Van Mourik Broekmanweg 6
2628 XE Delft
Postbus 49
2600 AA Delft

www.tno.nl

**TNO-rapport**

**TNO 2016 R10150**

# Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX

| | |
|---|---|
| Datum | 12 februari 2016 |
| Auteur(s) | Prof.dr. Bert-Jaap Koops<br>Mr.dr. Arnold Roosendaal<br>Dr. Eleni Kosta<br>Marc van Lieshout, MSc<br>Mr. Elaine Oldhoff |
| Reviewer | Prof.mr.dr. Mireille Hildebrandt |
| *Exemplaarnummer* | |
| Oplage | |
| Aantal pagina's | 186 (incl. bijlagen) |
| Aantal bijlagen | |
| Opdrachtgever | Ministerie van Binnenlandse Zaken en Koninkrijksrelaties |
| Projectnaam | |
| Projectnummer | 060.17368 |

Alle rechten voorbehouden.
Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van TNO.

Indien dit rapport in opdracht werd uitgebracht, wordt voor de rechten en verplichtingen van opdrachtgever en opdrachtnemer verwezen naar de Algemene Voorwaarden voor opdrachten aan TNO, dan wel de betreffende terzake tussen de partijen gesloten overeenkomst.
Het ter inzage geven van het TNO-rapport aan direct belanghebbenden is toegestaan.

© 2016 TNO

# Inhoudsopgave

# Samenvatting

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft tezamen met drie collega-ministeries een concept voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv 20xx) opgesteld, ter vervanging van de huidige Wiv 2002. Vanwege de potentiële privacyinbreuken die inherent zijn aan de werkzaamheden van de inlichtingen- en veiligheidsdiensten heeft de minister van BZK de Tweede Kamer toegezegd een Privacy Impact Assessment (PIA) over de wet uit te laten voeren. Dit rapport geeft de uitkomsten van deze PIA weer, die in onafhankelijkheid is uitgevoerd door het PI.lab. Het doel van de PIA is om de privacyrisico's van de voorgestelde maatregelen te inventariseren en te kijken of de daarbij voorgestelde waarborgen voldoende zijn om de privacyrisico's voldoende af te dekken. De PIA betreft uitdrukkelijk geen juridische toetsing van het wetsvoorstel aan de eisen van artikel 8 van het Europees Verdrag voor de Rechten van de Mens of aan artikelen 10-13 Grondwet, maar een risicoinventarisatie.

Het wetsontwerp beoogt tegemoet te komen aan diverse vragen die zijn gerezen over kwesties die zich in de toepassingspraktijk van de Wiv 2002 voordeden, en aan een sterk veranderende technologische omgeving die nieuwe uitdagingen stelt. Beide ontwikkelingen bieden een aanleiding om de bevoegdheden van de diensten aan te passen en op onderdelen te verruimen. Met betrekking tot de gerezen toepassingsvragen delen wij de opvatting dat het wenselijk is om de wet te herzien en, waar de noodzaak voldoende is onderbouwd, op onderdelen bevoegdheden te verruimen. Met betrekking tot de technologische omgeving is onze conclusie evenwel dat het wetsvoorstel onvoldoende rekening houdt met huidige en voorzienbare toekomstige ontwikkelingen. Ervan uitgaande dat de wet het passende kader moet bieden voor situaties die in de komende tien tot vijftien jaar het speelveld van de diensten zullen bepalen, is het noodzakelijk om de wet hier nu al zoveel mogelijk op toe te snijden. Er is evenwel te weinig sprake in het wetsontwerp en de bijbehorende toelichting van een serieuze analyse en doordenking van de belangrijkste toekomstige technologische uitdagingen en mogelijkheden, zoals die bijvoorbeeld zichtbaar zijn in de toepasbaarheid van drones, nieuwe observatiemiddelen in combinatie met geavanceerde data-analyses, en de data-overvloed en interconnectiviteit die het Internet der Dingen met zich meebrengt.

Deze omissie wreekt zich in delen van het wetsontwerp die, door het ontbreken van een visie op de belangrijkste technologische ontwikkelingen, geen goed of volledig perspectief hanteren om de huidige en voorzienbare uitdagingen op een evenwichtige wijze te adresseren. In dit rapport wijzen wij op de privacyrisico's die gepaard gaan met de voorgestelde bevoegdheden in het licht van technologische ontwikkelingen, en stellen wij op basis van een analyse van deze risico's en de voorgestelde waarborgen de nodige aanscherpingen voor. De analyse is onderwerpsgewijs gegroepeerd langs de relevante privacyperspectieven: algemene bepalingen, informationele privacy, lichamelijke privacy, ruimtelijke privacy en communicatie-gerelateerde privacy.

De bevindingen geven aan dat op een aanzienlijk aantal onderdelen heroverweging aangewezen is, in het licht van de met de voorgestelde bevoegdheden gepaard gaande privacyrisico's en adequate waarborgen die nodig zijn om deze risico's te

ondervangen. Een overzicht van alle punten is te vinden in het afsluitende hoofdstuk met conclusies en aanbevelingen. Op enkele onderdelen betreft het een fundamentele heroverweging; andere punten kunnen veelal worden geadresseerd door aanscherping van een voorgestelde bevoegdheid, versteviging van het stelsel van waarborgen, of aanvulling van de wet met een nieuwe bepaling. Op veel punten is er daarbij behoefte aan verduidelijking of uitbreiding van de toelichting, omdat de huidige, sobere Memorie van Toelichting vaak onvoldoende aanknopingspunten die de noodzaak van een voorstel kunnen onderbouwen, of onvoldoende inzicht geeft in wat een voorgestelde bepaling feitelijk behelst. Ook kan het stelsel van waarborgen eenvoudiger worden gestructureerd, wat eveneens de voorzienbaarheid bij wet zal bevorderen. De voorzienbaarheid bij wet is een ankerpunt voor een wet die zeer ingrijpende bevoegdheden reguleert, zowel voor de diensten en de toezichthouder om zorgvuldige afwegingen te kunnen maken, als voor burgers om zekerheid en duidelijkheid te hebben over wat zij kunnen verwachten met betrekking tot mogelijke inmenging van de diensten in hun privésfeer. Een Memorie van Toelichting die niet zozeer parafraseert wat in de bepalingen staat maar vooral meer visie, voorbeelden en argumenten geeft, is daarbij onontbeerlijk.

Naast een analyse van de voorgestelde bevoegdheden, waarbij wij vanuit het kader van privacyrisico's bij de onderbouwing hiervan in een aantal gevallen serieuze twijfels uiten, hebben wij ons ook gebogen over de voorgestelde mogelijkheden tot effectief toezicht. De toerusting van de CTIVD met een extra kamer voor klachtafhandeling is een te verwelkomen versterking van het onafhankelijke toezicht. Met name de mogelijkheid voor de CTIVD om in dit kader bindende uitspraken te kunnen doen, is een zwaarwegende privacywaarborg. Aangezien onterechte handelingen van de diensten niet in alle gevallen, of niet altijd tijdig, tot klachten leiden, zou de wetgever nadrukkelijk moeten overwegen om de CTIVD in het algemeen bindend adviesrecht te geven, ook buiten de klachtprocedure om. Daarnaast verdient het aanbeveling om een bepaling betreffende gegevensbescherming *by design* en gegevensbescherming *by default* op te nemen in de Wiv 20xx. Het bevorderen dat bij de technische inrichting van systemen, zowel in ontwerp als in standaardinstellingen, privacyinbreuken zoveel mogelijk worden voorkomen of beperkt, kan in dit tijdsgewricht een waardevolle aanvulling betekenen op de juridische waarborgen. Daarbij zou de technische expertise binnen de toezichthouder versterkt moeten worden, een aanbeveling die ook ongeacht wettelijke verankering van gegevensbescherming *by design* en *by default* opgeld doet.

De algemene conclusie van onze analyse is dat er nog het nodige te winnen valt om de privacyrisico's van de Wiv 20xx afdoende te adresseren, door een aanzienlijke aanscherping van diverse onderdelen, alsook door een betere en uitgebreidere toelichting die meer houvast biedt om de noodzaak van bepaalde voorstellen te onderbouwen en de reikwijdte van de wet te kunnen overzien, ook in het licht van de huidige en voorzienbare technologische ontwikkelingen in de komende jaren. In enkele gevallen argumenteren we dat de wetgever er verstandig aan doet om een voorgestelde bepaling te heroverwegen, omdat de noodzaak ervan niet is aangetoond en onzes inziens ook moeilijk aannemelijk is te maken, ook niet als er zwaardere waarborgen zouden worden voorgesteld. In de rapportage presenteren we deze argumentatie in extenso. In het laatste hoofdstuk staan alle aanbevelingen bij elkaar. Gegeven het belang van privacybescherming van burgers en goed functionerende diensten in een democratische samenleving,

hebben we de aanbevelingen scherp geformuleerd. Het doel van deze PIA is immers om de privacyrisico's zo duidelijk mogelijk voor het voetlicht te brengen, en op die manier bij te dragen aan de zorgvuldige totstandkoming van een Wiv 20xx waarin de privacyrisico's die inherent zijn aan het werk van inlichtingen- en veiligheidsdiensten, zo goed mogelijk, met inachtneming van het belang dat de diensten de komende jaren effectief én legitiem kunnen functioneren, zijn geadresseerd.

# Afkortingen

| | |
|---|---|
| AIVD | Algemene Inlichtingen- en Veiligheidsdienst |
| Avg | Algemene verordening gegevensbescherming |
| Awbi | Algemene wet op het binnentreden |
| BVerfG | Bundesverfassungsgericht [Duits constitutioneel hof] |
| CFR | Charter of Fundamental Rights of the European Union |
| CJEU | Court of Justice of the European Union |
| CTIVD | Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten |
| DPbD | Gegevensbescherming *by design* en *by default* |
| ECHR | European Convention on Human Rights |
| ECJ | European Court of Justice |
| ECtHR | European Court of Human Rights |
| EHJ | Europees Hof van Justitie |
| EHRM | Europees Hof van de Rechten van de Mens |
| EVRM | Europees Verdrag voor de Rechten van de Mens |
| ITU | International Telecommunications Union |
| MIVD | Militaire Inlichtingen- en Veiligheidsdienst |
| MvT | Memorie van Toelichting |
| OSINT | Open Source Intelligence |
| PIA | Privacy Impact Assessment |
| Sr | Wetboek van Strafrecht |
| Sv | Wetboek van Strafvordering |
| Tw | Telecommunicatiewet |
| Wbp | Wet bescherming persoonsgegevens |
| Wpg | Wet politiegegevens |
| WRR | Wetenschappelijke Raad voor het Regeringsbeleid |

# 1 Inleiding

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft het PI.lab gevraagd een Privacy Impact Assessment (PIA) op de voorgenomen Wet op de inlichtingen- en veiligheidsdiensten 20xx (Wiv 20xx) uit te voeren. Hoewel daar wettelijk geen verplichting toe bestaat (de Wiv 20xx bestrijkt het terrein van nationale veiligheid; dit terrein is uitgezonderd van de werkingssfeer van de Wet bescherming persoonsgegevens), heeft de minister van BZK de Tweede Kamer toegezegd een PIA op de Wiv 20xx uit te laten voeren.[1] Gegeven de inhoud van de Wiv 20xx is dit een terechte keuze: veel van de voorgestelde maatregelen maken een potentieel grote inbreuk op de persoonlijke levenssfeer van betrokkenen. Daarbij gaat het niet alleen om nieuwe bevoegdheden of uitbreiding van bestaande bevoegdheden; ook de impact die bestaande (en ongewijzigde) bevoegdheden kunnen hebben op de privacy, is door de technologische ontwikkelingen in belangrijke mate veranderd sinds 2002. Een analyse van de privacyrisico's van het wetsontwerp, bestaande uit een verkenning van de gevolgen voor de persoonlijke levenssfeer van burgers en de waarborgen die deze inbreuken in banen moeten leiden, is belangrijk om een wet tot stand te brengen die voldoende waarborgen biedt om de privacy van burgers te beschermen zonder de slagkracht van inlichtingen- en veiligheidsdiensten onnodig in te perken.

Het PI.lab is aangezocht om als onafhankelijke partij de PIA op de Wiv 20xx uit te voeren. Het PI.lab is een samenwerkingsverband tussen de TNO en de universiteiten van Nijmegen (Radboud Universiteit, in het bijzonder de vakgroep Digital security van het Institute for Computing and Information Sciences) en Tilburg (Tilburg University, in het bijzonder Tilburg Institute for Law, Technology and Society, TILT), ondersteund door SIDN. Het onderhavige onderzoek is uitgevoerd door onderzoekers van TNO en TILT, met een interne review vanuit de Radboud Universiteit.

De PIA is uitgevoerd op de consultatieversie van het wetsontwerp voor de Wiv 20xx en de bijbehorende Memorie van Toelichting uit juni 2015.[2] Deze lezer moet dus voor ogen houden dat de verwijzingen in dit rapport naar het wetsvoorstel en de toelichting de consultatieversie uit juni 2015 betreffen, en niet de versie van het wetsvoorstel zoals die uiteindelijk is of zal worden ingediend bij de Tweede Kamer.

## 1.1 Achtergrond

Het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20xx volgt op een meerjarige evaluatieprocedure rond de huidige Wiv 2002. Al geruime tijd staat het via de Wiv 2002 aangegeven kader dat de bevoegdheden van de diensten regelt ter discussie. De AIVD en de MIVD ervaren beperkingen in hun mogelijkheden om effectief op te treden in het kader van de hun toegewezen taakstelling. Met name het op onderdelen technologie-afhankelijke kader is naar zeggen onvoldoende afgestemd op de eisen van de huidige tijd.[3] Waar aan de ene

[1] Tweede Kamer, vergaderjaar 2014-2015, 33 820, nr 5.
[2] Zie https://www.internetconsultatie.nl/wiv (geraadpleegd 1 december 2015).
[3] Tweede Kamer, vergaderjaar 2014-2015, 33 820, nr 5. De minister maakt onder meer melding van de noodzaak tot aanpassing van de interceptiebevoegdheid. Zie ook Hoofdstuk 5, 'Inzet van

kant behoefte is aan uitbreiding van bevoegdheden brengt dit aan de andere kant de behoefte met zich mee tot een hierop toegesneden verzameling van waarborgen. In de evaluatie die door de commissie Evaluatie Wiv 2002 is uitgevoerd, komen beide aspecten uitgebreid aan de orde.[4] Deze commissie, naar haar voorzitter de commissie-Dessens genoemd, gaat in op de behoefte van de diensten aan de mogelijkheid om ook dataverkeer dat via kabelnetwerken wordt getransporteerd, in bulk te mogen onderscheppen en analyseren. Deze kabelgebonden bulkinterceptie[5] betekent een aanmerkelijke uitbreiding van de bijzondere bevoegdheden van de diensten. De grondslag voor deze behoefte wordt gezien in het feit dat inmiddels meer dan 80% van het dataverkeer via de kabel verloopt. Indien het voor de diensten niet toegestaan zou zijn dit dataverkeer in bulk te onderscheppen, lopen de diensten naar eigen zeggen achter de feiten aan, en zijn ze niet meer op gepaste wijze in staat de nationale veiligheid te garanderen. Door de omvang van het dataverkeer dat onderschept zou kunnen worden en het toegenomen vermogen van computeralgoritmen om verbanden te herleiden tussen grote hoeveelheden data (Big Data Analytics) is een zorgvuldige weging noodzakelijk van wat de diensten vermogen en hoe dit ingebed moet zijn in waarborgen die binnen een democratische rechtstaat gepast zijn. De commissie-Dessens doet hier een aantal voorstellen voor in haar evaluatierapport. Op soortgelijke wijze heeft ook de Commissie Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) in verschillende rapporten stilgestaan bij de technologische ontwikkelingen, de daaruit voortvloeiende behoeften van de diensten en de noodzaak om deze behoeften in te kaderen in een toereikend stelsel van waarborgen.[6]

Met de totstandkoming van de concept-Wiv 20xx is het mogelijk te onderzoeken wat de privacyrisico's zijn van de (bijzondere) bevoegdheden van de diensten in relatie tot de waarborgen voor de bescherming van de privacy van burgers. Het gaat dan enerzijds om een onderzoek naar de mate waarin de (bijzondere) bevoegdheden van de diensten kunnen leiden tot een inbreuk op de privacy, en anderzijds naar de kwaliteit van de waarborgen om deze inbreuken te voorkomen dan wel van het juiste wettelijke en organisatorische kader te voorzien zodat gepaste controle en toezicht mogelijk is, uitwassen kunnen worden voorkomen en burgers voldoende middelen hebben om zich te vergewissen van de wijze waarop de diensten hebben geopereerd. Een Privacy Impact Assessment is hiervoor een geschikt instrument.

## 1.2 Doelstelling

Het doel van het onderzoek is het uitvoeren van een Privacy Impact Assessment op de concept-Wet op de inlichtingen- en veiligheidsdiensten 20xx om te komen tot een onafhankelijke beoordeling van de privacy-implicaties van de concept-Wiv 20xx. Specifiek wordt beoogd inzicht te verschaffen in de relevante aspecten waar risico's voor de bescherming van privacy van burgers optreden of kunnen optreden en waaraan vanuit die achtergrond op dit moment in het wetgevingstraject of in andersoortige borging van beschermende maatregelen nadere aandacht besteed dient te worden.

---

bijzondere bevoegdheden in de digitale wereld', in Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013).

[4] Zie Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013).

[5] Over de keuze van terminologie om deze bevoegdheid aan te duiden, zie par. 8.3.1

[6] Zie bijvoorbeeld het jaarverslag van de CTIVD 2014-2015, met name hoofdstuk 5.

## 1.3 Karakter van deze PIA en onderzoekskader

Voor een Privacy Impact Assessment op de Wiv 20xx is geen vaststaand, gevalideerd raamwerk beschikbaar. Er bestaat een ‘Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst’, maar dat is formeel geen goed uitgangspunt, omdat het zich richt op een toets van persoonsgegevensverwerking op basis van de Wet bescherming persoonsgegevens (en de daarachter liggende Europese richtlijn 95/46/EG), die niet van toepassing is op het werk van de inlichtingen- en veiligheidsdiensten.

Bovendien gaat het bij het Toetsmodel vooral om een *toets*, waarbij wordt vastgesteld of een wetsvoorstel of systeem voldoet aan de juridische eisen op het gebied van privacy en bescherming van persoonsgegevens. Een Privacy Impact Assessment is daarentegen niet zozeer een juridische toets als wel een inschatting van de uitwerking die een voorstel kan hebben op de privacy. Het is belangrijk om het karakter van de PIA zoals wij deze in dit onderzoek hebben opgevat, te benadrukken.

De Privacy Impact Assessment in dit rapport betreft **geen privacytoets**, **maar een inschatting van privacyrisico’s** van de voorgestelde wettelijke regeling en van de voorgestelde wettelijke maatregelen om deze privacyrisico’s te beperken. Dit rapport toetst dus niet of het wetsontwerp Wiv 20xx voldoet aan de eisen van artikel 8 EVRM. Het biedt een analyse van de mate waarin de privacy van burgers geraakt wordt door het wetsvoorstel en van onderdelen waar de voorgestelde normering van de bevoegdheden vragen oproept gegeven deze mate van privacyinbreuk.

Voor een begrip van de mate waarin privacy geraakt wordt, sluiten wij aan bij artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM), dat in het eerste lid de reikwijdte van de bescherming van de persoonlijke levenssfeer aangeeft en in het tweede lid de voorwaarden waaronder inmenging van het openbaar gezag is toegestaan. In de bepaling van wat dan precies tot de bescherming van de persoonlijke levenssfeer behoort, is in de loop der jaren veel jurisprudentie ontwikkeld, onder andere via de uitspraken van het Europees Hof van de Rechten van de Mens (EHRM). Deze uitspraken bieden een interpretatie van wat het Europees Hof verstaat onder privacy en onder de vereisten die een inbreuk op de privacy kunnen rechtvaardigen. Daarbij gaat het vooral om legaliteit (voorzienbaarheid bij wet) en noodzakelijkheid. Onder voorzienbaarheid bij wet valt niet alleen de vraag of een privacyinbreuk geregeld is in een formele wet (of in een andere vorm van regelgeving die voldoende inzichtelijk is voor burgers), maar ook de vraag of de wet voldoende kwaliteit heeft: is de privacyinbreuk voldoende gedetailleerd uitgewerkt en met voldoende precieze waarborgen omkleed? Onder noodzakelijkheid in een democratische samenleving wordt verstaan of maatregelen voldoen aan de vereisten van proportionaliteit (keuze voor een middel dat in verhouding staat tot het te realiseren doel) en subsidiariteit (keuze voor het minst ingrijpende middel dat geschikt is het doel te bereiken), waarbij een scherpe beoordeling plaatsvindt of deze worden gerechtvaardigd door een ‘pressing social need’. Het derde vereiste, dat de privacyinbreuk een legitiem doel dient, krijgt minder aandacht in dit rapport, aangezien het wetsvoorstel maatregelen regelt in het kader van nationale veiligheid, dat expliciet als doel is genoemd in artikel 8 lid 2 EVRM (al is de interpretatie van dat begrip niet eenduidig, zie par. 3.1).

