegreerde en multilaterale aanpak, *januari 2006*
48 MAATSCHAPPIJ EN KRIJGSMACHT, *april 2006*
49 TERRORISMEBESTRIJDING IN MONDIAAL EN EUROPEES PERSPECTIEF, *september 2006*
50 PRIVATE SECTOR ONTWIKKELING EN ARMOEDEBESTRIJDING, *oktober 2006*
51 DE ROL VAN NGO'S EN BEDRIJVEN IN INTERNATIONALE ORGANISATIES, *oktober 2006*
52 EUROPA EEN PRIORITEIT!, *november 2006*
53 BENELUX, NUT EN NOODZAAK VAN NAUWERE SAMENWERKING, *februari 2007*
54 DE OESO VAN DE TOEKOMST, *maart 2007*
55 MET HET OOG OP CHINA: op weg naar een volwassen relatie, *april 2007*
56 INZET VAN DE KRIJGSMACHT: wisselwerking tussen nationale en internationale besluitvorming, *mei 2007*
57 HET VN-VERDRAGSSYSTEEM VOOR DE RECHTEN VAN DE MENS: stapsgewijze versterking in een politiek geladen context, *juli 2007*
58 DE FINANCIËN VAN DE EUROPESE UNIE, *december 2007*
59 DE INHUUR VAN PRIVATE MILITAIRE BEDRIJVEN: een kwestie van verantwoordelijkheid, *december 2007*
60 NEDERLAND EN DE EUROPESE ONTWIKKELINGSSAMENWERKING, *mei 2008*
61 DE SAMENWERKING TUSSEN DE EUROPESE UNIE EN RUSLAND: een zaak van wederzijds belang, *juli 2008*
62 KLIMAAT, ENERGIE EN ARMOEDEBESTRIJDING, *november 2008*
63 UNIVERSALITEIT VAN DE RECHTEN VAN DE MENS: principes, praktijk en perspectieven, *november 2008*
64 CRISISBEHEERSINGSOPERATIES IN FRAGIELE STATEN: de noodzaak van een samenhangende aanpak, *maart 2009*
65 TRANSITIONAL JUSTICE: gerechtigheid en vrede in overgangssituaties, *april 2009***
66 DEMOGRAFISCHE VERANDERINGEN EN ONTWIKKELINGSSAMENWERKING, *juli 2009*
67 HET NIEUWE STRATEGISCH CONCEPT VAN DE NAVO, *januari 2010*
68 DE EU EN DE CRISIS: lessen en leringen, *januari 2010*
69 SAMENHANG IN INTERNATIONALE SAMENWERKING: reactie op WRR-rapport 'Minder pretentie, meer ambitie', *mei 2010*
70 NEDERLAND EN DE 'RESPONSIBILITY TO PROTECT': de verantwoordelijkheid om mensen te beschermen tegen massale wreedheden, *juni 2010*
71 HET VERMOGEN VAN DE EU TOT VERDERE UITBREIDING, *juli 2010*
72 PIRATERIJBESTRIJDING OP ZEE: een herijking van publieke en private verantwoordelijkheden, *december 2010*
73 HET MENSENRECHTENBELEID VAN DE NEDERLANDSE REGERING: zoeken naar constanten in een veranderende omgeving, *februari 2011*
74 ONTWIKKELINGSAGENDA NA 2015: millennium ontwikkelingsdoelen in perspectief, *april 2011*
75 HERVORMINGEN IN DE ARABISCHE REGIO: kansen voor democratie en rechtsstaat?, *mei 2011*
76 HET MENSENRECHTENBELEID VAN DE EUROPESE UNIE: tussen ambitie en ambivalentie, *juli 2011*
77 DIGITALE OORLOGVOERING, *december 2011***
78 EUROPESE DEFENSIESAMENWERKING: soevereiniteit en handelingsvermogen, *januari 2012*