Hoewel dit rapport geen toets uitvoert, vormt artikel 8 EVRM aldus wel een belangrijk deel van het kader waarbinnen deze PIA vorm krijgt. Daarom is in bijlage I een overzicht opgenomen van het privacykader van artikel 8 EVRM. Bij de interpretatie daarvan speelt inmiddels ook artikel 7 en 8 van het Handvest van de Grondrechten van de EU in toenemende mate een rol, vanwege artikel 52 lid 3 Handvest dat aangeeft dat de desbetreffende grondrechten dezelfde betekenis en reikwijdte hebben (zie Bijlage, par. A.1.2). In deze rapportage wordt verder verwezen naar EHRM- en EHJ-jurisprudentie waar deze bijdraagt aan het beter begrijpen van de privacyrisico's; de bijlage biedt daarbij een referentiekader voor de lezer om desgewenst na te kijken welke rol de desbetreffende uitspraak speelt binnen het kader van artikel 8 EVRM.

Naast artikel 8 EVRM vult ook de Nederlandse grondwettelijke bescherming van privacy (artikelen 10, 11, 12 en 13 Gw) het privacykader voor deze PIA nader in. Het betreft hier de mate van toegestane inbreuk op de persoonlijke levenssfeer, de lichamelijke integriteit, het huisrecht, en het brief- en telecommunicatiegeheim,[7] en de hiermee corresponderende waarborgen. Via de band van artikel 8 EVRM en artikel 10 leden 2-3 Gw kleuren daarnaast ook de beginselen van bescherming van persoonsgegevens, zoals doelbinding en proportionaliteit en subsidiariteit van gegevensverwerking, het privacybegrip nader in.

## 1.4 Afbakening van het onderzoek

Er valt veel te zeggen over de privacyimplicaties van het wetsontwerp. Een grondige analyse van alle privacyrisico's vergt veel meer onderzoekscapaciteit dan ons ter beschikking stond voor dit onderzoek. Daarom zijn keuzes nodig geweest.

In de eerste plaats hebben wij ervoor gekozen om ons te richten op een brede analyse van het wetsontwerp – het gaat tenslotte om een PIA op de wet als geheel – en dus een meer globale inschatting te geven van privacyrisico's van veel onderdelen, in plaats van een diepgaande inschatting van privacyrisico's van slechts enkele onderdelen. Ook bij een brede analyse was het echter niet mogelijk om op alle onderdelen in te gaan; vanwege de beperking in onderzoekscapaciteit hebben we sommige onderdelen buiten beschouwing moeten laten, zoals de inzet van agenten, naslag, het 'treffen van maatregelen' (verstoring), notificatie, klokkenluidersregeling, inzage- en correctierechten en het klachtrecht. Daarbij hebben we laten meewegen dat het minder urgent is om aandacht te besteden aan onderdelen die reeds in andere deelonderzoeken of rapporten zijn behandeld[8] en aan onderdelen die materieel ongewijzigd zijn van de Wiv 2002 (tenzij technologische ontwikkelingen de invulling van bestaande onderdelen wezenlijk beïnvloeden).

[7] Er is een voorstel aanhangig om art. 13 Gw om te vormen tot een brief- en telecommunicatiegeheim (*Kamerstukken II* 2013-14, 33 989, nrs. 1-2). Hoewel dit voorstel nog niet is aangenomen, gaan wij er voor de doeleinden van dit onderzoek van uit dat onder art. 13 Gw alle vormen van telecommunicatie vallen, inclusief Internet-gebaseerde communicatie, aangezien hierover min of meer consensus bestaat. Over de grondwettelijke regeling van de beperkingen op het brief- en telecommunicatiegeheim in het kader van de nationale veiligheid bestaat geen consensus, zodat we daarover geen uitspraken zullen doen. Gezien het grote gewicht van de bescherming van communicatie binnen de privacybescherming, gaan we er echter wel van uit dat er zware eisen zullen moeten worden gesteld aan inbreuken op het telecommunicatiegeheim, ongeacht of deze eisen grondwettelijk verankerd zijn dan wel in lagere wetgeving – in de Wiv 20xx zelf – worden geregeld.

[8] Zie onder andere Loof e.a. 2015; Eskens, van Daalen & van Eijk 2015.

In de tweede plaats hebben wij ervoor gekozen om vooral ook die onderdelen te behandelen die wel degelijk privacyrisico's oproepen maar die mogelijk onderbelicht blijven in het publieke debat en wetgevingstraject, omdat ze minder prominent zijn dan de meest in het oog springende onderdelen. Parallel aan de onderhavige PIA heeft het ministerie een consultatie uitgezet in juli-augustus 2015, die ruim 1100 reacties heeft opgeleverd, waarvan ongeveer de helft openbaar. Veel van de reacties gaan in op de voorgenomen verbreding van de bevoegdheden van de diensten met betrekking tot de zogenoemde kabelgebonden bulkinterceptie en/of op de regeling van het toezicht. Omdat veel van de reacties uit de consultatie, alsook andere gepubliceerde bijdragen aan het debat over de nieuwe Wiv, betrekking hebben op de kabelgebonden bulkinterceptie en de regeling van het toezicht, hebben wij besloten om deze aspecten wel kort mee te nemen in de PIA maar er geen bijzondere nadruk op te leggen. De omvang en argumentatie van de reacties geeft immers al genoeg aanleiding voor de wetgever om zich fundamenteel te herbezinnen op deze onderdelen van het wetsvoorstel.

Dit betekent de PIA vooral ruimte biedt om ook andere aspecten te bekijken die eveneens vragen om een goede balans tussen bevoegdheden en beperkingen en die in het publieke debat tot nu toe minder prominent naar voren zijn gekomen, zoals de regeling van observatie of het binnendringen in computers, of de afwezigheid van een regeling betreffende onderzoek van open (Internet-)bronnen of een bepaling over privacy en gegevensbescherming *by design* en *by default*.
In de derde plaats beperken wij ons tot de privacy van burgers. De privacy van medewerkers van de AIVD en MIVD of personen die werkzaamheden verrichten voor de diensten valt buiten het bestek van deze rapportage. Niet dat de privacy van deze personen niet van belang is (niet voor niets legt artikel 15 Wiv 20xx een zorgplicht op aan de diensthoofden om de veiligheid van hun ambtenaren te waarborgen, waarvoor onder andere de privacy van deze personen afdoende moet worden beschermd), maar dit belang is van een andere aard en reikwijdte dan het privacybelang van burgers die mogelijk geraakt worden door de taakuitoefening van de diensten.

In de vierde plaats is onze beschouwing relatief algemeen van aard: wij richten ons op de wettelijke regeling zelf, en de manier waarop deze wettelijke regeling geïnterpreteerd moet of kan worden volgens de Memorie van Toelichting. Hierbij moet voor ogen worden gehouden dat de concrete privacyrisico's van specifieke onderdelen van de wet kunnen verschillen afhankelijk van de context waarin deze worden toegepast. Zo zal de interpretatie van bepaalde onderdelen kunnen verschillen afhankelijk van de situatie of een bevoegdheid binnen Nederland of in het buitenland wordt uitgeoefend, of in de context van een concrete, urgente dreiging, een militaire missie dan wel een meer abstracte of langeretermijndreiging. Bij de inschatting van privacyrisico's nemen wij deze context slechts mee voor zover dit mogelijk is binnen een relatief algemene beschouwing over de wettelijke regeling en voor zover de Memorie van Toelichting voldoende aanknopingspunten biedt om de contextafhankelijkheid van voorgestelde bevoegdheden in te schatten. Waar de MvT bijvoorbeeld aangeeft dat een bepaalde bevoegdheid noodzakelijk is binnen een bepaalde context, dan wel een bepaalde waarborg niet goed kan worden getroffen in een specifieke situatie, zoals een militaire operatie of een acute dreiging, is dat meegenomen in onze analyse; waar de MvT echter dergelijke contextspecifieke voorbeelden achterwege laat, kon in onze analyse niet altijd rekening worden gehouden met specifieke contexten of uitzonderingssituaties die

zich in de uitvoeringspraktijk kunnen voordoen. Waar dit betekent dat onze analyse of aanbevelingen onvoldoende rekening houden met specifieke contexten of uitzonderingssituaties, zal de wetgever dit in de reactie op deze PIA kunnen aangeven en in de Memorie van Toelichting nader moeten toelichten hoe deze specifieke contexten uitwerken op de voorgestelde maatregelen.

## 1.5 Onderzoeksaanpak

Bij het uitvoeren van het onderzoek is de volgende onderzoeksaanpak gevolgd.

1. Ten eerste zijn de wettekst en de Memorie van Toelichting doorgenomen; dit levert een eerste beeld op van aspecten die in het kader van privacyrisico's nader bestudeerd dienen te worden.
2. Vervolgens zijn de meest relevante rapportages over de desbetreffende materie doorgenomen, met name de evaluatie van de commissie-Dessens en de van belang zijnde rapportages van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten.
3. Er is een jurisprudentie-onderzoek uitgevoerd van relevante uitspraken van het Europees Hof voor de Rechten van de Mens, die van belang zijn voor de in de Wiv 20xx voorziene uitvoering van de bevoegdheden van de diensten; dit geeft een beeld op van de mate waarin privacy wordt geraakt en van maatregelen die nodig zijn om privacyinbreuken te rechtvaardigen. Het overzicht is opgenomen in bijlage I; de inzichten zijn verder verwerkt in de analyse, waarbij op relevante plaatsen in de tekst wordt verwezen naar jurisprudentie uit de bijlage.
4. Op basis van de voorgaande stappen is een eerste analyse gemaakt van de privacyrisico's van het wetsontwerp.
5. Met behulp van vier interviews, met vertegenwoordigers van de diensten, de CTIVD en een onafhankelijke expert (zie bijlage II), is het beeld van zaken die aandacht verdienen nader aangescherpt. Ook is door de interviews meer contextinformatie verkregen over de praktische uitwerking van de regeling van de activiteiten van de diensten onder de Wiv 2002 en het concept-wetsvoorstel. De interviews dienden aldus ter aanvulling op de tussentijdse bevindingen en ter contextualisering van de wetsteksten.
6. Tot slot is een eerste versie van de bevindingen intern beoordeeld door prof.dr. Mireille Hildebrandt, verbonden aan de Radboud Universiteit. Zij heeft geen andere rol gespeeld in het eerdere werk van de onderzoekers dan het aanleveren van potentieel interessante stukken en het aanreiken van pertinente aandachtspunten inzake de afwegingen die bij de aanschaf, inrichting en transparantie van de technische systemen gemaakt moeten worden.

Het PI.lab heeft het onderzoek in volstrekte onafhankelijkheid uitgevoerd. Bij de aanvang van het project is er een overleg geweest met de opdrachtgever, de directie Constitutionele Zaken en Wetgeving van het ministerie van BZK. Bij dit overleg zijn het hoofd juridische zaken van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het hoofd juridische zaken van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) aanwezig geweest. Hierbij is de vraagstelling verduidelijkt. Een concept van het rapport is aan het eind van het traject voorgelegd aan de opdrachtgever, waarbij dezelfde betrokkenen in de gelegenheid zijn gesteld opmerkingen te maken en op feitelijke onjuistheden te wijzen. De onderzoekers hebben naar aanleiding hiervan feitelijke onjuistheden verbeterd en verder naar eigen inzicht de opmerkingen verwerkt, wat op enkele punten tot aanscherping van de argumentatie of verduidelijking van de tekst heeft geleid.

Het onderzoek is uitgevoerd van juli tot november 2015. De rapportage is afgerond in januari 2016.

## 1.6 Opbouw van de rapportage

In de komende hoofdstukken worden de verschillende aspecten aan de Wiv 20xx op systematische wijze doorgenomen. Hoofdstuk 2 geeft een inleidende beschouwing over de Wiv 20xx als geheel, met een algemene indruk van de noodzaak tot wijziging en de met het wetsvoorstel gepaard gaande privacyrisico's, inclusief enkele algemene opvalpunten. Hoofdstuk 3 gaat in op de taakstelling van de diensten, en belicht de veranderingen in de aard van de samenwerking tussen de diensten. Hoofdstuk 4 gaat in op het algemene kader dat de bevoegdheden van de diensten normeert, waaronder zowel de algemene bepalingen over gegevensverwerking vallen als het algemene kader voor bijzondere bevoegdheden.

Vervolgens worden de bevoegdheden besproken, gegroepeerd naar de aard van privacy waarop deze bevoegdheden inbreuk maken. De groepering is ingegeven door een indeling van het privacybegrip in vier dimensies: informationele, lichamelijke, ruimtelijke en relationele privacy. Deze indeling wordt ook gehanteerd in de Grondwet, waarbij naast het algemene privacyrecht (art. 10 lid 1 Gw) vier bijzondere aspecten van privacy apart worden geregeld: persoonsgegevens (art. 10 lid 2-3 Gw), het lichaam (art. 11 Gw), het huis (art. 12 Gw) en de (middellijke[9]) communicatie (art. 13 Gw). In hoofdstuk 5 behandelen we vier onderdelen die aandacht vergen vanuit de informationele privacy: de algemene bevoegdheid tot gegevensverwerking, het verwerken van gegevens uit open bronnen (OSINT), geautomatiseerde data-analyse en het delen van gegevens (met name met opsporingsdiensten en met buitenlandse inlichtingen- en veiligheidsdiensten). Hoofdstuk 6 behandelt het DNA-onderzoek, dat samenhangt met de lichamelijke privacy. In hoofdstuk 7 komt de ruimtelijke privacy aan de orde, waaronder bevoegdheden tot observatie binnen en buiten de woning en het onderzoeken van plaatsen, waarbij we ook ingaan op de veranderende rol van observatie in de publieke ruimte. Daarnaast wordt het binnendringen in computers hier behandeld, als eigentijdse digitale variant van het onderzoek van fysieke plaatsen. Hoofdstuk 8 behandelt vervolgens vier aspecten van het onderzoek van communicatie: het onderscheppen van brieven, medewerkingsplichten voor communicatieaanbieders en de gerichte en bulkinterceptie.

Na de bespreking van bevoegdheden komen twee typen waarborgen aan bod. Hoofdstuk 9 behandelt het toezicht op de uitoefening van bevoegdheden, zowel toezicht vooraf als achteraf. Hoofdstuk 10 bespreekt de rol van waarborgen in de technische en organisatorische architectuur van de taakuitvoering en de systemen waarmee bevoegdheden worden uitgevoerd.
Hoofdstuk 11 geeft tot slot een overzicht van de belangrijkste conclusies en aanbevelingen.

[9] De kern van art.13 Gw is het beschermen van communicatiekanalen waarlangs communicatie plaatsvindt die aan derden voor transport is toevertrouwd. Dit kan worden aangeduid als 'middellijke communicatie', ter onderscheiding van onmiddellijke communicatie (het zogenoemde 'live gesprek'). Voor het doeleinde van dit rapport behandelen we overigens de onmiddellijke communicatie tegelijk met de middellijke communicatie, omdat beide betrekking hebben op relationele privacy en daarnaast het wetsvoorstel zelf ook geen aparte regeling kent voor beide typen.

Waar in de tekst verwezen wordt naar paragrafen en hoofdstukken, betreffen deze de onderhavige rapportage; waar verwezen wordt naar paragrafen in het wetsontwerp, wordt dat expliciet vermeld.

# 2 Algemene indruk Wiv 20xx

## 2.1 Achtergrond

De Wiv 20xx is het resultaat van een besluitvormingsproces dat begon in 2006 met de indiening van een aanpassing op de Wet inlichtingen- en veiligheidsdiensten 2002, het zogenoemde post-Madrid-wetsvoorstel.[10] Deze aanpassing werd in de Tweede Kamer aangenomen, maar stuitte op sterk en blijvend verzet van de Eerste Kamer, onder meer vanwege de erin vervatte eis van verplichte medewerking door aanbieders van communicatiediensten tot het leveren van gegevens. Bij brief d.d. 17 maart 2011 trok de minister van BZK het wetsvoorstel in,[11] onder verwijzing naar de mogelijkheid om bepaalde wijzigingen op te nemen in een eventueel nieuw in te dienen wetsvoorstel. De voorbereiding van dat nieuwe wetsvoorstel was reeds begonnen, resulterend in een concept eind 2011. Als gevolg van het verschijnen van het toezichtsrapport nr. 28 van de CTIVD is echter door de toenmalige minister van Defensie aangegeven dat het wetsvoorstel ook een regeling zou moeten gaan treffen voor onder andere de door de CTIVD geconstateerde gebreken in de wetgeving. Daaraan is in de eerste helft van 2012 gewerkt. Voorts is in 2012 in de Tweede Kamer een motie aangenomen om een evaluatieonderzoek in te stellen van de dan tien jaar oude Wet inlichtingen- en veiligheidsdiensten 2002.[12] Met de instelling van de Evaluatiecommissie Wiv 2002, naar haar voorzitter de commissie-Dessens genaamd, werd het wetgevingsproces opgeschort.

Het rapport van de commissie-Dessens verscheen in december 2013. De Commissie bepleit een zorgvuldig en gebalanceerd stelsel van toezicht en controle in het licht van een noodzaak tot uitbreiding van de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten. De Commissie gaat voor een deel mee in de argumentatie van het kabinet dat veranderende technologische omstandigheden nopen tot een uitbreiding van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Wel stelt de Commissie dat, bij een dergelijke uitbreiding van bevoegdheden, een passend stelsel van waarborgen noodzakelijk is. De Commissie argumenteert om deze waarborgen waar noodzakelijk, gegeven de mogelijke inbreuk op de persoonlijke levenssfeer van betrokkenen, te realiseren via de instelling van een onafhankelijk toetsend orgaan.[13] Het Kabinet besloot deze argumentatie van de commissie-Dessens niet te volgen, en te blijven bij het stelsel van Ministeriële toestemming, waarbij politieke controle via de Commissie inlichtingen- en veiligheidsdiensten (CIVD) geboden zou kunnen worden en verder het klachtrecht versterkt zou worden door de CTIVD aan te wijzen als onafhankelijke klachtbehandelaar met bindende oordelen.

Mede op basis van de evaluatie is een nieuw wetsontwerp gemaakt dat de huidige Wiv 2002 moet vervangen, waarbij ook enkele onderdelen uit het gesneuvelde post-Madrid-voorstel zijn overgenomen. Dit wetsontwerp, een voorstel voor een

[10] *Kamerstukken II* 2005/06, 30 553 nr. 2; zie ook Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p. 42-43.
[11] *Kamerstukken II* 2010/11, 30 553, nr. 18.
[12] *Kamerstukken II* 2011/12, 29 924, nr. 81.
[13] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), pp. 99-100. De Commissie ontvouwt een argumentatie waarin zij tot de conclusie komt dat extern preventief toezicht slechts gewenst is als blijkt dat het niet mogelijk is om via andere vormen van toezicht dit toezicht effectief te versterken.

Wet inlichtingen- en veiligheidsdiensten 20xx, is in juni 2015 opengesteld voor publieke consultatie. Dit moet het voorlopige sluitstuk worden van een procedure die inmiddels bijna tien jaar geleden is gestart. Een voordeel van de vertraging in de realisering van een op de huidige technologische ontwikkelingen toegesneden wettelijk regime is dat ook technische ontwikkelingen van meer recente datum kunnen worden meegenomen, zoals Big Data en het steeds naderbij komende Internet der Dingen (Internet of Things). Hoewel de wetgever streeft naar technologie-onafhankelijke regelgeving, om te voorkomen dat de wet te snel verouderd raakt, en daarom geen specifieke technologieën worden genoemd in de wettelijke bepalingen, baseert hij zich, bij het vormgeven van de bepalingen, natuurlijk wel op wat op dit moment voorstelbaar is in technische zin om de bevoegdheden van de diensten uit te voeren. Het huidige wetsvoorstel kan dan ook niet los worden gezien van de technologische ontwikkelingen die momenteel en in de voorzienbare toekomst plaatsvinden. Aangezien de wetgever beoogt de bevoegdheden van de diensten zoveel mogelijk los van concrete technologieën te formuleren, zal de koppeling tussen de abstract geformuleerde bevoegdheden en de concrete uitwerking daarvan in de praktijk vooral in de Memorie van Toelichting moeten worden gelegd. Of dat voldoende gebeurt, zal in de desbetreffende delen van deze rapportage bekeken worden.

## 2.2 Algemene indruk van het wetsvoorstel

De behoefte aan een omvangrijk stelsel van wetsartikelen – in ieder geval dus beduidend omvangrijker dan de Wiv 2002 – blijkt uit een aantal aspecten die vanuit een oogpunt van waarborging van de privacy van belang zijn. Relevante voorbeelden zijn:

1. Het concept-wetsvoorstel bevat een nieuw wetsartikel (artikel 28) dat het verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen toestaat onder voorwaarde dat dit gebeurt om de identiteit van een persoon vast te stellen.
2. De bevoegdheid om binnen te dringen in een geautomatiseerd werk wordt uitgebreid, onder meer met het verkennen van de technische kenmerken van de geautomatiseerde werken (die op een telecommunicatienetwerk zijn aangesloten; artikel 30).
3. Ongerichte interceptie is niet langer beperkt tot draadloze telecommunicatie, maar wordt uitgebreid tot elke vorm van telecommunicatie of overdracht van gegevens via geautomatiseerde werken (artikel 33, 34 en 35). De regeling volgt het drietrapsmechanisme dat voor deze interceptie is opgesteld.[14] Dit drietrapsmechanisme is in de opeenvolgende artikelen 33 tot en met 35 uitgewerkt.
4. Er worden nieuwe eisen gesteld aan de informatie- en medewerkingsplicht van aanbieders van communicatiediensten. Deels betreft dit nieuwe plichten (artikel 36, 37 en 38); deels betreft dit een wijziging van bestaande informatie- en medewerkingsplichten (rond verkeersgegevens en abonneegegevens; artikel 39 en 40).
5. De bevoegdheid tot het binnentreden van plaatsen en deze plaatsen te voorzien van registratie- en observatiemiddelen wordt verruimd (artikel 42).
6. De notificatieplicht (artikel 46) heeft betrekking op vergelijkbare artikelen in de Wiv 2002, waarbij de nieuwe aanpak rond bulkinterceptie van elke vorm van

[14] Zie onder meer *Kamerstukken II* 2014/15, 33 820, nr. 4, p. 4-5.

telecommunicatie of gegevensoverdracht via een geautomatiseerd werk in het voorstel wordt uitgezonderd van de notificatieplicht (artikelen 33-35).

7. De Wiv 20xx spreekt over samenwerkingsrelaties tussen de inlichtingen- en veiligheidsdiensten van Nederland en andere landen (artikel 76 en 77) waar in de Wiv 2002 sprake was van het onderhouden van verbindingen (artikel 59 Wiv 2002). In de samenwerkingsrelaties kan sprake zijn van het uitwisselen van ongeëvalueerde gegevens (artikel 77 lid 2).
8. Het aantal instanties dat werkzaamheden kan verrichten ten behoeve van de AIVD wordt uitgebreid ten opzichte van de Wiv 2002 met de Hoofddirecteur van de IND van het ministerie van Veiligheid en Justitie en de inspecteur-generaal van de inspectie SWZ van het ministerie van Sociale Zaken en Werkgelegenheid (artikel 79).
9. Aan de kant van de aanvullende waarborgen bevat het wetsvoorstel de instelling van een aparte afdeling Klachtafhandeling als onderdeel van de Commissie Toezicht Inlichtingen- en Veiligheidsdiensten (CTIVD; artikelen 85-94 – instelling aparte afdeling klachtenafhandeling; artikelen 95-99 – algemene bevoegdheden; artikelen 103-113 – procedure klachtafhandeling; artikel 114-120 – melding van een misstand).

Uit dit schetsmatige overzicht komt naar voren dat er op verschillende onderdelen sprake is van een verruiming van de bevoegdheden van de inlichtingen- en veiligheidsdiensten. Deze verruiming zal gepaard moeten gaan met de inzet van een juist instrumentarium aan waarborgen zodat de balans tussen bevoegdheden en waarborgen geborgd blijft. In dit rapport staat centraal of het concept-wetsvoorstel bij het vinden van deze balans voldoende rekening houdt met de impact van de voorstellen op de privacy. Op dit moment volstaat het wetsontwerp met de constatering dat de wetgever inzet op striktere toepassing van het toestemmingsvereiste door de betreffende Minister en de instelling van een nieuwe afdeling Klachtafhandeling bij de CTIVD. Zoals hiervoor al opgemerkt gaat de wetgever met deze aanpak voorbij aan de argumentatie die de commissie-Dessens ten aanzien van extern toezicht op de toestemmingsvereiste heeft ontvouwd.[15] In het licht van een recente uitspraak van Hof Den Haag (zie hfd.9) is deze keuze van de wetgever op voorhand betwijfelbaar. De nadere analyse in deze rapportage zal het belang onderstrepen van adequaat en onafhankelijk toezicht, gezien de privacyrisico's die de uitbreiding dan wel veranderde vormgeving van bevoegdheden met zich meebrengt.

## 2.3 Algemene opvalpunten

Bij onze analyse van het wetsontwerp zijn drie meer algemene punten opgevallen die aandacht vergen vanuit privacybescherming (maar ook meer algemeen vanuit het belang van zorgvuldige wetgeving en rechtsbescherming). Het gaat om mechanismen die een belangrijk risico inhouden voor de zorgvuldigheid waarmee wetgeving en rechtsbescherming tot stand komen.

### *2.3.1 De wet volgt de praktijk?*

Het eerste mechanisme is dat in diverse opzichten de wet de praktijk lijkt te volgen, terwijl – normaliter – het omgekeerde het geval zou moeten zijn. In het concept-wetsvoorstel worden enkele bestaande praktijken gecodificeerd, zoals het doen van naslag (het nazoeken in de eigen bestanden, op verzoek van derden, om te kijken

[15] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p. 99-100.

of er relevante informatie over iemand in staat, MvT, p. 10), het doen van DNA-onderzoek aan voorwerpen (MvT, p. 44), en het verlenen van toestemming op ministerieel niveau voor het binnendringen in computers (MvT, p. 54). Belangrijker is het feit dat op veel punten de bevoegdheden worden uitgebreid omdat de diensten in de praktijk tegen beperkingen aanlopen, zoals het binnendringen in computers ter ondersteuning van andere bevoegdheden, of bij verwerving en verwerking van satellietcommunicatie waarbij er geen wettelijke basis is voor bepaalde vormen van search of een regeling voor metadata-analyse.[16]

Het is evident dat wetten niet voor de eeuwigheid geschreven zijn en dat, waar de maatschappij ingrijpend verandert, een wet aangepast moet worden zodat deze het beoogde doel nog kan bereiken in een veranderde samenleving. Tegelijkertijd is het ook evident dat een wet niet uitsluitend aangepast moet worden enkel omdat er veranderingen in de maatschappij plaatsvinden. De wet normeert de praktijk, niet andersom. Daarom moet een wetgever terughoudend zijn met het aanpassen van de wet enkel op basis van het argument dat de uitvoeringspraktijk tegen problemen aanloopt. Weliswaar kan het legitiem zijn de wet aan te passen waar er onvoorziene obstakels rijzen in de uitvoering, maar men moet zich steeds afvragen of deze obstakels daadwerkelijk onvoorzien(baar) waren, en of de grenzen van de wet niet juist ook bedoeld zijn om de uitvoering aan bepaalde beperkingen te onderwerpen. Juist in een domein waarin de balans tussen de behoefte in de praktijk om zoveel mogelijk informatie te verzamelen enerzijds en de bescherming van privacy (en andere grondrechten) zo precair is als in de nationale veiligheid, moet de vraag voorop staan of beperkingen waar de uitvoeringspraktijk tegenaan loopt inherent zijn aan de balans die de wetgever heeft gezocht – de diensten moeten nu eenmaal niet alles kunnen wat technisch mogelijk is – dan wel of deze beperkingen dermate onvoorzien of onvoorzienbaar zijn dat deze de getroffen balans feitelijk verstoren doordat zij de uitvoering meer dan nodig begrenzen.

In het huidige wetsontwerp geeft de wetgever zich naar onze indruk niet altijd voldoende rekenschap van het feit dat de wet de praktijk behoort te normeren, en niet andersom. De toelichting redeneert regelmatig tamelijk gemakkelijk dat een beperking waar in de praktijk tegenaan wordt gelopen redengevend is om de wet op dat punt aan te passen. Daarmee is de noodzaak in een democratische samenleving echter nog lang niet aangetoond. Het moet duidelijk gemaakt worden dat een bepaalde ontwikkeling, zoals een verandering in het technologische landschap, een beperking oplevert voor de diensten die a) niet beoogd is door de wetgever en b) niet acceptabel is, voordat deze redengevend kan zijn voor een uitbreiding van bevoegdheden.

Een andere conclusie die voortvloeit uit het mechanisme dat het wetsontwerp soms nogal gemakkelijk te huidige praktijk als referentiekader hanteert, is dat het vragen oproept over de normeringskracht van de voorgestelde wet voor de werkzaamheden van de diensten in de toekomst. Aangezien de wetgever beoogt om met de huidige wet aan te geven wat de balans is tussen effectiviteit van de taakuitvoering van de diensten om de nationale veiligheid te beschermen en rechtsbescherming van burgers, kan het niet zo zijn dat wanneer de wet eenmaal van kracht is, er weer praktijken ontstaan die een inbreuk op grondrechten maken waarin de wet niet voorziet.

[16] Zie ook CTIVD 2015c, p. 31.

Dit betekent dat in elk geval het toezicht op de taakuitoefening scherp zal moeten bewaken dat de grenzen van de wet niet worden overschreden door nieuwe toepassingen of praktijken die in het huidige voorstel niet zijn voorzien; het is niet de bedoeling dat de diensten via een praktische interpretatie van ruim geformuleerde bevoegdheden mogelijkheden in de wet inlezen die niet door de huidige wetgever zijn beoogd. Dat komt in strijd met de voorzienbaarheid van de wet voor de burgers, en met de rechtszekerheid. Hiervoor is onafhankelijk en kritisch toezicht een noodzakelijke voorwaarde. Het betekent ook dat de toelichting bij de wet zoveel mogelijk moet duiden op welke manier de ruim geformuleerde bevoegdheden uitgelegd moeten worden in het licht van technologische ontwikkelingen die op dit moment voorzienbaar zijn. Dit versterkt de in par. 2.1 al aangestipte noodzaak om in de MvT uitgebreid in te gaan op huidige en toekomstige technologieën. Maar bovenal betekent het dat er geen dynamiek moet ontstaan dat in elke nieuwe versie van de Wiv actuele knelpunten in de praktijk vrijwel automatisch leiden tot een aanpassing, die veelal een uitbreiding inhoudt, van bevoegdheden. Tekenend is dat de huidige regeling van draadloze interceptie in de Wiv 2002 al een codificatie was van een voorheen gegroeide praktijk van de diensten onder de voorganger van de Wiv 2002 (MvT, p. 63), terwijl nu een in de praktijk ervaren knelpunt rond kabelgebonden verkeer als reden wordt opgevoerd om de interceptiebevoegdheden opnieuw verder uit te breiden. Op deze manier dreigt een neerwaartse spiraal van wetgeving die de behoeften van de praktijk volgt, in plaats van wetgeving die de behoeften van de praktijk kanaliseert en begrenst.

### *2.3.2 Gebruik van retorische middelen*

Een tweede mechanisme dat opvalt is dat op enkele plaatsen de Memorie van Toelichting gebruik maakt van retorische middelen (of, negatief uitgedrukt, retorische trucs). Mogelijk is dat niet bewust gedaan (het gaat om relatief ondergeschikte onderdelen), maar dat maakt niet uit voor het retorische effect van de gehanteerde argumentatiepatronen.

Ten eerste wordt op verschillende plaatsen gewezen op het feit dat een onderdeel al was opgenomen in het vorige, ingetrokken ('post-Madrid') wetsvoorstel.[17] De regelmaat waarmee deze verwijzingen door de MvT zijn verweven, zonder verdere toelichting, wekt de suggestie dat het hier om een redengevend argument gaat. Impliciet ontstaat namelijk de suggestie dat het feit dat een onderdeel reeds in het vorige, door de Tweede Kamer aanvaarde, wetsvoorstel was opgenomen, als zodanig een argument is voor de aanvaardbaarheid van het onderdeel. Dat miskent dat het wetsvoorstel niet door het parlement is aangenomen; het feit dat het onderdeel uitmaakte van het vorige wetsvoorstel zegt als zodanig niets en is dus niet relevant. Slechts op één plaats (MvT, p. 5) wordt tussen haakjes gemeld dat het om 'niet-controversiële' onderdelen van het post-Madrid-voorstel ging, oftewel onderdelen waar de kritiek van de Eerste Kamer zich niet op richtte. Dat kan als zodanig wel een argument zijn – het geeft aan dat het parlement zich eerder instemmend, of althans niet afstemmend, heeft uitgelaten over een onderdeel. Maar dat zou dan wel, voor elk afzonderlijk onderdeel, als zodanig benoemd en onderbouwd moeten worden met een specifieke verwijzing naar de instemming van de Eerste Kamer met dat onderdeel. Bovendien is het geen zwaarwegend argument: de Eerste Kamer heeft niet formeel ingestemd met het onderdeel, en bovendien ligt er zo'n vijf jaar tussen beide wetsvoorstellen; noch het parlement

[17] Zie MvT, p. 8, 27, 55, 57, 59, 68, 85, 111, 118, 147-149.

noch de maatschappelijke context zijn hetzelfde als toen het post-Madrid-voorstel werd behandeld. De vraag is dan ook met welk doel de vele verwijzingen naar het post-Madrid-voorstel in de toelichting zijn opgenomen. In elk geval moet worden voorkomen dat de indruk ontstaat dat het hier gaat om onderdelen die minder aandacht behoeven vanwege het enkele feit dat ze al eens in het parlement zijn besproken.

Ten tweede is er op enkele plaatsen sprake van verhullend taalgebruik, niet alleen in de toelichting maar ook in de voorgestelde wetstekst zelf. Het gaat dan om een term als ‘verzoek’ (zie bijvoorbeeld artikelen 30 en 36-41), waarbij degene die ‘verzocht’ wordt formeel verplicht is om mee te werken (art. 30 lid 8, art. 36 lid 4 enz.), zelfs met dreiging van gevangenisstraf bij niet-meewerken (zie daarover nader par. 7.2.8). Ook de term ‘zo spoedig mogelijk’ in artikelen 30 lid 9, 32 lid 10 en 38 lid 7 is een voorbeeld van verhullend taalgebruik, aangezien in deze bepalingen wordt aangegeven dat de diensten ‘zo spoedig mogelijk’ gegevens op relevantie onderzoeken, terwijl zij tegelijkertijd de mogelijkheid openlaten dat de gegevens na twaalf maanden nog niet zijn onderzocht op relevantie (in welk geval ze zouden moeten worden vernietigd). Het is misleidend om een term als ‘zo spoedig mogelijk’ te gebruiken als er een zo lange periode mee wordt bedoeld (zie nader par. 7.2.9). Ook vermijdt de wetgever een inhoudelijke term te kiezen om de bevoegdheden van artikelen 33-35, die in de plaats komen van de huidige ‘ongerichte interceptie’, aan te duiden; de gehanteerde term interceptie ‘in andere gevallen dan bedoeld in artikel 32’ (art. 33 lid 1 Wiv 20xx) geeft geen enkele inhoudelijke aanduiding van het type bevoegdheid dat hier aan de orde is. Hiermee wordt de burger geen enkel inzicht geboden dat het feitelijk gaat om niet op specifieke personen of organisaties gerichte, grootschalige of bulkinterceptie, die van een heel andere orde is dan de gerichte interceptie van artikel 32 (zie nader par. 8.3.1). De wetgever zou te allen tijde verhullend taalgebruik in de wet moeten vermijden, zowel vanuit het oogpunt van voorzienbaarheid bij wet als vanuit het belang van zorgvuldige wetgeving.

In de Memorie van Toelichting zijn daarnaast voorbeelden te vinden die vergelijkbaar zijn met verhullend taalgebruik, in de zin dat ze een verkeerde indruk (kunnen) wekken. Opvallend is dat waar de toelichting beoogt te illustreren hoe de diensten een bepaalde bevoegdheid kunnen inzetten, voorbeelden worden gebruikt van 20$^{e}$-eeuwse technologie in plaats van eigentijdse voorbeelden. Zo wordt bij observatie verwezen naar verrekijkers en foto- en videocamera’s. Nu zullen de diensten ongetwijfeld nog steeds wel eens een verrekijker gebruiken, maar de beperking van de toelichting tot dergelijke oude technologie is misleidend in een tijdperk waarin de diensten technieken als microdrones, WiFi-tracking en gezichtsherkenning kunnen gebruiken (zie nader par. 7.1.4). Meer in het algemeen valt op dat in de Memorie van Toelichting enige vorm van visie ontbreekt op grootschalige technologische ontwikkelingen die de komende decennia hun beslag krijgen, zoals het Internet der Dingen, Big Data Analytics, profilering, machinaal leren, drones en gezichtsherkenning. Daarmee verhult de toelichting de uitwerking die de algemeen omschreven bevoegdheden zullen gaan krijgen naarmate deze – voorzienbare – technologische ontwikkelingen steeds meer vorm gaan krijgen. Mogelijk is dit geen bewuste keuze voor verhullend taalgebruik in de MvT geweest, maar het resultaat is wel dat de burger niet de voorzienbaarheid bij wet wordt geboden die, juist bij technologie-neutraal geformuleerde bevoegdheden, nodig is om de ingrijpende privacyinbreuken te rechtvaardigen.

### *2.3.3 Een complexe wet en spaghetticonstructies*

Met in totaal 151 artikelen bevat de Wiv 20xx bijna de helft meer artikelen dan de Wiv 2002 (106 artikelen). Dit is niet alleen een gevolg van uitbreiding van bevoegdheden, maar ook van nadere en specifiekere wettelijke regeling van de taakuitvoering van de diensten. Een specifiekere regeling komt de rechtszekerheid en kenbaarheid van de wet ten goede. Maar de uitgebreidheid van de wet maakt deze ook minder overzienbaar. Het voorstel betreft een complexe wet, niet alleen door de complexiteit van de materie, maar ook door de structuur van de wet die niet altijd helder is. Met name is het normeringskader voor de inzet van bevoegdheden weinig overzichtelijk, doordat onderdelen hiervan uiteen zijn getrokken (art. 17-21, 23-24, 43-45, 57) en onderscheid wordt gemaakt tussen een 'algemene' bevoegdheid en 'bijzondere' bevoegdheden waarbij de eerste minder genormeerd is. Los van het feit dat dit laatste inhoudelijk moeilijk te begrijpen is (par. 5.1), verhoogt deze keuze ook de onduidelijkheid van de structuur. Ook bevat het normeringskader twee typen regels: voor de omgang met (persoons)gegevens en voor de inzet van bevoegdheden. Dat schept verwarring omdat hierdoor de vraag kan rijzen of belangrijke en generieke waarborgen, zoals subsidiariteit en proportionaliteit, alleen onder het laatste vallen of ook (impliciet) onder het eerste (zie par. 4.1.3).

Door de uitgebreidheid en niet al te heldere structuur van de wet ontstaat hierdoor een risico dat in de discussie over het wetsontwerp niet altijd duidelijk is aan welke waarborgen bepaalde activiteiten van de diensten moeten voldoen. Wij bevelen daarom aan de algemene normerende onderdelen uit het wetsontwerp bij elkaar te plaatsen in één normeringskader en, voor zover mogelijk, van toepassing te laten zijn op alle activiteiten van de diensten die inbreuk kunnen maken op grondrechten.

Naast de structuur van de wet vraagt ook een wetgevingstechniek aandacht. Het wetsontwerp bevat vele kruisverwijzingen, waardoor de reikwijdte van de regels moeilijk te overzien valt. Nu is kruisverwijzing – waarbij een regel uit een andere bepaling van toepassing wordt verklaard – een veelgebruikte wetgevingstechniek, en een nuttig hulpmiddel om wetgeving kort en daardoor overzichtelijker te houden; het voorkomt nodeloze herhaling. Het nadeel is echter dat de regel elders opgezocht moet worden en de inhoud niet in één oogopslag in samenhang met het verwijzende artikel te overzien valt, wat juist ten koste gaat van de overzichtelijkheid in de zin van begrijpelijkheid van wat een bepaling inhoudt. De wetgever moet in het algemeen dan ook zorgvuldig omgaan met kruisverwijzingen.