79 DE ARABISCHE REGIO, EEN ONZEKERE TOEKOMST, *mei 2012*
80 ONGELIJKE WERELDEN: armoede, groei, ongelijkheid en de rol van internationale samenwerking, *september 2012*
81 NEDERLAND EN HET EUROPEES PARLEMENT: investeren in nieuwe verhoudingen, *november 2012*
82 WISSELWERKING TUSSEN ACTOREN IN INTERNATIONALE SAMENWERKING: naar flexibiliteit en vertrouwen, *februari 2013*
83 TUSSEN WOORD EN DAAD: perspectieven op duurzame vrede in het Midden-Oosten, *maart 2013*
84 NIEUWE WEGEN VOOR INTERNATIONALE MILIEUSAMENWERKING, *maart 2013*
85 CRIMINALITEIT, CORRUPTIE EN INSTABILITEIT: een verkennend advies, *mei 2013*
86 AZIË IN OPMARS: strategische betekenis en gevolgen, *december 2013*
87 DE RECHTSSTAAT: waarborg voor Europese burgers en fundament van Europese samenwerking, *januari 2014*
88 NAAR EEN GEDRAGEN EUROPESE SAMENWERKING: werken aan vertrouwen, *april 2014*
89 NAAR BETERE MONDIALE FINANCIËLE VERBONDENHEID: het belang van een coherent internationaal economisch en financieel stelsel, *juni 2014*
90 DE TOEKOMST VAN DE ARCTISCHE REGIO: samenwerking of confrontatie?, *september 2014*
91 NEDERLAND EN DE ARABISCHE REGIO: principieel en pragmatisch, *november 2014*

Door de Adviesraad Internationale Vraagstukken uitgebrachte briefadviezen

1 Briefadvies UITBREIDING EUROPESE UNIE, *december 1997*
2 Briefadvies VN-COMITÉ TEGEN FOLTERING, *juli 1999*
3 Briefadvies HANDVEST GRONDRECHTEN, *november 2000*
4 Briefadvies OVER DE TOEKOMST VAN DE EUROPESE UNIE, *november 2001*
5 Briefadvies NEDERLANDS VOORZITTERSCHAP EU 2004, *mei 2003*****
6 Briefadvies RESULTAAT CONVENTIE, *augustus 2003*
7 Briefadvies VAN BINNENGRENZEN NAAR BUITENGRENZEN - ook voor een volwaardig Europees asiel- en migratiebeleid in 2009, *maart 2004*
8 Briefadvies DE ONTWERP-DECLARATIE INZAKE DE RECHTEN VAN INHEEMSE VOLKEN. Van impasse naar doorbraak?, *september 2004*
9 Briefadvies REACTIE OP HET SACHS-RAPPORT: Hoe halen wij de Millennium Doelen, *april 2005*
10 Briefadvies DE EU EN DE BAND MET DE NEDERLANDSE BURGER, *december 2005*
11 Briefadvies TERRORISMEBESTRIJDING IN EUROPEES EN INTERNATIONAAL PERSPECTIEF, interim-advies over het folterverbod, *december 2005*
12 Briefadvies REACTIE OP DE MENSENRECHTENSTRATEGIE 2007, *november 2007*
13 Briefadvies EEN OMBUDSMAN VOOR ONTWIKKELINGSSAMENWERKING, *december 2007*
14 Briefadvies KLIMAATVERANDERING EN VEILIGHEID, *januari 2009*
15 Briefadvies OOSTELIJK PARTNERSCHAP, *februari 2009*
16 Briefadvies ONTWIKKELINGSSAMENWERKING: Nut en noodzaak van draagvlak, *mei 2009*
17 Briefadvies KABINETSFORMATIE 2010, *juni 2010*
18 Briefadvies HET EUROPESE HOF VOOR DE RECHTEN VAN DE MENS: beschermer van burgerlijke rechten en vrijheden, *november 2011*
19 Briefadvies NAAR EEN VERSTERKT FINANCIEEL-ECONOMISCH BESTUUR IN DE EU, *februari 2012*
20 Briefadvies NUCLEAIR PROGRAMMA VAN IRAN: naar de-escalatie van een nucleaire crisis, *april 2012*

21 Briefadvies DE RECEPTORBENADERING: een kwestie van maatvoering, *april 2012*

22 Briefadvies KABINETSFORMATIE 2012: krijgsmacht in de knel, *september 2012*

23 Briefadvies NAAR EEN VERSTERKTE SOCIALE DIMENSIE VAN DE EUROPESE UNIE, *juni 2013*

24 Briefadvies MET KRACHT VOORUIT: reactie van de Adviesraad Internationale Vraagstukken op de beleidsbrief 'Respect en recht voor ieder mens', *september 2013*

25 Briefadvies ONTWIKKELINGSSAMENWERKING: meer dan een definitiekwestie, *mei 2014*

26 DE EU-GASAFHANKELIJKHEID VAN RUSLAND: hoe een geïntegreerd EU-beleid dit kan verminderen, *juni 2014*

* *Alle adviezen zijn ook beschikbaar in het Engels. Sommige adviezen ook in andere talen.*

** *Gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV).*

*** *Gezamenlijk advies van de Adviesraad Internationale Vraagstukken (AIV) en de Algemene Energieraad (AER).*

**** *Gezamenlijk briefadvies van de Adviesraad Internationale Vraagstukken (AIV) en de Adviescommissie voor Vreemdelingenzaken (ACVZ).*