Het risico van onoverzichtelijke wetgeving wordt echter veel groter wanneer de bepaling waarnaar doorverwezen wordt zelf ook weer kruisverwijzingen kent. Dan ontstaan spaghetticonstructies, waarbij een sliert aan verwijzingen door de kluwen van de wet gevolgd moet worden om de volledige reikwijdte te kunnen bevatten. Een pregnant voorbeeld daarvan is artikel 77 (verstrekking van gegevens aan buitenlandse diensten), dat in lid 3 verwijst naar (onder andere) artikel 55 (verstrekking van onbetrouwbare of oude gegevens), dat in lid 2 een uitzondering schept voor instanties genoemd in artikel 49 lid 1 onder d (dat wil zeggen buitenlandse diensten), waarbij op basis van artikel 55 lid 4 artikel 54 lid 3 van overeenkomstige toepassing is (inzagerecht in achterliggende gegevens), waarbij dan wel weer artikelen 124 en 125 leden 2-3 (geheimhouding en getuigenplicht) van overeenkomstige toepassing zijn, die weer samenhangen met de in deze artikelen vermelde strafrechtelijke artikelen. De spaghettisliert houdt hier nog niet op, maar is inmiddels tamelijk onzinnig geworden omdat nauwelijks nog te

interpreteren valt hoe de uitzondering op de geheimhoudingsplicht bij het optreden als getuige met ontheffing van Onze betrokken Minister en de Minister van V&J (125 lid 2) ‘van overeenkomstige toepassing’ is op buitenlandse agenten aan wie inzage is geboden in achterliggende gegevens in het kader van internationale samenwerking. Er zitten meer van dergelijke spaghettislierten in het wetsontwerp, niet alle even lang, maar vaak wel moeilijk te overzien zonder nauwkeurige en diepgravende analyse om de kluwen te ontwarren. Dat is misschien nog te doen voor gespecialiseerde juristen die problemen moeten oplossen bij de interpretatie van de wet, maar in het wetgevingstraject zal de reikwijdte van bepalingen in lang niet alle gevallen voldoende duidelijk zijn. Het zal duidelijk zijn dat dit een risico oplevert voor privacybescherming, omdat de reikwijdte van wat de diensten mogen doen via combinaties van bepalingen vaak onvoldoende in beeld zal zijn bij degenen die over het wetsvoorstel beslissen.

Kruisverwijzingen hoeven als zodanig niet geheel vermeden te worden, maar spaghettiwetgeving wel. Onderdelen die wezenlijk zijn voor het begrip van de reikwijdte van een artikel moeten bij voorkeur in het artikel zelf worden opgenomen (liever herhaling dan het risico van verwarring) en, waar herhaalde doorverwijzingen toch onvermijdelijk zijn, moeten deze spaghettislierten steeds expliciet in de toelichting worden benoemd en uitgelegd.

# 3 Taakstelling en samenwerking tussen de diensten

## 3.1 Taakstelling en het begrip ‘nationale veiligheid’

De taakstelling van de AIVD en de MIVD is geregeld in de artikelen 8 en 9 (AIVD) en 10 en 11 (MIVD). De artikelen 9 en 11 zijn gelijk aan de huidige artikelen 6a en 7a, die in 2006 aan de Wiv zijn toegevoegd. Zij regelen de inzet van de AIVD en de MIVD waar het gaat om het opstellen van dreigings- en risicoanalyses. Voor dit rapport is vooral de algemene taakstelling van artikelen 8 en 10 relevant.

De taakstelling van de AIVD en de MIVD wordt in het spraakgebruik vaak onderscheiden naar het sub-lid waaronder de taken genoemd zijn. De zogenoemde ‘a’-taak van de AIVD verwijst naar artikel 8, lid 2 sub a. Voor de MIVD is dit artikel 10 lid 2 sub a. Op vergelijkbare wijze is sprake van een ‘b’-taak, etc. De ‘a’- taak betreft het verrichten van onderzoek naar personen en organisaties die in woord en/of daad aanleiding geven ‘tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat’ (AIVD) dan wel naar ‘het potentieel en de strijdkrachten van andere mogendheden’ en onderzoek ‘naar factoren die van invloed zijn of kunnen zijn op de handhaving en bevordering van de internationale rechtsorde’ (MIVD). Daarnaast verricht de MIVD onderzoek dat zowel ondersteuning biedt bij een goede mobilisatie en concentratie van strijdkrachten als bij het voorkómen van acties gericht tegen de krijgsmacht (‘c’-taak). De invulling van deze en de overige in artikelen 8 en 10 genoemde taken wordt in de Wiv 20xx, evenals in de Wiv 2002, nader omschreven in de bijzondere bevoegdheden die de AIVD en de MIVD hebben voor het verrichten van onderzoek conform hun taakstelling. We bespreken deze bijzondere bevoegdheden in de volgende hoofdstukken.

Van belang hier is wel de vraag wat de materiële grondslag van de taken van de AIVD en de MIVD is. Die materiële grondslag is voornamelijk gelegen in het handhaven van de ‘nationale veiligheid’. In dit begrip is enerzijds de soevereiniteit van een land aangegeven maar is anderzijds een veelheid van dimensies te onderscheiden waar de nationale veiligheid zich manifesteert. In de Strategie Nationale Veiligheid wordt de nationale veiligheid getypeerd als zich strekkende over domeinen zoals territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, en sociale en politieke veiligheid,[18] wat een ruime interpretatie mogelijk maakt over wat tot nationale veiligheid gerekend zou moeten worden. In de MvT bij het wetsontwerp wordt geen enkele aanduiding gegeven wat het begrip ‘nationale veiligheid’ betekent, anders dan dat het ‘breed’ moet worden opgevat, p. 10, en dat het een ‘ruim begrip’ is. Daarmee laat het wetsontwerp nadrukkelijk de mogelijkheid open dat de taakuitoefening van de diensten zich over het brede scala van aspecten van nationale veiligheid, zoals genoemd in de Strategie Nationale Veiligheid, uitstrekt.

De impact op de privacy van personen kan bij een ruime interpretatie van het begrip nationale veiligheid groter en onverwachter zijn (een grotere groep mensen en instellingen kan op de radar van de AIVD of de MIVD terechtkomen), en het is

[18] Minister van V&J (2015), Voortgangsbrief nationale veiligheid. 12 mei 2015, p. 2.

daarom een relevante vraag of het stelsel van toegestane inbreuken op de privacy voldoende waarborgen biedt om te controleren of de inbreuken, ook bij aspecten die men in het algemeen minder snel met de klassieke invulling van het begrip nationale veiligheid zal associëren, zoals ecologische of economische veiligheid, noodzakelijk zijn in een democratische samenleving, en proportioneel in het licht van het beoogde doel terwijl er geen middelen voorhanden zijn om met een geringere inbreuk hetzelfde doel te realiseren. De toelaatbaarheid van een privacy-inbreuk zal afhangen van de inschatting van de impact die het niet-ingrijpen door de AIVD en de MIVD zou hebben op de nationale veiligheid; die inschatting kan anders uitpakken voor de verschillende dimensies van het begrip nationale veiligheid.[19] Dit is iets wat met name in het toezicht op de feitelijke uitoefening van de diensten steeds zal moeten worden beoordeeld. De toezichthouders zullen, met name bij het gebruik van de meest ingrijpende en de uitgebreide bevoegdheden in relatie tot doeleinden die minder snel met de klassieke invulling van het begrip nationale veiligheid worden geassocieerd, scherp moeten beoordelen of de uitoefening wel noodzakelijk is in een democratische samenleving voor dat specifieke doel.

In dat verband is de ook door anderen reeds gestelde vraag relevant of het begrip ‘nationale veiligheid’ niet in de wet gedefinieerd (dan wel anderszins nauw omschreven) zou moeten worden. Voor de privacybescherming zou een nauwe omschrijving waardevol kunnen zijn, omdat het bijdraagt aan de voorzienbaarheid bij wet en omdat het mogelijk de meer ‘perifere’ activiteiten van de diensten kan inperken. Tegelijkertijd kan een wettelijke omschrijving ook onwenselijke neveneffecten hebben voor de privacybescherming, bijvoorbeeld als een te nauwe omschrijving ertoe zou leiden dat de diensten bepaalde dreigingen zouden her-etiketteren onder wel toegestane doeleinden, zodat de voorzienbaarheid bij wet juist vermindert, of als een te ruime omschrijving de diensten juist meer ruimte zou geven voor privacyinbreuken. Wij volstaan hier met de constatering dat de Wiv 20xx in dit opzicht geen verandering biedt ten opzichte van de Wiv 2002, waar het begrip ‘nationale veiligheid’ evenmin is gedefinieerd (maar wel, in de woorden van de CTIVD, ‘breed’ moet worden opgevat, aldus MvT, p. 10, met verwijzingen), en dat het voor de privacybescherming het belangrijkste is dat er scherp toezicht plaatsvindt op de proportionaliteit en subsidiariteit van de feitelijke taakuitoefening van de diensten, steeds in verhouding tot het specifieke doel dat in een situatie wordt beoogd.

Daarbij tekenen wij wel aan dat de Memorie van Toelichting op het punt van de materiële grondslag van de taakuitoefening van de diensten mager is.[20] De MvT geeft slechts enkele voorbeelden van wat wel onder ‘nationale veiligheid’ wordt verstaan (spionage, staatsgeheimen, terrorisme, oproepen tot geweld, en voor de veiligheidsdienst schadelijke geschriften – dat zijn allemaal ‘duidelijke gevallen’ die in de kern liggen van het begrip) en één voorbeeld van wat er niet onder wordt verstaan (opsporing van strafbare feiten), maar dit laat een groot grijs gebied open, terwijl juist in de twijfelgevallen (zoals economische spionage, ecologische

[19] Ter illustratie: het is niet denkbeeldig dat het handhaven van ecologische veiligheid – bijvoorbeeld het voorkomen van giflozingen – een andere noodzakelijkheid (subsidiariteit en proportionaliteit) met betrekking tot toegestane inbreuken op de privacy van personen met zich meebrengt dan het handhaven van fysieke veiligheid – bijvoorbeeld het voorkomen van een bomaanslag.

[20] De uitleg van het begrip ‘nationale veiligheid’ is beperkt tot enkele opmerkingen in het kader van de voorgestelde nieuwe bevoegdheid tot naslag (MvT, pp. 10-11) en tien regels tekst in de paragraaf over mensenrechten (p. 176).

veiligheid of financiële stabiliteit van het land) behoefte is aan kenbaarheid of deze wel of niet onder de taakstelling van de diensten vallen. Daarom zou het begrip ‘nationale veiligheid’, zo niet in een wettelijke definitie, ten minste in de toelichting duidelijker moeten worden uitgelegd, zodat de burger weet wat de wetgever daaronder verstaat.

## 3.2 Samenwerking tussen de diensten

Hoofdstuk 6 van de Wiv 20xx handelt over vormen en aard van samenwerking, tussen de AIVD en de MIVD en van de diensten met derden. Hoewel de samenwerking met derden binnen Nederland, bijvoorbeeld in samenwerkingsverbanden als de Contra-Terrorisme Infobox (een samenwerkingsverband onder het beheer van de AIVD waarin informatie wordt gedeeld tussen diverse overheidsinstanties), ook met privacyrisico’s gepaard gaan, laten we die vanwege de beperkingen in onderzoekscapaciteit in dit rapport buiten beschouwing – niet omdat ze niet belangrijk zijn, maar omdat ze een gedetailleerde analyse vergen van de vormen van gegevensdeling en technische ondersteuning die binnen dergelijke samenwerkingen mogelijk zijn, wat een studie op zich vormt.[21] De samenwerking met buitenlandse diensten analyseren we bij de informationele privacy (par. 5.4). Hier beperken we ons hier tot de samenwerking tussen de diensten onderling.

In de evaluatie van de commissie-Dessens pleit deze voor intensievere samenwerking, ‘waarbij met behoud van de eigenheid van de diensten (geleidelijk) wordt toegegroeid naar een intrinsieke, diepgaande samenwerking, waarbij zoveel mogelijk vanuit een gezamenlijke visie en planvorming voor de komende tien jaar wordt gewerkt.’[22] Voor een deel komt deze aanbeveling voort uit de behoefte om zo efficiënt mogelijk met beschikbare middelen om te gaan, en voor een deel is deze gebaseerd op de noodzaak te voorkomen dat de diensten verschillende signalen afgeven, bijvoorbeeld bij de inlichtingentaak buitenland.[23] Daaronder valt ook een verandering van de wettelijke grondslag van de plicht om elkaar zoveel mogelijk medewerking te verlenen naar een wettelijke grondslag van de plicht om zoveel mogelijk samen te werken.[24]

Het wetsvoorstel neemt verschillende van de aanbevelingen van de evaluatiecommissie over. In hoofdstuk 6 van het wetsontwerp komt het sterkere ‘werken zoveel mogelijk samen’ (art. 74 lid 1) in de plaats van het huidige ‘verlenen elkaar zoveel mogelijk medewerking’. De samenwerking bestaat in elk geval uit het delen van gegevens en technische en andere vormen van ondersteuning (art. 74 lid

[21] Wel kunnen we hier opmerken dat onderdelen van onze analyse ook relevant zijn voor de regeling van samenwerking en gegevensuitwisseling met andere instanties in Nederland. De analyse van de privacyrisico’s van gegevensopvraging op basis van de ‘algemene’ bevoegdheid (par. 5.1) is mutatis mutandis van belang voor de artikel 79-ambtenaren (de huidige artikel 60-ambtenaren die in de Wiv 2002 een informatieverplichting hebben jegens de diensten) die in het wetsontwerp worden uitgebreid. Daarbij zijn vooral ook de kritische opmerkingen in par. 5.1.3 belangrijk, nu art. 82 lid 2 aangeeft dat ook sprake kan zijn van toelevering van gegevens op rechtstreeks geautomatiseerde wijze. De toelichting bij dat voorstel (p. 149) miskent evenals de toelichting bij geautomatiseerde toegang tot databestanden van derden op basis van artikel 22 lid 3, de grote privacyrisico’s van deze vorm van gegevens delen.

[22] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p. 114.

[23] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p. 111 en volgende.

[24] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p. 113-114.

2). Als het verzoek tot ondersteuning de inzet van bijzondere bevoegdheden betreft, is daarvoor toestemming van de minister nodig (lid 3). Het nieuwe lid 4 van artikel 74 creëert de mogelijkheid tot het instellen van gezamenlijke werkverbanden; als binnen dergelijke verbanden de inzet van bijzondere bevoegdheden bij ministeriële regeling geregeld wordt, vervalt de toestemmingseis van lid 3. De Memorie van Toelichting geeft aan dat dit ruimte biedt om een samenwerkingsverband als de Joint Sigint Cyber Unit (JSCU) onder de werking van de Wiv 20xx te plaatsen en daarmee van een – mogelijk gewenste – wettelijke grondslag te voorzien (MvT, p. 133-134).

Artikel 75 bevat voorts een zorgplicht voor de diensten tot het intensiever informeren van de andere dienst over voorgenomen operationele activiteiten die naar verwachting van invloed kunnen zijn op een goede taakuitvoering van de andere dienst (‘need to share’). Ook hier staat de wetgever ‘een intensieve taakoverstijgende samenwerking’ voor ogen, ‘waarbij afstemming “aan de voorkant” centraal staat (…,). Maximale onderlinge voorafgaande afstemming staat daarbij voorop’ (MvT, p. 134-5). Dit vervangt de huidige zogenoemde ‘deconflictieregeling’, die inhoudt in dat onder de Wiv 2002 de MIVD handelt in overeenstemming met de minister van BZK bij het doen van onderzoek of inzetten van bevoegdheden in het civiele domein (zie art. 20 lid 2, 22 lid 2 en 4, 23 lid 3, 24 lid 3, 25 lid 3 en 5, 27 lid 8 en 28 lid 5 Wiv 2002); dit teneinde interferentie tussen de diensten te voorkomen.

De privacyrisico’s van deze intensievere samenwerking zijn moeilijk in algemene zin aan te geven. Aan de ene kant levert intensievere uitwisseling van gegevens een grotere privacyinbreuk op – de diensten zullen immers vaker en meer gegevens delen, en hoogstwaarschijnlijk dus ook meer gegevens verwerken dan nu gebeurt. Aan de andere kant kan het delen van gegevens de mogelijke privacyinbreuk ook verkleinen, omdat betere samenwerking kan voorkomen dat twee keer gepoogd wordt dezelfde gegevens te vergaren. Het delen van gegevens kan voorkomen dat de ene dienst een bevoegdheid inzet (met navenante privacyinbreuk en mogelijke bijvangst) terwijl de andere dienst de gegevens beschikbaar heeft. Ook kan het delen van gegevens enerzijds leiden tot betere kwaliteit van gegevens, wanneer gegevens in hun totaliteit beter kunnen worden gewaardeerd en beoordeeld doordat meer context en analyse beschikbaar is, maar anderzijds ook leiden tot verkeerde interpretaties omdat gegevens ook buiten hun oorspronkelijke context terechtkomen en daarmee een andere kleuring kunnen krijgen. In het algemeen kan men daarom moeilijk zeggen of de privacyrisico’s door de intensievere samenwerking duidelijk zullen toenemen.

Wat echter wel vastgesteld kan worden is dat het delen van gegevens (te) weinig normering kent. Alleen de algemene bepalingen (art. 17-21) en de vernietigingsplicht (art. 57) zijn van toepassing, maar niet de algemene bepalingen betreffende bijzondere bevoegdheden (art. 23-24) evenmin als het afwegingskader (art. 43-44). Het delen van gegevens op basis van artikel 74 lid 2 is immers geen bevoegdheid. De MvT zegt hier verder niets over. Dat is opmerkelijk, omdat het betekent dat enkele beginselen van persoonsgegevensverwerking hier niet van toepassing lijken te zijn. Nu de eisen van subsidiariteit en proportionaliteit in het wetsontwerp niet gecodificeerd worden in de algemene bepalingen maar in artikelen 43 en 44, is het de vraag of de diensten in dit geval wel voldoende gebonden zijn aan subsidiariteit en proportionaliteit. Het zou kunnen impliceren dat de diensten ook gegevens mogen, of wellicht zelfs moeten, delen, als dat voor het doel van het delen niet proportioneel is, of als hetzelfde doel met een simpel

telefoontje met een algemene inlichting ook zou kunnen worden bereikt. Het kan volgens ons niet de bedoeling zijn dat de gegevensuitwisseling tussen de diensten op deze manier zou worden gemaximaliseerd (zoveel mogelijk gegevens delen, ook als het niet nodig is) in plaats van geoptimaliseerd (gegevens delen waar dat nuttig is en geen onevenredige neveneffecten heeft). De eisen van subsidiariteit en proportionaliteit uit het afwegingskader zouden dan ook expliciet van toepassing moeten worden verklaard op artikel 74, door deze duidelijker op te nemen in het algemene kader van artikel 17 (zie par. 4.1.3).

Daarnaast bestaat er geen duidelijke eis van doelbinding. In het algemeen is doelbinding vervat in de algemene bepaling van artikel 17 lid 2 (zie par. 4.1.2), omdat deze bepaling aangeeft dat gegevens slechts voor een bepaald doel mogen worden verwerkt, en normaliter zal dat het doel betreffen waarvoor de gegevens zijn vergaard, veelal met inzet van een bevoegdheid. De verstrekking aan de andere dienst van gegevens kan datzelfde doel dienen (bijvoorbeeld een onderzoek naar een specifieke terroristische dreiging), maar het kan evengoed een ander doel dienen, als de gegevens in enig opzicht nuttig worden geacht voor de andere dienst. In dat geval mag de ontvangende dienst de gegevens alleen gebruiken voor ‘een bepaald doel’, maar dat doel kan dus een ander doel zijn, waarvan het maar de vraag is of dat doel verenigbaar is met het oorspronkelijke doel waarvoor de verstrekkende dienst die gegevens had verzameld. Deze mogelijkheid van doelafwijkende verstrekking wordt nergens toegelicht of gemotiveerd in de Memorie van Toelichting. Dit levert een privacyrisico op, omdat doelafwijkende gegevensverstrekking eerder kan leiden tot interpretatiefouten, vanwege de nieuwe context waarbinnen de verstrekte gegevens gaan worden gebruikt. Ook hier lijkt zich het ontbreken van een duidelijk normeringskader voor de gegevensuitwisseling van artikel 77 lid 2 te wreken. Het verdient dan ook aanbeveling om, evenals een beoordeling op subsidiariteit en proportionaliteit, ook de doelbinding expliciet te betrekken bij de afweging om gegevens te verstrekken aan de collega-dienst.

Daarbij is een afwijkend doel niet uitgesloten, maar dat vergt dan wel een afweging of het doelafwijkend gebruik gerechtvaardigd is, omdat hiervoor een nieuwe grondslag nodig is. Doelafwijkende verstrekkingen hebben daarom de toestemming nodig op ten minste hetzelfde niveau als de toestemming die nodig was voor het verkrijgen van de gegevens door de verstrekkende dienst.

# 4 Algemene bepalingen

In dit hoofdstuk wordt aandacht besteed aan de algemene bepalingen over het verwerken van (persoons)gegevens door de inlichtingen- en veiligheidsdiensten (art. 17-21, 57) en de algemene bepalingen die gelden voor bijzondere bevoegdheden (art. 23-24, 43-45).

Conform de jurisprudentie van het EHRM raakt het verzamelen van informatie door autoriteiten over burgers zonder hun toestemming altijd hun privéleven en valt het daarmee binnen de bescherming van artikel 8 EVRM. Met name in de jurisprudentie van het EHRM met betrekking tot artikel 8 EVRM is waar het gaat om (vormen van) '*secret measures of surveillance*' een daarop toegespitst normenkader ontwikkeld. Dit betreft waarborgen die niet uitsluitend de (uitoefening van de) bevoegdheden raken, maar ook zien op andere aspecten verbonden aan de (verdere) verwerking van de met de bijzondere bevoegdheden verzamelde gegevens.

In de zaak Weber en Saravia tegen Duitsland, heeft het EHRM een aantal minimumwaarborgen geformuleerd waar het gaat om de zwaarste inbreuken op het door artikel 8 EVRM gegarandeerde recht op privacy. Het betreft hier de volgende minimumwaarborgen die in wetgeving (*statute law*) moeten zijn uitgewerkt om misbruik van (de interceptie)bevoegdheid te voorkomen:[25]

'a. de aard van de gedragingen die tot een interceptiebevel kunnen leiden;
b. de categorieën van personen van wie communicatie kan worden onderschept;
c. een beperking van de duur van de interceptie;
d. de procedure die gevolgd moet worden voor het onderzoeken, gebruiken en opslaan van de verkregen gegevens;
e. de voorzorgsmaatregelen die moeten worden getroffen als de gegevens met derden worden gedeeld;
f. de omstandigheden waaronder gegevens moeten worden gewist of opnamen vernietigd.'

Mutatis mutandis kunnen deze eisen ook worden geacht te gelden voor veiligheidsdiensten (al kan daarbij de interpretatie wanneer aan een eis is voldaan enigszins anders uitvallen dan bij opsporing van strafbare feiten, afhankelijk van de context) en ook voor andere ingrijpende bevoegdheden. Voor een deel zullen deze eisen tot uitdrukking moeten komen in de regeling van specifieke bevoegdheden, zoals interceptie, maar deels zullen zij ook naar voren moeten komen uit het algemene kader voor de omgang met persoonsgegevens.

De algemene bepalingen omvatten drie onderdelen. Ten eerste bevatten artikelen 17 tot en met 21 algemene bepalingen voor gegevensverwerking door de diensten. Onder gegevens worden zowel persoonsgegevens als andere gegevens verstaan; voor dit rapport zijn persoonsgegevens van belang – een begrip dat overigens zo ruim is dat tegenwoordig de meeste gegevens daaronder vallen, aangezien vrijwel alle gegevens (in combinatie met andere gegevens) door iemand (en zeker door de diensten) uiteindelijk herleid kunnen worden tot identificeerbare personen. In dit verband gaan we hieronder in paragrafen 4.1 tot en met 4.3 in op de algemene

[25] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §95 (onze vertaling).

eisen (art. 17), de categorie personen (art. 18) en de zorgplicht om voorzieningen te treffen (art. 21). De verwerking van gegevens door ambtenaren ten behoeve van de AIVD en MIVD (art. 19) en de geheimhoudingsplicht (art. 20) laten we vanwege de beperkingen van dit onderzoek buiten beschouwing.

Ten tweede bevatten artikelen 23 en 24 algemene bepalingen voor de uitoefening van bijzondere bevoegdheden (die dus niet gelden voor de 'algemene' bevoegdheid); deze bespreken we in paragraaf 4.4. Ten derde worden deze algemene bepalingen aangevuld met een 'afwegingskader' en een bepaling over verslaglegging (art. 43-45), die eveneens beperkt zijn tot de bijzondere bevoegdheden (par. 4.5). Wat echter ontbreekt, is een algemene bepaling over bewaartermijnen en een onderzoeksplicht gerelateerd aan de vernietigingsplicht (par. 4.6).

## 4.1 Algemene eisen voor gegevensverwerking

### *4.1.1 Inleiding*

In paragraaf 3.1 van het wetsvoorstel worden de algemene regels met betrekking tot de verwerking van gegevens door de diensten vastgelegd. In artikel 17 (ongewijzigd ten opzichte van art. 12 Wiv 2002) zijn enkele algemene regels vastgelegd over de verwerking van gegevens.

Artikel 17

1. De diensten zijn bevoegd tot het verwerken van gegevens met inachtneming van de eisen die daaraan bij of krachtens deze wet of de Wet veiligheidsonderzoeken zijn gesteld.
2. De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken.
3. De verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze.
4. De gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt, zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend.

De algemene eisen omvatten enkele van de algemene principes van bescherming van persoonsgegevens. Lid 1 biedt een algemene wettelijke grondslag voor de verwerking van persoonsgegevens. Lid 2 formuleert het principe van doelbinding door vast te stellen dat verwerking alleen toegestaan is voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van de Wiv 20xx. Ook moeten de verwerkingen voorzienbaar zijn bij wet, zoals in lid 3 vastgesteld door overeenstemming met de wet te vereisen. Vervolgens zijn in lid 3 en lid 4 nog enkele eisen opgenomen om de kwaliteit van de gegevens die verwerkt worden te waarborgen. De verwerking zelf dient op behoorlijke en zorgvuldige wijze plaats te vinden (lid 3), waarmee in beginsel een blijvende kwaliteit gewaarborgd zou moeten worden. In lid 4 wordt vastgesteld dat de gegevens voorzien dienen te zijn van een aanduiding van de betrouwbaarheid van een gegeven of van een verwijzing naar het document of de bron van de gegevens.

### *4.1.2 Doelbinding*

De activiteiten van de diensten moeten altijd aan een specifiek doel verbonden zijn en ook noodzakelijk zijn voor het bereiken van dat doel (lid 2 van artikel 17). Het doel op zich dient weer noodzakelijk te zijn voor een goede uitvoering van de wet of van de Wet veiligheidsonderzoeken. Doelbinding is een waarborg voor de privacy, waarmee voorkomen wordt dat gegevens steeds verder verwerkt mogen worden zonder toetsing of die verwerking wel past bij, en dus voorzienbaar was bij, de verkrijging van de gegevens. Doelen moeten vooraf zo specifiek mogelijk vastgesteld worden, waardoor de reden van verwerking ook vastligt. Bovendien kan aan de hand van het te bereiken doel beoordeeld worden of de te verwerken gegevens inderdaad noodzakelijk zijn om dat doel te bereiken. Andersom kan vanuit het doel bekeken worden welke persoonsgegevens noodzakelijkerwijs verwerkt dienen te worden.

Het vereiste van doelbinding leidt dus tot een limitering van de te verwerken gegevens en de verwerkingen die uitgevoerd worden ten aanzien van die gegevens. In vergelijkbare zin kan vanuit het doel ook een beperking afgeleid worden ten aanzien van welke personen gegevens verwerkt worden. Het verwerken van gegevens over personen die niet de aandacht van de diensten hebben in relatie tot het specifieke doel moet dan ook voorkomen worden. Wanneer dat voorkomen niet mogelijk is, bijvoorbeeld omdat gegevens niet afzonderlijk van andere gegevens verwerkt kunnen worden, dienen gegevens over personen die niet de aandacht hebben zo spoedig mogelijk te worden vernietigd om verdere verwerking te voorkomen.

Uit gesprekken met de diensten blijkt ook dat zij uitgaan van een sterke doelbinding in hun activiteiten. Vooral ten aanzien van de bijzondere bevoegdheden is doelbinding een gegeven, aangezien de diensten het doel en de noodzaak in het verzoek tot een last van de minister moeten verantwoorden. Aangezien doelbinding een limitering voorschrijft, is het met name in het geval van grootschalige gegevensverwerking van belang om zo spoedig mogelijk tot een beperking te komen. Dat betekent dat de inzet van bulkinterceptiebevoegdheden bijzondere aandacht verdient in het licht van het doelbindingsvereiste (zie par. 8.3.2). Met een goede naleving van dit vereiste, ook en vooral bij de bevoegdheden die minder precies gericht zijn op onderzoekssubjecten, wordt de inbreuk op de persoonlijke levenssfeer van met name personen die niet de aandacht van de diensten (zouden moeten) hebben, zo beperkt mogelijk gehouden.

### *4.1.3 Subsidiariteit en proportionaliteit*

In het begrip ‘noodzakelijk’ in lid 2 zit, naar wij aannemen, ook de eis dat persoonsgegevensverwerking moet voldoen aan de eisen van subsidiariteit en proportionaliteit. Als iets niet subsidiair is (er is een minder ingrijpend middel voorhanden), is het immers niet noodzakelijk; en als iets niet proportioneel is (het middel staat niet in verhouding tot het doel), is het evenmin noodzakelijk. Het wetsontwerp schept echter enige verwarring door de beginselen van subsidiariteit en proportionaliteit te codificeren in artikel 43 (leden 2-4), dat van toepassing is op de uitoefening van bijzondere bevoegdheden, maar niet op andere vormen van gegevensverwerking door de diensten.[26] Daaruit zou men kunnen afleiden dat—nu

[26] Hoewel leden 3 en 4, anders dan leden 1 en 2, van art. 43 in de formulering niet beperkt zijn tot bevoegdheden ‘als bedoeld in paragraaf 3.2.2’ (en daarmee a contrario van toepassing lijken op alle handelingen van de diensten die als bevoegdheid zijn geformuleerd, ook buiten par. 3.2.2), is

de beginselen wel expliciet van toepassing worden verklaard op bijzondere bevoegdheden—ze niet zijn inbegrepen in het begrip ‘noodzakelijk’ van artikel 17 lid 2. Dat kan echter niet de bedoeling van de wetgever zijn, omdat het dermate algemene beginselen betreft dat deze al het handelen van de diensten moeten normeren. Ook privacyinbreuken door andere vormen van gegevensverwerking dan de inzet van bijzondere bevoegdheden, bijvoorbeeld geautomatiseerde data-analyse (art. 47) of gegevensverstrekkingen (art. 74, 77), vallen immers onder artikel 8 EVRM en daarmee onder de vereisten van subsidiariteit en proportionaliteit. Uit de toelichting (MvT, p. 21) blijkt echter niet expliciet dat (ondanks de expliciete vermelding van de beginselen van subsidiariteit en proportionaliteit in artikel 43) artikel 17 lid 2, door het begrip ‘noodzakelijk’, *eveneens* deze beginselen omvat. De toelichting zou op dit punt moeten worden verhelderd.

#### *4.1.4 Betrouwbaarheids- en bronaanduiding*

Artikel 17 lid 4 vereist een aanduiding van de betrouwbaarheid van een gegeven of van de bron van de gegevens. Dit vereiste dient als een waarborg voor de kwaliteit van gegevens die door de diensten worden gebruikt in het kader van hun taakuitvoering. De MvT voegt hieraan toe: ‘Gelet op het gebruik [dat] van deze gegevens kan worden gemaakt – bijvoorbeeld als basis voor een mededeling als bedoeld in artikel 49 jo. 54 van het wetsvoorstel) – en de gevolgen die dat kan hebben voor personen of organisaties waarop die gegevens betrekking hebben, is het van belang dat expliciet wordt vastgesteld wat de kwaliteit van die gegevens is.’ (p. 21). Dit is dus vooral ook belangrijk vanwege de grote gevolgen die personen of organisaties kunnen ondervinden als gevolg van de verstrekking van de gegevens door de diensten aan derden.

Met het toevoegen van een betrouwbaarheidsaanduiding of verwijzing naar de bron wordt in zekere zin een waarborg ingebracht dat de gegevens zorgvuldig kunnen worden gewogen op betrouwbaarheid. Als het goed is zou dat ook houvast moeten geven voor beoordeling van de betrouwbaarheid van afgeleide gegevens die bijvoorbeeld volgen uit nadere analyse of samenvoeging van de oorspronkelijke gegevens. Bij de inzet van bepaalde technologieën, zoals *data mining*, valt echter te bezien of een aanduiding van de oorspronkelijke betrouwbaarheid een voldoende waarborg biedt tegen foute interpretaties. Bij het samenvoegen van verschillende gegevensbestanden ontstaat immers een vermenging van bronnen waarbij gegevens in een ander licht kunnen komen te staan en uit hun context kunnen worden getrokken, terwijl ook verschillen tussen de oorspronkelijke bestanden, die wellicht niet allemaal even betrouwbaar zijn, van invloed kunnen zijn op de inschatting van de betrouwbaarheid van het resultaat. Dat kan tot gevolg hebben dat gegevens betrouwbaarder worden, maar ook minder betrouwbaar of meer vatbaar voor misinterpretatie. Afhankelijk van het type analyse ontstaan nieuwe of andersoortige gegevens waarvan de betrouwbaarheid of de bron daarom niet altijd eenduidig is vast te stellen. Ook zorgvuldige verwerkingen van gegevens met bronaanduiding met behulp van geavanceerde algoritmes zijn om die reden geen garantie voor een hoog betrouwbaarheidsniveau van uitkomsten van analyses. Naast de bronaanduiding zou daarom verplicht gedocumenteerd moeten worden welke analysemethoden zijn gebruikt, inclusief een aanduiding van de betrouwbaarheid van deze methoden. In dat licht valt aan te bevelen dat artikel 17

---

artikel 43 onderdeel van paragraaf 3.2.2 en zal vanuit systematisch oogpunt de reikwijdte daartoe ook beperkt zijn.

niet alleen verplicht tot betrouwbaarheids- of bronaanduiding van gegevens zelf, maar daarnaast ook een verplichting bevat tot betrouwbaarheidsaanduiding van de programmatuur waarmee deze gegevensverzamelingen worden geanalyseerd. Een betrouwbaarheidsaanduiding van analysesoftware kan worden gebaseerd op softwareverificatie, toetsing van de vooronderstellingen die aan de programmatuur ten grondslag liggen, de verhouding tussen fout-positieven en fout-negatieven bij *data mining*, en het testen van algoritmes voor machinaal leren.

Ook als analyseprogramma's en gebruikte gegevenssets (relatief) betrouwbaar zijn, moeten de resultaten nog steeds geverifieerd worden door analisten alvorens op grond daarvan beslissingen kunnen worden genomen die personen raken. Er kunnen immers altijd fout-positieven optreden. Daarmee wordt gevolg gegeven aan het principe dat personen niet aan volledig geautomatiseerde beslissingen mogen worden onderworpen indien daar rechtsgevolgen of een significante impact aan verbonden zijn voor die personen (zie ook par. 5.3.3).

## 4.2 Categorie personen

### *4.2.1 Inleiding*

Artikel 18 geeft in de eerste plaats een afbakening van de kring van personen over wie gegevens verwerkt mogen worden. Daarnaast is een regeling opgenomen over de verwerking van gevoelige persoonsgegevens. De MvT spreekt over 'gevoelige persoonsgegevens', waar de Wet bescherming persoonsgegevens (Wbp) hiervoor de term 'bijzondere persoonsgegevens' gebruikt. 'Gevoelig' sluit echter eerder aan op het algemene spraakgebruik en omschrijft ook beter de categorie van gegevens.

Lid 3 stelt een verbod op de verwerking van gegevens betreffende godsdienst of levensovertuiging, ras, gezondheid en seksuele leven. Politieke gezindheid (in de Wbp ook als bijzonder gegeven aangemerkt) ontbreekt, omdat dit vaak relevant zal zijn bij de beoordeling van een bedreiging van de rechtsorde (MvT, p. 22). Lid 4 geeft aan dat verwerking van gevoelige gegevens alleen is toegestaan indien het voor het doel van de verwerking onvermijdelijk is dat die gegevens verwerkt worden en in aanvulling op de verwerking van andere gegevens. Onvermijdelijk betekent volgens de MvT dat hier een zwaarwegender eis geldt dan het noodzakelijkheidscriterium uit artikel 17 lid 2 (p. 22).[27] Wat het criterium 'in aanvulling op' betekent, wordt in de MvT niet uitgelegd.

In artikel 18 lid 5 is toegevoegd (ten opzichte van het oude artikel 13): 'diensten zijn bevoegd tot verwerking van gegevens omtrent andere personen, indien gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden'. De MvT zegt hierover dat in veel gevallen in het verlengde van het verwerken van gegevens over bepaalde personen ook gegevens over andere personen verwerkt zullen worden. Voor zover er twijfel zou kunnen ontstaan over de geoorloofdheid van de verwerking van dergelijke persoonsgegevens omtrent andere personen (die in principe zou moeten volgen uit art. 18 lid 1 en 2) is ervoor gekozen om dit afzonderlijk te regelen. Dat komt volgens de MvT de rechtszekerheid ten goede.

[27] In het kader van de parlementaire behandeling van de Wiv 2002 werd als voorbeeld gegeven dat het onvermijdelijk zal zijn om bijvoorbeeld de godsdienstige of levensovertuiging van personen of organisaties vast te leggen in de gevallen dat antidemocratische, staatsgevaarlijke of antimilitaristische activiteiten worden ontplooid waarbij de daders hun godsdienstige overtuiging als motief aanvoeren voor hun activiteiten.

*4.2.2 Analyse en beschouwing*

In artikel 18 lid 1 en 2 zijn de personen met betrekking tot wie de diensten persoonsgegevens mogen verwerken limitatief opgesomd. De lijst van categorieën personen vertoont duidelijk een verband met de taakstellingen van de diensten.

Lid 3 van artikel 18 verbiedt de verwerking van gevoelige persoonsgegevens (een synoniem voor de term 'bijzondere persoonsgegevens' uit de Wbp). In de opsomming van categorieën gevoelige persoonsgegevens is politieke gezindheid niet opgenomen, omdat, zoals de MvT (p. 22) stelt, deze niet buiten beschouwing gelaten kan worden bij de beoordeling of iemand een gevaar vormt voor de democratische rechtsorde, de veiligheid of paraatheid van de Nederlandse krijgsmacht of voor andere in de wet genoemde gewichtige belangen. In de MvT (p. 22) wordt daarbij aangetekend dat uiteraard voldaan moet zijn aan het noodzakelijkheidsvereiste van de verwerking van dergelijke gegevens voor een goede uitvoering van de Wiv.

De MvT gaat echter niet in op andere categorieën die in de persoonsgegevenswetgeving ook als 'bijzonder' (oftewel gevoelig) worden aangeduid: lidmaatschap van een vakvereniging en (kort gezegd) strafrechtelijke persoonsgegevens. Voor de laatste categorie kan een vergelijkbare redenering gelden als voor politieke gezindheid, aangezien strafrechtelijke persoonsgegevens (zoals veroordelingen) vaak direct relevant zijn voor de taakuitoefening van de diensten. Niettemin zou dit dan wel in de MvT gemotiveerd moeten worden.

Voor gegevens betreffende lidmaatschap van een vakvereniging valt echter niet direct in te zien waarom deze niet uitgesloten zouden moeten worden, behoudens onvermijdelijkheid, van verwerking door de diensten. Lidmaatschap van een vakbond heeft geen direct raakvlak met de nationale veiligheid, evenmin als levensovertuiging of gezondheid dat heeft. Voor de innerlijke consistentie van de privacybescherming in de Nederlandse wetgeving is het wenselijk dat eenzelfde invulling wordt gegeven aan het begrip 'bijzondere' oftewel gevoelige categorieën persoonsgegevens, tenzij de aard van een wet een andere invulling noodzakelijk maakt. In dat licht verdient de keuze om lidmaatschap van een vakvereniging niet te noemen in art. 18 lid 3 heroverweging.

In lid 4 is een uitzondering op het verbod uit lid 3 opgenomen. Indien het voor het doel van de gegevensverwerking onvermijdelijk is mogen de gegevens, in aanvulling op de verwerking van andere gegevens, wel verwerkt worden. Van een dergelijke onvermijdelijkheid zal, in lijn met het voorbeeld dat in de parlementaire behandeling van de Wiv 2002 werd gehanteerd, sprake zijn indien de gegevens onlosmakelijk verbonden zijn met een onderzoek dat de diensten uitvoeren in het kader van hun taakuitoefening, omdat de bedreiging rechtstreeks samenhangt met het gevoelige persoonskenmerk (zoals godsdienst of levensovertuiging). Het aanvoeren van een geloofsovertuiging als motief voor staatsgevaarlijke activiteiten betekent immers dat gegevens over die geloofsovertuiging onvermijdelijk (een zwaardere eis dan noodzakelijk) onderdeel van het onderzoek zullen vormen. Alleen in dergelijke gevallen mogen de gegevens in aanvulling op andere gegevens verwerkt worden. De gevoelige persoonsgegevens mogen dus nooit op zichzelf staand verwerkt worden, en ook nooit op zichzelf een grondslag vormen voor een beslissing.

De leden 3 en 4 stonden ook in de Wiv 2002. Veranderde technologische mogelijkheden kunnen echter de praktische betekenis van deze bepalingen wel beïnvloeden. Die beïnvloeding zit met name in het feit dat gevoelige persoonsgegevens steeds vaker onbedoeld kunnen worden gecreëerd door Big Data-toepassingen, wat vragen oproept of, en onder welke voorwaarden, dit 'onvermijdelijk' is. Wanneer met behulp van Big Data-toepassingen bepaalde correlaties worden vastgesteld waaruit automatisch een gevoelig persoonsgegeven ontstaat (bijvoorbeeld een profiel dat iemand een bepaalde godsdienst aanhangt), worden deze gevoelige gegevens niet in aanvulling op andere gegevens verzameld en verwerkt, maar in feite gecreëerd als gevolg van een verwerking. In hoeverre in dergelijke gevallen van onvermijdelijkheid gesproken kan worden, zou nader moeten worden uitgelegd in de MvT. Daarbij kan ook worden ingegaan op de mogelijkheid om technologisch dergelijke gegevens uit te filteren, zodat het niet onvermijdelijk is dat deze gegevens ontstaan. Alleen als het doel van een dergelijke Big Data-analyse gericht is op het verkrijgen van profielen die onvermijdelijk samenhangen met gevoelige persoonsgegevens, zou zo'n verwerking op basis van lid 4 toegestaan kunnen zijn, waarbij echter duidelijk is dat het onderzoek steeds ook gebaseerd moet zijn op andere aanwijzingen dat er sprake is van een relevante dreiging en dat een beslissing nooit op basis van enkel een dergelijk profiel mogen worden genomen.

In lid 5 wordt de bevoegdheid vastgesteld tot het verwerken van gegevens over andere personen indien deze een logisch en onlosmakelijk geheel vormen binnen een gegevensbestand. De vraag rijst wat de betekenis daarvan is in geval van gegevens die in bulk worden verzameld, zoals bij kabelgebonden bulkinterceptie. Strikt genomen zijn de personen over wie de diensten gegevens mogen verwerken limitatief vastgesteld middels de categorisering in respectievelijk lid 1 en 2 van artikel 18. Het inzetten van een bevoegdheid zal dus gericht moeten zijn op het verkrijgen of anderszins verwerken van gegevens over personen die binnen die limitatieve kring van categorieën vallen. Op het moment dat een bevoegdheid wordt ingezet en gegevens verwerkt worden, zal het in gevallen voorkomen dat noodzakelijkerwijs ook gegevens over andere personen worden verwerkt, indien deze gegevens een logisch en onlosmakelijk onderdeel van de te verwerken gegevens vormen.

Dat geldt met name bij bevoegdheden waarbij grote(re) hoeveelheden data tegelijk kunnen worden verzameld, zoals OSINT (wat onzes inziens ook als bevoegdheid zou moeten worden geregeld, zie par. 5.2), de 'algemene' bevoegdheid van gegevensopvraging, en bulkinterceptie. Bij dergelijke bevoegdheden kan vooraf niet vastgesteld worden welke van de te verzamelen gegevens uit een gegevensset betrekking hebben op personen die binnen artikel 18 lid 1 en 2 worden genoemd. Lid 5 biedt daarom een uitzondering op het beginsel dat alleen van relevante personen gegevens mogen verwerkt. Het gaat hier echter om zeer ruime bevoegdheden, die bovendien geen uitzonderingsbevoegdheden zijn, maar eerder tot de kernactiviteiten van de diensten lijken te behoren (in elk geval waar het OSINT en de 'algemene' bevoegdheid betreft). Dat betekent dat de situatie van lid 5 in dermate veel gevallen zal voorkomen, dat we hier niet meer kunnen spreken van een uitzondering maar eerder van een extra regel die de basisregel van lid 1 en 2 aanvult.

Dat is problematisch in het licht van de privacyrisico's voor de personen over wie (onvermijdelijk onterecht) gegevens worden verzameld. Het gaat immers om grote

groepen burgers. Daarnaast is het ook problematisch in het licht van *Weber en Saravia*, dat vereist dat de categorieën personen die onderworpen kunnen worden aan heimelijke gegevensverzameling moeten worden gedefinieerd. Het gaat bij art. 18 lid 5 j$^{o}$ art. 22 (met name lid 3) en art. 33 feitelijk om de categorie 'iedereen', omdat op basis van deze bevoegdheden over iedereen gegevens kunnen worden verzameld die in opgevraagde databestanden zitten of via bulk-onderschepte communicatiekanalen communiceren.

Tegelijkertijd kan niet worden ontkend dat het moeilijk is om de categorie personen nauwkeuriger te omschrijven dan in lid 5 gebeurt. Het gaat immers om gegevens over irrelevante personen die op geen enkele manier vooraf uitgefilterd kunnen worden, ook niet bij een zo gericht mogelijke inzet van bevoegdheden. (Daarbij gaan we er wel van uit dat lid 5, juist omdat het gaat om een aanvullende regel en niet een sporadische uitzondering, een sterk normerende werking zal moeten hebben op de diensten om de inzet van brede bevoegdheden, ook de 'ongerichte' interceptie, op voorhand zo gericht mogelijk te maken. De toezichthouder zal daarop ook scherp moeten toezien.)

Lid 5 levert daarmee nauwelijks voorzienbaarheid bij wet op, omdat het een categorie aanduidt: 'iedereen, afhankelijk van in welk databestand dat de diensten verzamelen je toevallig zit'. Omdat de voorzienbaarheid bij wet hier moeilijk te verbeteren valt door een scherpere definitie, moet dit gebrek worden gecompenseerd door andere maatregelen. Het is in het licht van de privacyrisico's van irrelevante personen wezenlijk dat de verzamelde gegevens zo snel mogelijk worden onderzocht en dat niet-relevante gegevens direct worden verwijderd. In dit opzicht schiet het wetsvoorstel te kort, omdat er lange bewaartermijnen worden gehanteerd en er veel te weinig wordt geëist dat niet-relevante gegevens terstond worden vernietigd (zie par. 4.6). Met name is in dit verband de driestappenregeling van bulkinterceptie problematisch, omdat de gegevens in het huidige systeem niet direct gefilterd hoeven te worden op relevantie; een benadering in twee fasen waarbij in fase 1 een directe, snelle en vluchtige toets op relevantie plaatsvindt en gegevens terstond worden verwijderd zodra niet-relevantie blijkt, verdient de voorkeur (zie par. 8.3.2) – juist ook ter compensatie van de problematisch ruime reikwijdte van art. 18 lid 5.

## 4.3 Technische en organisatorische voorzieningen

Artikel 21 bepaalt dat de hoofden van de diensten zorg dragen voor de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de gegevens die worden verwerkt (kwaliteitsvereiste), een adequate technische en organisatorische beveiliging van de gegevens, en de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens. Dit komt tegemoet aan de eis onder d van *Weber en Saravia*: 'the procedure to be followed for examining, using and storing the data obtained'.[28] De zorgplicht in artikel 21 komt volgens de MvT geheel overeen met hetgeen in het huidige artikel 16 is geregeld. Deze zorgverplichtingen zullen in de praktijk met name hun uitwerking moeten krijgen in concrete maatregelen op het vlak van de (inrichting van de) organisatie, het personeel en de invulling van de aan de gegevensverwerking gerelateerde werkprocessen (MvT, p. 23).

[28] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §95.

Uit onze gesprekken met de diensten is gebleken dat er op organisatorisch vlak veel waarborgen zijn ingericht. Allereerst leggen medewerkers een eed af waarin zij verklaren zich te houden aan de wet en zorgvuldig om te gaan met de gegevens die zij verzamelen of verder bewerken. Er wordt tevens gebruik gemaakt van doorgaand intern bevragen van medewerkers over de inzet van bevoegdheden. Ook dienen er verschillende stappen intern te worden doorlopen voordat een verzoek tot een last aan de Minister wordt verstuurd. Die interne stappen voorzien ook in meermalige controle op de motivering van het verzoek, met name op het gebied van noodzakelijkheid en proportionaliteit.

In het kader van de uitvoering van de werkzaamheden van de diensten wordt gebruik gemaakt van verschillende scheidingen binnen de organisatie. Zo wordt onderscheid gemaakt tussen wie aan welke onderzoeken werkt en wordt intern het ‘need to know’-principe gehanteerd. Bovendien wordt bij bepaalde bevoegdheden, zoals interceptie, onderscheiden naar de fase van het onderzoek aan de gegevens, waarbij medewerkers niet steeds gedurende de gehele cyclus betrokken hoeven zijn, maar slechts bij een bepaalde fase.

Opvallend is dat de organisatorische maatregelen hoofdzakelijk een interne aangelegenheid zijn, waarbij afspraken zijn gemaakt over de te volgen procedures en werkwijzen. Er wordt geen nadere uitwerking of richting gegeven in de wetstekst zelf, behoudens de genoemde, algemeen geformuleerde zorgplicht. De organisatorische maatregelen zijn daardoor sterk afhankelijk van de professionaliteit en betrouwbaarheid van de betrokken personen en de leiding, en in veel gevallen slechts achteraf toetsbaar op hun praktische uitwerking.

In de zin van het voorgaande ontbreekt nadere duiding over welke technische en organisatorische waarborgen nodig zijn. Gezien de aard van de gegevens die de diensten verwerken en de doelen waarvoor dat gebeurt, zal er een dringende en erkende noodzaak zijn tot adequate beveiliging van de gegevens. Ook wordt geborgd dat niet iedere medewerker bij alle gegevens kan. Het doel van privacybescherming wordt daarmee gediend, maar ook de veiligheid van de medewerkers die daardoor in beginsel niet over volledige informatie kunnen of zullen beschikken. Toch is het opvallend dat het wetsvoorstel nauwelijks aandacht heeft voor de benodigde invulling en vormgeving van de technisch-organisatorische maatregelen. Het vereisen van *Chinese Wall*-constructies of zo nodig het fysiek scheiden van locaties waar bepaalde verwerkingen van gegevens plaatsvinden, is prima te formuleren – bijvoorbeeld in een AMvB – om zo de organisatorische scheiding van processen ook technisch en fysiek vorm te geven. Vanuit het oogpunt van zorgvuldigheid zou het principe van Privacy en gegevensbescherming *by design* en *by default* (DPbD) dan ook als uitgangspunt moeten gelden. Ongeacht of (aankomende) wetgeving die dat vereist van toepassing is op de diensten, kan hiermee een bijdrage geleverd worden aan gerechtvaardigd vertrouwen in de diensten. DPbD kan een signaal zijn voor het serieus nemen van privacy en gegevensbescherming. Bovendien kan met de toepassing van DPbD voorkomen worden dat onrechtmatigheden of fouten optreden, simpelweg omdat deze technisch op voorhand onmogelijk zijn gemaakt. We bevelen daarom aan om een bepaling op te nemen waarin het toepassen van Privacy en gegevensbescherming *by design* en *by default* in het licht van technische en organisatorische waarborgen voor de zorgvuldigheid van de verwerking van gegevens verplicht wordt gesteld (zie hfd. 10).

## 4.4 Algemeen kader bijzondere bevoegdheden

Naast een ‘algemene’ bevoegdheid (zie par. 5.1, hebben de AIVD en de MIVD de nodige bijzondere bevoegdheden tot gegevensverzameling. In paragraaf 3.2.2 van het wetsvoorstel worden deze bevoegdheden uiteengezet. Het betreft bijvoorbeeld de inzet van personen in specifieke hoedanigheden (agenten) of de inzet van bepaalde middelen (zoals toegang tot besloten plaatsen) of technieken (zoals DNA-onderzoek) om gegevens te verzamelen. Deze bevoegdheden worden meestal in het geheim uitgeoefend, wat het des te belangrijker maakt om ze van voldoende waarborgen te voorzien. De huidige wettelijke regeling voorziet daar volgens de MvT reeds in, maar dient in diverse opzichten – zowel naar aanleiding van het kabinetsstandpunt inzake het rapport van de commissie-Dessens als naar aanleiding van ontwikkelingen in de jurisprudentie van het EHRM – nadere aanvulling en aanscherping, aldus de MvT.

### *4.4.1 Doelen van inzet van bevoegdheden*

Evenals het huidige artikel 18 Wiv 2002 bepaalt artikel 23 Wiv 20xx dat bijzondere bevoegdheden mogen worden uitgeoefend voor zover noodzakelijk voor de goede uitvoering van de taken van de diensten (art 8 lid 2 a en d en 10 lid 2 a, c en d). Voor de overige taken (bijvoorbeeld een veiligheidsonderzoek zoals bedoeld in art 8 lid 2 b) volstaat de algemene bevoegdheid tot het verzamelen van gegevens als bedoeld in artikel 22. Daaraan is in de Wiv 20xx toegevoegd dat deze bevoegdheden voorts mogen worden uitgeoefend *ter ondersteuning* van een goede taakuitvoering (een uitbreiding ten opzichte van ‘*in het kader van* een goede taakuitvoering’) van de diensten, wanneer dat noodzakelijk is om

- de noodzaak tot het treffen van bijzondere veiligheidsmaatregelen voor een persoon die werkzaam is voor of ten behoeve van de dienst te beoordelen, of
- om te beoordelen of de personen die meewerken aan het verzamelen van gegevens betrouwbaar zijn.

De ondersteuning van de taakuitvoering is dus specifiek afgebakend voor twee doelen, namelijk een beveiligingsonderzoek of een betrouwbaarheidsonderzoek. Voor het treffen van bijzondere veiligheidsmaatregelen rust een bijzondere verantwoordelijkheid op de hoofden van de diensten. Volgens de MvT kan het onder bepaalde omstandigheden (onder strikte voorwaarden, zoals toestemming, waarbij extra voorwaarden gelden in artikel 24) noodzakelijk zijn om bijzondere bevoegdheden in te zetten, bijvoorbeeld voor het in kaart brengen van de risico’s die een bron loopt, door zicht te krijgen op de omgeving of het netwerk waarin deze zich begeeft, bijvoorbeeld door hem te volgen of om verkeersgegevens op te vragen (p. 32). Dit geldt ook voor de beoordeling van de betrouwbaarheid van personen die medewerking verlenen aan het verzamelen van gegevens. Dat kan, volgens de MvT, bijvoorbeeld aan de orde zijn om te controleren of een agent ook niet gerund wordt door een andere dienst.

Met deze uitbreiding van de inzet van bijzondere bevoegdheden ten behoeve van deze doeleinden doen zich geen grote privacyrisico’s voor. Weliswaar bestaat de kans dat personen in de omgeving van de onderzochte mensen onderwerp van onderzoek worden, maar het doel van het onderzoek is specifiek afgebakend en gericht op de persoon zelf, zodat het risico dat over andere personen veel informatie wordt verzameld, gering blijft. Bovendien wordt hier een zorgvuldigheidsbelang gediend, dat ten goede komt van de algemene kwaliteit van de werkzaamheden van de diensten en ook als zodanig een privacywaarborg dient.

### *4.4.2 Toestemming*

Dat de waarborgen in het wetsvoorstel steeds zwaarder worden naarmate de inbreuk op de persoonlijke levenssfeer groter is, komt onder meer tot uiting in de toestemmingssystematiek (art. 24). De uitoefening van bijzondere bevoegdheden is alleen toegestaan – tenzij specifiek anders wordt bepaald in een artikel – met toestemming van de betrokken minister of namens deze het betrokken hoofd van de dienst (lid 1). De toestemming kan volgens lid 2 echter ook door ondergeschikte ambtenaren worden verleend als deze daartoe schriftelijk zijn aangewezen door het diensthoofd (het zogeheten onder-mandaat). Dit maakt het mogelijk voor de betrokken minister om volledige ministeriële verantwoordelijkheid te dragen voor de inzet van bijzondere bevoegdheden door de inlichtingen- en veiligheidsdienst en daarover parlementaire verantwoording af te leggen.

Over het mandaat en onder-mandaat bij het verlenen van toestemming schrijft de MvT dat de minister de bevoegdheid houdt om zelf toestemming te geven, en dat het evident is dat in alle gevallen dat toestemming in (onder)mandaat kan worden verleend, deze gevallen toch ter besluitvorming aan de minister worden voorgelegd ‘indien aan de uitoefening van een bepaalde bijzondere bevoegdheid mogelijk een groot politiek of andersoortig risico is verbonden’ (p. 34). Dat is belangrijk, omdat in sommige gevallen waarin relatief lichte bevoegdheden (die niet per se toestemming op ministerieel of diensthoofdniveau nodig hebben) worden overwogen, ondergeschikte medewerkers de consequenties van de inzet van dergelijke bevoegdheden niet altijd goed zullen kunnen overzien, bijvoorbeeld als handelingen door de MIVD het civiele domein raken of handelingen van de AIVD het militaire domein. Interne procedures en trainingen zullen moeten bevorderen dat gemandateerde medewerkers alleen beslissingen kunnen nemen over inzet van bevoegdheden wanneer zij voldoende alle aspecten (waaronder de privacyimplicaties) van deze inzet kunnen overzien.

Lid 6 geeft de vereisten aan waaraan een verzoek om toestemming moet voldoen. De MvT merkt op dat bij de gronden voor het verlenen van toestemming ook de eisen van proportionaliteit en subsidiariteit hun beslag dienen te krijgen bij de overweging (p. 36). Aangezien bij de inzet van bevoegdheden altijd een inbreuk op de persoonlijke levenssfeer plaatsvindt, is een zorgvuldige afweging over de noodzaak van de inzet belangrijk. De minister moet daarom op basis van een gemotiveerd verzoek tot toestemming in staat zijn die zorgvuldige afweging te maken.

Alleen voor het uitoefenen van een bevoegdheid jegens een journalist, gericht op het achterhalen van de bron van de journalist, is, des verzocht door de betrokken minister, toestemming van de rechtbank Den Haag nodig (lid 4). Hiermee volgt het wetsvoorstel de uitspraak van het EHRM van 22 november 2012 in een door de Telegraaf c.s. tegen de Staat der Nederlanden aanhangig gemaakte zaak, waarin het EHRM unaniem tot het oordeel kwam dat de inzet van bijzondere bevoegdheden van de AIVD jegens journalisten (van De Telegraaf) onder de Wiv 2002 een schending opleverde van artikel 8 en 13 EVRM.[29] Een brief van de minister van BZK, mede namens de minister van V&J (15 september 2012), over de

[29] EHRM, Telegraaf Media Nederland Landelijke Media B.V. en anderen t. Nederland (No. 39315/06).

gevolgen van deze uitspraak heeft geleid tot een wetsvoorstel tot wijziging van de Wiv 2002.[30]

Uit artikel 24 lid 5 volgt vervolgens dat de toestemming voor de gevallen als genoemd in artikel 23 lid 2 (namelijk bijzondere bevoegdheden ten aanzien van veiligheidsmaatregelen en betrouwbaarheid van personen) uitsluitend door de minister gegeven kan worden gegeven op verzoek van het hoofd van de desbetreffende dienst. Volgens lid 5 moet de CTIVD hier op de hoogte gesteld worden van de verleende toestemming. De uitsluitende mogelijkheid tot het verlenen van toestemming door de minister komt, indien van toepassing, steeds terug in de daarop volgende artikelen (bijvoorbeeld artikel 25 lid 2).

## 4.5 Afwegingskader en verslaglegging

In de artikelen 43-45 van het wetsvoorstel is een afwegingskader opgenomen voor de inzet van bijzondere bevoegdheden door de diensten, dat overeenstemt met de regeling in de Wiv 2002 (artikelen 31-33). Allereerst wordt in het eerste lid van artikel 43 aangegeven dat de inzet van bijzondere bevoegdheden slechts geoorloofd is indien de benodigde informatie niet verzameld kan worden uit openbare bronnen of bronnen waarop de dienst een recht tot kennisneming is verleend. De inzet van bijzondere bevoegdheden is dus niet geoorloofd als de informatie ook uit regulier beschikbare bronnen verkregen kan worden. Leden 2, 3 en 4 van artikel 43 stellen vervolgens dat, indien wel een bijzondere bevoegdheid wordt ingezet, voldaan moet worden aan proportionaliteit en subsidiariteit van de inzet van de bevoegdheid.

Artikel 44 bepaalt vervolgens dat zodra het doel van de uitoefening van de bevoegdheid is bereikt dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan, de uitoefening van de bevoegdheid onmiddellijk wordt gestaakt. Met deze bepaling wordt uitdrukking gegeven aan de vereisten van doelbinding en subsidiariteit voor de inzet van een bijzondere bevoegdheid. Artikel 45 bepaalt ten slotte dat van de inzet van een bijzondere bevoegdheid een schriftelijk verslag wordt gemaakt.

Het doel van het afwegingskader is dat de diensten per concrete situatie een zorgvuldige afweging maken over de inzet van bevoegdheden. Er is geen absolute (in abstracto geldende) rangorde in bevoegdheden en de zwaarte van de inbreuk op de persoonlijke levenssfeer – het hangt ervan af hoe deze in concreto wordt toegepast (MvT, p. 94). Het afwegingskader moet ervoor zorgen dat de diensten de inbreuken die zij maken op de grondrechten van burgers, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, van geval tot geval kunnen legitimeren. Om ook gedurende de inzet van een bevoegdheid en achteraf de rechtmatigheidstoets te kunnen maken (door de CTIVD) dient er schriftelijke verslaglegging plaats te vinden.

Het afwegingskader geeft invulling aan een aantal van de vereisten die volgen uit het EVRM voor de legitimiteit van een beperking van het recht op de persoonlijke levenssfeer, waarbij met name doelbinding, proportionaliteit en subsidiariteit zijn vereist. Ook wordt accountability vergroot door de eis van de schriftelijke verslaglegging. Dit zijn belangrijke eisen vanuit het oogpunt van

[30] *Kamerstukken II* 2014/15, 34 027, nrs. 1-4.

privacybescherming, omdat ze richtinggevend (moeten) zijn voor de inzet die diensten in concrete situaties plegen op basis van de hun toegekende, vaak algemeen geformuleerde en veelal ook zeer ruime, wettelijke bevoegdheden.

In het licht van de normerende werking van deze eisen is het onlogisch dat ze aan het eind van de catalogus van bevoegdheden staan, en losgekoppeld zijn van de algemene bepalingen die voor bijzondere bevoegdheden gelden. Het valt niet in te zien waarom het afwegingskader en de verslagleggingsplicht niet aan het begin van de paragraaf staan, samen met de algemene bepalingen ten aanzien van bijzondere bevoegdheden (artikelen 23-24). Door integratie van de algemene eisen wordt ook in de indeling van de wet aangegeven dat de algemene bepalingen die de inzet van de bevoegdheden normeren nauw samenhangen – ze vormen bij elkaar een normeringskader. En door plaatsing aan het begin wordt ook duidelijk gemaakt dat de afweging over de inzet van bevoegdheden juist voorafgaand aan deze inzet plaatsvindt.

## 4.6 Bewaartermijnen en vernietigingsplicht

Een van de basisbeginselen van bescherming van persoonsgegevens is het vernietigen van gegevens die niet (meer) relevant zijn voor het doel (of een verenigbaar doel) waarvoor ze zijn verzameld (en geen andere, zelfstandige, grondslag hebben voor verdere verwerking). Het is ook een van de eisen uit het algemene kader van *Weber en Saravia*: 'the circumstances in which recordings must be erased or the tapes destroyed.'[31] Het wetsvoorstel kent hiertoe een algemene bepaling in paragraaf 3.5 over de verwijdering, vernietiging en overbrenging van gegevens:

---

Artikel 57

1. De gegevens die, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, worden verwijderd.
2. Indien blijkt dat gegevens onjuist zijn of ten onrechte worden verwerkt, worden deze verbeterd onderscheidenlijk verwijderd. Onze betrokken Minister doet daarvan zo spoedig mogelijk mededeling aan hen wie hij de desbetreffende gegevens heeft verstrekt.
3. De verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.
4. Indien met betrekking tot de voor vernietiging in aanmerking komende gegevens een aanvraag als bedoeld in artikel 64 [het inzagerecht, red.] is gedaan, wordt de vernietiging van de desbetreffende gegevens opgeschort tot ten minste het moment waarop op de aanvraag onherroepelijk is beslist. Voor zover de aanvraag om kennisneming is ingewilligd, worden de desbetreffende gegevens niet eerder vernietigd dan nadat de betrokkene van de desbetreffende gegevens overeenkomstig artikel 64, tweede lid, kennis heeft kunnen nemen.

---

De bepaling is ongewijzigd ten opzichte van het huidige artikel 43.

### *4.6.1 Wetssystematische opmerkingen*

Evenals bij het afwegingskader, kan bij deze bepaling worden opgemerkt dat het vanuit het oogpunt van wetssystematiek meer voor de hand ligt om deze bij de

[31] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §95.

andere algemene normerende bepalingen te plaatsen in één normeringskader. De bepaling is immers thematisch nauw verwant met art. 17 lid 2 (doelbinding), de koppeling van gegevensverwerking aan de taakstelling (art. 18) en de plicht een bevoegdheid stop te zetten als het doel is bereikt (art. 44) – al deze bepalingen zijn uitwerkingen van het algemene beginsel van doelbinding.

Een andere wetstechnische kanttekening – die echter ook privacyconsequenties heeft omdat een verkeerde lezing van de bepaling aanzienlijke gevolgen heeft voor de privacybescherming – is dat lid 1 volgens een grammaticale interpretatie alleen van toepassing is op gegevens die ooit relevantie gehad hebben voor het doel waarvoor ze worden verwerkt. Het gaat immers om gegevens die hun relevantie hebben *verloren*, dus niet om gegevens die nooit relevant zijn geweest. Dat negeert volledig het probleem van bijvangst: ook als bevoegdheden zeer doelspecifiek en gericht worden ingezet, zal het altijd kunnen gebeuren dat er niet-relevante gegevens tussen zitten. Wij nemen aan dat het hier om een ongelukkige formulering gaat (die overigens ook al in de huidige wet voorkomt), en dat de wetgever beoogt om met deze bepaling – juist – ook gegevens die überhaupt niet relevant zijn te laten vernietigen. Dat kan ondervangen worden door de bepaling aan te passen: ‘gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren, worden verwijderd.’

### *4.6.2 Algemene beschouwing over bewaartermijnen*

Artikel 57 maakt een onderscheid tussen verwijdering, waarbij de gegevens worden afgezonderd uit de bedrijfssystemen en apart worden bewaard (‘Bij de AIVD worden de verwijderde gegevens verplaatst naar een semistatisch archief, waar de gegevens slechts voor een beperkt aantal medewerkers toegankelijk zijn’, MvT, p. 116), en vernietiging, waarbij de gegevens onherstelbaar worden vernietigd. Naast de algemene bepaling kennen sommige specifieke bevoegdheden ook bepalingen over vernietiging van gegevens die niet relevant zijn, of waarvan de relevantie niet is vastgesteld, na een bepaalde tijd (zie onder en bij de bespreking van de desbetreffende bevoegdheden). Voor gegevens die (nog) wel relevant zijn voor het doel waarvoor ze worden verwerkt gelden verder geen bewaartermijnen: relevante gegevens mogen voor onbepaalde tijd worden bewaard. Ook gegevens waarvan de (huidige) relevantie niet is beoordeeld, lijken voor onbepaalde tijd te mogen worden bewaard, tenzij de gegevens afkomstig zijn van één van de bevoegdheden waarvoor een specifieke bewaartermijn geldt voor niet-onderzochte gegevens.

De regeling van bewaring en vernietiging van gegevens is hiermee rijkelijk ruimhartig voor de diensten.[32] Uit de regeling noch uit de toelichting spreekt enige urgentie in de omgang met niet-relevante gegevens. Dat is kwalijk, omdat de diensten uit de aard der zaak grote hoeveelheden gegevens verzamelen, waarbij vaak veel meer gegevens dan nodig zullen zitten (de spreekwoordelijke hooiberg, die qua omvang veel groter is dan de speld); ook neemt de relevantie van gegevens na verloop van tijd af. Het levert dan ook een groot privacyrisico om gegevens zo ruimhartig te bewaren. Dat is onnodig, en het wordt ook op geen enkele manier door de MvT toegelicht waarom de regeling op dit punt zo ruim zou moeten zijn. Wij lichten dat in het volgende toe en geven aan op welke punten verbeteringen kunnen worden aangebracht, zonder dat dat overigens ten koste zou hoeven te gaan van de slagkracht van de diensten.

[32] Zie ook de reactie van de CTIVD op het voorstel, die inhoudt dat de termijnen lang zijn en dat de onderbouwing tekortschiet, CTIVD 2015c, p. 48.

De regeling van bewaartermijnen bij specifieke bevoegdheden is gebrekkig en slecht onderbouwd (zoals ook besproken in par. 5.1.4 (informanten), 5.6 (celmateriaal), 6.6 (DNA-databank), 7.2.9 (binnendringen in computers), 8.1.4 (gevorderde communicatie-inhoud), 8.2 (gerichte interceptie) en 8.3.2 (bulkinterceptie)). Er worden verschillende bewaartermijnen gehanteerd, waarbinnen gegevens moeten worden onderzocht op relevantie (na ommekomst van de termijn moeten zowel de niet-relevante als de nog niet-onderzochte gegevens worden vernietigd). Deze termijnen lopen uiteen van drie maanden (celmateriaal), een jaar (gegevens verzameld door binnendringen computers, het vorderen van opgeslagen communicatie-inhoud bij aanbieders, gerichte interceptie) tot drie jaar (bulkinterceptie). Er wordt geen onderbouwing gegeven waarom deze bewaartermijnen nodig zijn, noch waarom er zulke grote verschillen bestaan. Mogelijk heeft dat te maken met de onderzoekscapaciteit bij de diensten – hoe meer data, hoe langer het duurt om ze te onderzoeken? – maar gebrek aan capaciteit is geen sterk argument om een privacyinbreuk te laten voortduren.

In het bijzonder bij gegevens die worden verzameld met behulp van bulkinterceptie is het moeilijk te verdedigen dat ook gegevens van personen die geen bedreiging voor de nationale veiligheid vormen (en daaruit zal de overgrote meerderheid van de data bestaan) gedurende drie jaar bewaard mogen blijven. Aangezien ook kabelgebonden bulkinterceptie in het licht van doelbinding zoveel mogelijk doelgericht moet zijn (zie par. 8.3.2), moet er zo snel mogelijk een selectie worden gemaakt tussen relevante gegevens en irrelevante gegevens. Het valt niet in te zien hoe een termijn van drie jaar te verenigen is met het zo snel mogelijk onderzoeken van gegevens; maar ook een termijn van twaalf maanden is daarvoor al onbegrijpelijk lang (zie par. 7.2.9 en 8.1.4; vgl. ook par. 2.3.2). Dergelijke termijnen zijn moeilijk te verdedigen en in ieder geval zonder nadere onderbouwing volstrekt disproportioneel. Het enkele feit *dat* een bewaartermijn wordt vastgesteld, betekent niet dat er ook voldaan is aan het noodzakelijkheidsvereiste van artikel 8 EVRM; de wetgeving moet ook aan minimale kwaliteitseisen voldoen. Zonder heldere onderbouwing van de noodzaak tot langdurige bewaring, kan daar niet aan worden voldaan.

### *4.6.3 Onderzoeksplicht op relevantie*

Een ander probleem is dat er alleen bij enkele bevoegdheden een onderzoeksplicht wordt gehanteerd om binnen een bepaalde termijn de relevantie van gegevens te beoordelen. Gegevens verzameld via andere bevoegdheden (zoals via geautomatiseerde toegang verkregen databestanden van derden, OSINT of observatie) – waar ook vaak niet-relevante gegevens tussen zullen zitten – hoeven niet per se binnen een bepaalde termijn op relevantie worden onderzocht. Hoewel men mag aannemen dat de diensten alle door hen verzamelde gegevens binnen redelijke termijn bekijken (waarom zouden de gegevens anders verzameld moeten worden?), levert het ontbreken van een algemene onderzoeksplicht een aanzienlijk privacyrisico op. Nu zullen via observatie verkregen camerabeelden niet jaren worden bewaard (in verband met de opslagcapaciteit), maar via observatie van Internet verzamelde gegevens uit sociale media kunnen wel heel lang worden bewaard. Het valt niet in te zien waarom alleen gegevens die door de meest ingrijpende bevoegdheden (binnendringen in computers, interceptie) verkregen zijn wel binnen een bepaalde termijn op relevantie onderzocht moeten worden, maar gegevens die door minder ingrijpende bevoegdheden zijn verkregen niet. Voor de (ir)relevantie van gegevens maakt het immers niet uit wat de ingrijpendheid is van

het middel waarmee het is verkregen, en de privacyinbreuk is even groot als gegevens over derden als bijvangst in de bestanden van de diensten terecht komt via interceptie als via observatie of gegevensopvragingen.

Daarom is het aangewezen om een *algemene* bepaling op te nemen met de strekking dat gegevens zo spoedig mogelijk op relevantie moeten worden onderzocht en dat dit onderzoek binnen een bepaalde periode moet plaatsvinden. Vooral de opname van een element ‘zo spoedig mogelijk’ is hierin belangrijk, omdat het de urgentie aangeeft dat niet-relevante gegevens zo snel mogelijk verwijderd behoren te worden, volgens het principe van ‘select while you collect’. Vanwege datzelfde principe is het belangrijk een onderscheid te maken tussen gegevens waarvan is vastgesteld dat deze niet relevant zijn, en gegevens die nog niet op relevantie zijn onderzocht. Een wezenlijk manco van de huidige bepalingen hieromtrent bij specifieke bevoegdheden is dat, doordat beide typen op één hoop worden gegooid, ook gegevens waarvan is vastgesteld dat die niet-relevant zijn, pas na afloop van de genoemde maximumtermijn worden verwijderd. Dat is in strijd met het algemene beginsel van doelbinding (niet-relevante gegevens dienen immers geen doel en mogen dan ook niet verder verwerkt worden, dus ook niet opgeslagen blijven omdat ook opslag een vorm van verwerking is). Op basis hiervan en in lijn met het uitgangspunt van ‘select while you collect’ zou de algemene bepaling dan bijvoorbeeld kunnen luiden (gemodelleerd naar, met de aanbevolen aanpassingen, art. 32 lid 10):

> ‘Gegevens verkregen door uitoefening van een bevoegdheid worden zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven onderzocht. Gegevens waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek, worden terstond verwijderd. Gegevens die niet op hun relevantie voor het onderzoek zijn onderzocht, worden [tenzij anders bepaald] na een periode van [termijn] verwijderd.’

Ons lijkt bij een dergelijke bepaling over een onderzoeksplicht een termijn van drie maanden redelijk als algemene richtlijn, aangezien men van de diensten toch mag verwachten dat zij in staat zijn om, als zij de inzet van een bevoegdheid nodig achten, tenminste binnen drie maanden de verkregen gegevens ook daadwerkelijk te onderzoeken. Waar nodig kan voor specifieke bevoegdheden een afwijkende langere termijn worden bepaald, als de aard van de verzamelde gegevens dat nodig maakt, bijvoorbeeld bij gerichte interceptie, waar gesprekken een voor een uitgeluisterd (en mogelijk vertaald) moeten worden. Mochten er redenen zijn waarom de diensten gegevens niet binnen drie maanden kunnen bekijken, dan zou in de algemene bepaling over de onderzoeksplicht ook een lid toegevoegd kunnen worden dat, als er termen zijn waarom de gegevens niet binnen de gestelde termijn kunnen worden onderzocht, de periode eenmalig verlengd kan worden (bijvoorbeeld met maximaal negen maanden), met toestemming van het diensthoofd; dat valt te prefereren boven een langere standaardtermijn, omdat dan een korte periode de regel is en een langere periode de uitzondering op basis van specifieke redenen moet worden verantwoord.

### *4.6.4 Verwijdering en vernietiging van niet-relevante gegevens*

Een ander privacyrisico in de regeling ontstaat door het onderscheid tussen verwijdering en vernietiging. De wetgever maakt dit onderscheid omdat gegevens die niet voor het onderzoeksdoel relevant (meer) zijn, en dus vernietigd zouden moeten worden, in sommige situaties toch bewaard dienen te blijven. Daarom

worden gegevens niet direct vernietigd maar overgeplaatst, en pas daarna vernietigd. Wet noch toelichting geven daarbij hoe lang verwijderde gegevens beschikbaar blijven in het reservearchief en op welk tijdstip ze kunnen worden vernietigd. Dit bergt een groot privacyrisico in zich dat verwijderde gegevens nog langere tijd in het reservearchief bewaard blijven en in die periode alsnog weer kunnen worden hergebruikt voor operationele doeleinden. De MvT zegt daarover:

> ‘Verwijderen wil zeggen dat de gegevens niet langer toegankelijk zijn voor het reguliere bedrijfsproces (dat wil zeggen ten behoeve van de taakuitvoering van de diensten); zij dienen daarvan te worden afgezonderd. Wel blijven de verwijderde gegevens beschikbaar voor archiefdoeleinden, klachtbehandeling e.d. Dit in tegenstelling tot vernietigen waarbij de gegevens definitief en onomkeerbaar uit de systemen waarin dan wel van de gegevensdragers waarop ze zijn vastgelegd verdwijnen. Verwijderde gegevens kunnen daarom, vanwege het feit dat ze nog niet zijn vernietigd, *onder omstandigheden toch weer opnieuw gebruikt worden, indien het doel waarvoor ze aanvankelijk waren verworven weer actueel is geworden of voor een eventueel ander doel*, mits uiteraard wordt voldaan aan de aan eisen die in algemene zin aan gegevensverwerking worden gesteld. Waar het gaat om verwijderde gegevens zal het vaak ook gaan om gegevens die inmiddels wat ouder zijn; dit gegeven – mede gelet op het bepaalde in artikel 55 van het wetsvoorstel – dient nadrukkelijk bij de beslissing over (verder) gebruik betrokken te worden.’ (p. 116, cursivering toegevoegd)

Ook uit dit citaat spreekt dat het wetsontwerp geen urgentie kent om niet-relevante gegevens die niet voor klachtbehandeling of archiefplicht bewaard moeten worden te vernietigen. Nergens wordt een termijn genoemd, noch wordt gesteld dat verwijderde gegevens zo spoedig mogelijk vernietigd moeten worden als geen van de uitzonderingssituaties (klacht, archiveringsplicht) van toepassing is. Integendeel, het citaat ademt eerder, door de uitgebreide aandacht voor hergebruik, een geest uit van ‘wie wat bewaart die heeft wat’. Het wekt de suggestie dat het reservearchief mede bedoeld is om niet-relevante gegevens nog een tijdje achter de hand te hebben; je weet maar nooit of ze ooit nog weer relevant worden voor het oorspronkelijke doel, of ergens anders van pas komen.

De hier met zoveel woorden geboden, of in elk geval expliciet overwogen, mogelijkheid tot *function creep* moet sterk worden afgewezen. Het valt immers niet in te zien waarom gegevens die verwijderd moeten worden wegens niet-relevantie voor operationele doeleinden, en waarbij niet een andere grond (zoals archiefplicht) bestaat om ze nog verder te verwerken, überhaupt in een reservearchief zouden moeten worden opgenomen. Natuurlijk kunnen niet-relevante gegevens ooit relevant worden, maar dat kan geen argument zijn om ze door de diensten te laten bewaren; dat argument zou een blanco check betekenen voor de diensten om willekeurig welk gegeven te verzamelen, ongeacht doelbinding, omdat het ooit eens relevant zou kunnen worden.

De wet zou kortom moeten bepalen dat gegevens terstond worden vernietigd zodra blijkt dat ze niet (of niet meer) relevant zijn (of wanneer de termijn voor onderzoek op relevantie is verstreken), tenzij ze voor klachtbehandeling of vanwege de archiefplicht bewaard moeten blijven; in de laatste gevallen zou de wet (gesteund door adequate technische en organisatorische maatregelen) dan expliciet moeten uitsluiten dat de gegevens in die situatie alsnog weer voor operationele doeleinden

kunnen worden gebruikt. Indien zich noodsituaties voordoen waarin verwijderde gegevens essentieel blijken voor operationele doelen, dan zou daarvoor een aparte procedure, met onafhankelijke toestemming vooraf, moeten gelden (zie onder). Een en ander geldt zowel voor de specifieke bevoegdheden waarin aparte onderzoeksplichten met termijnen worden genoemd, als voor de algemene bepaling van artikel 57. Dat de diensten feitelijk in staat zijn om gegevens terstond te vernietigen in plaats van ze eerst in een reservebestand te plaatsen, blijkt bijvoorbeeld uit artikel 32 lid 4 en artikel 32 lid 9; uitvoeringsbezwaren hoeven dus geen belemmering te vormen tegen directe vernietiging.

Daarbij is het wel relevant om artikel 57 lid 4 te behouden, dat bepaalt dat zodra er een verzoek is tot kennisneming van gegevens door een betrokkene, de vernietigingsplicht wordt opgeschort. Voor privacybescherming is het inzagerecht van groot belang, en voorkomen moet worden dat diensten, wanneer een verzoek tot kennisneming binnenkomt, ter plekke besluiten om bepaalde gegevens te vernietigen omdat ze toch niet meer relevant zijn, om dan te kunnen antwoorden dat ze geen, of slechts een beperkt aantal, gegevens over de betrokkene verwerken. Lid 4 voorziet daarin.[33] De combinatie van beide privacybelangen – terstond vernietigen van niet relevante gegevens, maar niet als er een inzageverzoek ligt of binnenkomt – kan geadresseerd worden door artikel 57 lid 3 te integreren in lid 1 en een verwijzing naar het inzagerecht te voegen: de gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren, worden terstond vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan of een aanvraag als bedoeld in artikel 64[34] met betrekking tot deze gegevens is gedaan.

Het is daarbij wenselijk dat de CTIVD de bevoegdheid verkrijgt om erop toe te zien dat irrelevante gegevens ook daadwerkelijk zo spoedig mogelijk worden vernietigd en niet nog een tijdje achter de hand worden gehouden, en dat de uitzonderingen (voor archiefdoeleinden of inzagerecht) strikt worden nageleefd. Ook is het wenselijk dat, vanuit het principe van gegevensbescherming *by design*, gegevens die op basis van een uitzonderingsgrond worden bewaard, dusdanig worden opgeslagen dat ze ook alleen voor dat doel (archiefplicht, inzagerecht) kunnen worden gebruikt. De Memorie van Toelichting gaat zoals hierboven gesignaleerd te makkelijk om met doelafwijkende nieuwe verwerkingen, wat een groot privacyrisico oplevert.

Als er klemmende redenen zijn om toch de voor een specifieke uitzondering de bewaarde, voor vernietiging gemarkeerde, gegevens voor een ander doel te gebruiken (bijvoorbeeld het oorspronkelijke onderzoek of een nieuw onderzoek), dan zou de beslissing daarover bij een onafhankelijk orgaan, zoals de CTIVD of de rechter, moeten liggen. Hiervoor kan bijvoorbeeld de techniek van ‘revocable privacy’ worden gebruikt, waarbij gegevens dusdanig worden opgeslagen dat ze

[33] Ons is onbekend of er ook behoefte bestaat aan een uitzondering om voor vernietiging in aanmerking komende gegevens te bewaren voor klachtbehandeling. De MvT (p. 116) noemt klachtbehandeling als een van de grondslagen om verwijderde gegevens te verwerken die in het reservearchief zijn opgeslagen. Het wetsontwerp kent echter geen uitzonderingsregel voor klachtbehandeling, zoals die in lid 4 wel bestaat voor inzageverzoeken. Het is voorstelbaar dat het bij klachtprocedures onwenselijk is dat gegevens tussentijds door de diensten vernietigd worden; in dat geval zou een analoge bepaling als in lid 4 moeten worden opgenomen voor klachten ex artikel 103.

[34] En eventueel een klacht als bedoel in artikel 103, zie vorige noot.

onleesbaar zijn, tenzij ze ontsleuteld worden op basis van geautoriseerde toestemming; die ontsleuteling voor doelafwijkend gebruik zou vooraf getoetst moeten worden door de CTIVD, gezien het uitzonderlijke karakter van de situatie. Waar het papieren gegevensdragers betreft, kunnen analoge maatregelen worden getroffen door de papieren in een kluis te bewaren, waarbij de toegangscode in twee delen wordt gesplitst en één deel bij bijvoorbeeld het diensthoofd wordt ondergebracht en het andere deel bij de voorzitter van de CTIVD. De kluis kan dan alleen worden geopend indien beiden toestemming geven.

### *4.6.5 Bewaartermijn en controleplicht voor relevante gegevens*

Terwijl er een regeling wordt getroffen voor verwijdering en vernietiging van niet-relevante (en, in sommige gevallen, niet onderzochte) gegevens (die zoals boven aangegeven aanpassing behoeft), bestaat er geen regeling met een bewaartermijn voor relevante gegevens. Deze mogen dus voor onbepaalde tijd worden bewaard.[35] De gedachte daarbij zal zijn dat relevante gegevens uit de aard der zaak bewaard moeten blijven – ze zijn immers relevant. Het maakt niet uit of het tien, twintig of tachtig jaar duurt, zolang de gegevens maar relevant zijn. Dat brengt het risico met zich mee dat gegevens bewaard blijven ook nadat ze hun relevantie hebben verloren.

Hoewel het een aannemelijke gedachtegang lijkt om relevante gegevens voor onbepaalde tijd te bewaren, is deze gebaseerd op een foute aanname. Er wordt kennelijk van uitgegaan dat vanzelf en tijdig ontdekt wordt dat gegevens hun betekenis verloren hebben. Gegevens zijn echter passief en stom: ze blijven zitten waar ze zitten en kunnen niet zelf om vernietiging vragen als ze zich niet meer thuis voelen in de bestanden van de diensten. Er zullen mensen naar moeten kijken om vast te stellen of gegevens nog relevant zijn. Daartoe ontbreekt een bepaling. Er bestaat slechts bij sommige bevoegdheden een clausule die eist dat de relevantie van verzamelde gegevens wordt onderzocht, die als boven betoogd veralgemeniseerd zou moeten worden (par. 4.6.3). Dat is echter niet voldoende: het gaat daarbij alleen om een eerste toets na de verwerving van de gegevens. Is eenmaal vastgesteld dat gegevens relevant zijn, dan kunnen deze voor onbepaalde tijd worden bewaard en gebruikt voor het doel waarvoor ze verzameld zijn, of een ander doel als daar een grondslag voor is. Maar het kan voorkomen dat gegevens *niet* worden gebruikt, en verder nooit meer worden bekeken.

[35] Dat zal althans de bedoeling zijn van de wetgever. Grammaticaal gesproken bindt het wetsontwerp bewaring van relevante gegevens aan een maximumtermijn van een jaar, voor zover ze verzameld zijn via binnendringen in een computer, gerichte interceptie of communicatie-inhoudsvordering. De specifieke vernietigingsplichten in art. 30, 32 en 38 luiden immers: ‘Gegevens, waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste twaalf maanden vernietigd.’ ‘Gegevens’ slaat hierin op de gegevens die verkregen zijn door uitoefening van de desbetreffende bevoegdheid. Omdat er een komma staat tussen ‘gegevens’ en ‘waarvan’, gaat het in de bepaling om een uitbreidende bijzin, en niet om een beperkende bijzin. Dit betekent dit dat de bepaling van toepassing is op *alle* gegevens (uitbreidende bijzinnen kunnen immers worden weggelaten zonder dat de betekenis van de hoofdzin verandert), en niet alleen op het type dat vermeld wordt in de bijzin. Grammaticale interpretatie betekent dan ook een vernietigingsplicht voor alle gehackte of gericht onderschepte gegevens na afloop van een jaar, ook als deze (nog) relevant zijn voor het onderzoek in het kader waarvan ze zijn verzameld. Dat is prettig voor de privacy, maar vermoedelijk niet de bedoeling van de wetgever.

Dit levert een groot privacyrisico op: er is een aanzienlijke kans dat gegevens langer worden bewaard dan nodig is. Het omslagpunt waarbij gegevens hun relevantie verliezen zal niet automatisch in beeld komen; vaak zullen ooit relevante gegevens dus nog een tijd bewaard blijven, ook lang nadat ze hun betekenis hebben verloren. Gedurende deze periode bestaat het risico dat gegevens die onterecht (want zonder doel) bewaard blijven, worden gehackt, gelekt of misbruikt. Dat risico moet zoveel mogelijk worden uitgesloten.

Waar het omslagpunt van relevantie naar irrelevantie ligt, kan niet in absolute zin worden voorspeld: het zal voor elk gegeven van de omstandigheden afhangen. Wat wel mogelijk is, is een combinatie van twee maatregelen.

Ten eerste kan een maximale bewaartermijn worden ingevoerd, omdat er een natuurlijke grens zit aan de relevantie van gegevens die voor specifieke onderzoeken door de diensten worden verzameld. Ter vergelijking kan worden gekeken naar de Wet strafvorderlijke en justitiële gegevens (Wsjg), waarin bewaartermijnen zijn vastgesteld die gekoppeld zijn aan de verjaringstermijnen van bepaalde misdrijven. De noodzakelijkheid van het bewaren van de gegevens is in dat verband concreet gekoppeld aan het doel en de limitering van de bewaartermijn die door dat doel bepaald wordt in de vorm van verjaring. Denkbaar is dat voor de onderscheiden typen onderzoeken die de diensten uitvoeren (als bepaald in artikel 18) maximale bewaartermijnen worden vastgesteld die gekoppeld zijn aan het type doel dat met dat type onderzoek gemoeid is en de termijn die redelijkerwijs nodig kan zijn om nog relevantie te houden voor dat doel.

Ten tweede zou een periodieke controleplicht moeten worden ingevoerd. Dat is nodig, omdat gegevens nu eenmaal niet uit zichzelf aangeven dat ze relevantie aan het verliezen zijn. In EHRM-rechtspraak wordt in *Weber en Saravia* verwezen naar een Duitse bepaling als een geschikte waarborg. Deze bepaling stelt dat opgeslagen gegevens elke zes maanden moeten worden (her)beoordeeld op relevantie.

‘Moreover, the G 10 Act contained strict provisions concerning the storage and destruction of data. The responsibility for reviewing stored files on a six-month basis was entrusted to an official qualified to hold judicial office. Data had to be destroyed as soon as they were no longer needed to achieve the purpose pursued.’[36]

Op basis van deze bepaling moeten dus de met ingrijpende, heimelijke bevoegdheden vergaarde gegevens elke zes maanden worden herbeoordeeld door een gekwalificeerd persoon, en vernietigd zodra blijkt dat ze niet meer nodig zijn. Wij kunnen ons voorstellen dat de zesmaandsperiode uit de Duitse G10-wet niet voor alle typen bevoegdheden veralgemeniseerd kan worden en dat het praktisch moeilijk haalbaar is om alle door de diensten verzamelde gegevens elk half jaar te controleren op relevantie. Maar periodieke controle in enige vorm is nodig, om te voorkomen dat gegevens voor onbepaalde tijd opgeslagen kunnen blijven. Denkbaar is een combinatie van integrale periodieke controle op relevantie door daartoe aangewezen, gekwalificeerde medewerkers van de diensten, met steekproefsgewijze controles door de CTIVD, waar mogelijk gefaciliteerd door automatisering, om na te gaan of opgeslagen gegevens daadwerkelijk worden gebruikt, geanalyseerd en gecontroleerd op relevantie door de diensten. Wanneer

[36] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §116.

bij de integrale periodieke controle of bij een controle van de CTIVD wordt vastgesteld dat opslag niet meer noodzakelijk is, is er geen reden om de gegevens nog langer te bewaren en zouden ze dan ook terstond moeten worden verwijderd en, als er geen uitzonderingsgrond bestaat in verband met archiefplichten of inzageverzoeken, vernietigd.

# 5 Informationele privacy

In dit hoofdstuk besteden we aandacht aan de informationele privacy van burgers in relatie tot enkele bijzondere bevoegdheden tot het verzamelen van (persoons)gegevens. De relatie met privacy is primair gelegen in artikel 10 lid 2 en 3 van de Grondwet, maar ook de andere privacygrondrechten hebben veelal een informationele component, in de vorm van de regulering van kennis over lichaam, huis en communicatie.

Achtereenvolgens wordt ingegaan op de algemene bevoegdheid tot het verzamelen van persoonsgegevens (artikel 22 van het wetsvoorstel), op het verzamelen van gegevens uit open bronnen (OSINT), geautomatiseerde data-analyse, en het delen van gegevens met buitenlandse diensten. Bij OSINT en geautomatiseerde data-analyse wordt ook aandacht besteed aan de mogelijkheden tot profilering die uit deze bevoegdheden voortvloeien.
We gaan niet in op het verwerken van persoonsgegevens van agenten (artikel 26), naslag en op de andere vormen van het delen van gegevens, zoals met andere autoriteiten binnen Nederland.

## 5.1 Algemene bevoegdheid

### *5.1.1 Inleiding*

In paragraaf 3.2.1 van het wetsvoorstel is de algemene bevoegdheid van de diensten tot het verzamelen van gegevens omschreven. Artikel 22 van het voorstel geeft daarbij aan dat de diensten zich tot bestuursorganen, ambtenaren en voorts een ieder kunnen wenden die geacht wordt de benodigde gegevens te kunnen verstrekken.

---

Artikel 22

1. De diensten zijn bevoegd zich bij de uitvoering van hun taak, dan wel ter ondersteuning van een goede taakuitvoering, voor het verzamelen van gegevens te wenden tot bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken.
2. In het geval dat een verzoek als bedoeld in het eerste lid wordt gericht tot een verantwoordelijke voor een gegevensverwerking, is de daarmee belaste ambtenaar verplicht zich ten opzichte van de verantwoordelijke voor een gegevensverwerking te legitimeren aan de hand van een daartoe door het betrokken hoofd van een dienst verstrekt legitimatiebewijs.
3. Aan een verzoek als bedoeld in het eerste lid kan worden voldaan door het verlenen van rechtstreekse geautomatiseerde toegang aan de dienst tot de desbetreffende gegevens dan wel door het verstrekken van geautomatiseerde gegevensbestanden.
4. De bij of krachtens de wet geldende voorschriften voor de verantwoordelijke voor een gegevensverwerking betreffende de verstrekking van zodanige gegevens zijn niet van toepassing op verstrekkingen gedaan ingevolge een verzoek als bedoeld in het eerste lid.

5. Gegevens die betrekking hebben op dan wel kunnen leiden tot de vaststelling van de identiteit van een natuurlijke persoon die op heimelijke wijze medewerking heeft verleend aan een verzoek tot verstrekking van gegevens als bedoeld in het eerste lid worden 30 jaar nadat de medewerking van de desbetreffende natuurlijke persoon is beëindigd, vernietigd.

Ongewijzigd ten opzichte van de huidige Wiv 2002 is de bevoegdheid van de diensten zich voor het verzamelen van gegevens te wenden tot bestuursorganen en ambtenaren en eenieder die geacht wordt benodigde gegevens te kunnen verstrekken (lid 1). Nieuw is de bepaling dat aan het verzoek kan worden voldaan door het verlenen van rechtstreeks geautomatiseerde toegang tot desbetreffende gegevens of door het verstrekken van geautomatiseerde gegevensbestanden (lid 3).

### *5.1.2 Algemene beschouwing over gegevensverstrekking door derden*

De bevoegdheid uit artikel 22 kan uitgeoefend worden jegens eenieder. Het gaat om verstrekking op basis van vrijwilligheid; de bevraagde heeft dus de mogelijkheid om de gevraagde gegevens niet te verstrekken. Of de gevraagde daadwerkelijk de ruimte voelt om te kunnen weigeren, zal mede afhangen van de manier waarop het verzoek om gegevensverstrekking precies wordt gedaan. De MvT zegt daar niets over. Het zou wenselijk zijn dat verzoeken op basis van artikel 22 worden genormeerd door een protocol of richtlijnen die eisen stellen aan het verzoek, waarbij de bevraagde duidelijk wordt gemaakt dat het gaat om vrijwillige verstrekking en waarbij gewezen wordt op de mogelijke gevolgen van verstrekking voor de persoonlijke levenssfeer van betrokkenen, zodat de bevraagde een zelfstandige belangenafweging kan maken.

Afhankelijk van de hoeveelheid en het type gegevens kan, ook bij vrijwillige verstrekkingen, met deze bevoegdheid een gedetailleerd beeld van het persoonlijke leven van een persoon verkregen worden. Aangezien er in het artikel geen limiet of specificatie van typen gegevens is benoemd, is een brede, diepe en langdurige toepassing van de bevoegdheid mogelijk. Dat maakt de bevoegdheid potentieel zeer ingrijpend: uit bestanden van derden kan, zeker in combinatie, een zeer gedetailleerd beeld van iemands persoonlijke levenssfeer ontstaan. Vrijwel elk gedrag laat tegenwoordig digitale sporen na dat in een databank terecht komt, en de cumulatie van al deze sporen kan veel meer zeggen over een persoon dan een huiszoeking of telefoontap kan opleveren. Illustratief is bijvoorbeeld het onderzoek dat aangeeft dat met behulp van data-analyse iemands persoonlijkheid inmiddels beter in kaart kan worden gebracht, op basis van haar ‘vind-ik-leuk’-klikgegevens, dan de mensen in de naaste omgeving van de persoon dat kunnen (met uitzondering van de partner).[37]

Bovendien wordt de mogelijkheid gecreëerd om, in samenhang met lid 3, een real-time beeld te verkrijgen en bovendien permanent de gegevens te analyseren. Hier moet worden beseft dat alle drie van de waarschuwingsvlaggen aan de orde zijn, die de WRR heeft ontwikkeld voor een zorgvuldige ontwikkeling van processen van informatieverwerking door de overheid.[38] Er is immers sprake van 1) het vernetwerken van informatie (de informatie bij een gegevensverwerker wordt

[37] Alice Park, ‘Here’s Proof That Facebook Knows You Better Than Your Friends’, *Time*, 12 januari 2015, http://time.com/3663775/facebook-likes-personality/.
[38] Zie WRR 2011.

automatisch vernetwerkt met de gegevensverwerking door de diensten), 2) het samenstellen en verrijken van informatie (de ingewonnen gegevens worden gekoppeld, vergeleken en verrijkt met andere gegevens) en 3) het voeren van preventief en reactief beleid op basis van informatie (dat is immers het doel van de gegevensbevraging).

De potentiële inbreuk op de persoonlijke levenssfeer is dan ook erg groot. Hoewel de bevoegdheid als een 'algemene bevoegdheid' is omschreven, wat de suggestie wekt dat deze anders van aard is dan de 'bijzondere' bevoegdheden, betreft het dus wel degelijk een erg vergaande bevoegdheid, en behoort het vanuit privacyperspectief, vanwege het ongeclausuleerde bereik, tot de potentieel meest ingrijpende bevoegdheden. Daarnaast bestaat er een reële kans dat één of meer personen kennis en inzicht krijgen in de targets van de diensten en de gegevens die ten aanzien van die targets verzameld worden. Dat kan voor de verstrekkers van gegevens belastend zijn en ook aanvullende privacyrisico's voor betrokkenen met zich brengen (in dit verband ook lid 5, zie onder).

Gezien de mogelijk bijzonder grote privacyinbreuk zou deze bevoegdheid dan ook niet als een 'algemene' bevoegdheid moeten worden gepresenteerd, maar als een 'bijzondere' bevoegdheid. Het feit dat het gaat om verstrekking op basis van vrijwilligheid, doet daar niet aan af. De stand van de techniek leidt er immers toe dat de impact van de toepassing van deze bevoegdheid, die primair in de lijn ligt van het vragen om informatie aan derden, veel groter is dan voorheen. Vanwege elektronische communicatie en de uitwisseling van informatie via een veelheid aan platforms en toepassingen hebben bepaalde personen of instellingen immers mogelijk toegang tot een 'knooppunt' van elektronisch verkeer. Er is dus geen sprake van het verzamelen van verschillende kleine brokjes informatie die vervolgens met elkaar in verband moeten worden gebracht om zo een stukje van de gedragingen van een target bloot te leggen. In bepaalde gevallen zijn een heleboel stukjes tegelijkertijd toegankelijk en direct aan elkaar en aan bepaalde targets verbonden.

Omdat de uitoefening van de bevoegdheid een zware inbreuk op de persoonlijke levenssfeer kan opleveren, zijn zware waarborgen vereist. Evenals bij het oude artikel 17 gelden bij het voorgestelde artikel 22 de algemene bepalingen omtrent gegevensverwerking door de diensten. Een verzoek moet dus altijd plaatsvinden voor een bepaald doel, zorgvuldig en op behoorlijke wijze plaatsvinden en in overeenstemming met de wet. Het willekeurig opvragen van gegevens is dus niet geoorloofd (MvT, p. 25). Dat doet echter aan de mogelijke reikwijdte van de bevoegdheid niet af. Daarom zijn meer waarborgen nodig. Het is onbegrijpelijk dat de algemene bepalingen die gelden voor bijzondere bevoegdheden (art. 23-24) niet van toepassing zijn op deze 'algemene' bevoegdheid. Zo ontbreekt het noodzakelijkheidsvereiste (art. 23), is er geen termijn opgenomen gedurende welke de bevoegdheid uitgeoefend mag worden (art. 24 lid 3), ontbreekt bronbescherming voor journalisten (art. 24 lid 4), en is geen toestemming vooraf vereist (art. 24 lid 1-2).
Aangezien de 'algemene' bevoegdheid minstens even – en in sommige gevallen meer – ingrijpend kan zijn in vergelijking met de nodige bijzondere bevoegdheden, zou deze op zijn minst aan hetzelfde normeringskader moeten zijn onderworpen. Dit dient zowel het belang van rechtsbescherming als het belang van de rechtszekerheid van de derde die (als informant) betrokken wordt bij de activiteiten van de diensten. Feitelijk betekent dit dat artikel 22 moet worden geïntegreerd in

paragraaf 3.2.2 en dat het onderscheid tussen ‘algemene’ en ‘bijzondere’ bevoegdheden daarmee kan komen te vervallen. De algemene bepalingen van het normeringskader (zie hfd. 4) worden dan van toepassing op de bevoegdheid gegevens te doen verstrekken.
Dat is echter niet voldoende om deze, als gezegd ruime, bevoegdheid te normeren. In gevallen waarin er uit de gevraagde gegevens een indringend beeld van de persoonlijke levenssfeer kan ontstaan, zou de normering aanvullende eisen moeten stellen. In die gevallen is eerder toestemming op het niveau van het diensthoofd, of zelfs van de minister (voor geautomatiseerde toegang), aangewezen; het gaat dan immers om een privacyinbreuk die vergelijkbaar is met interceptie van communicatie. Ook voor het verkrijgen van gegevens via geautomatiseerde toegang zijn aanzienlijk zwaardere waarborgen nodig dan het algemene kader.

### *5.1.3 Geautomatiseerde toegang*

Artikel 22 lid 3 is nieuw en schept de mogelijkheid een koppeling te maken bij een gegevensverwerker waardoor rechtstreeks geautomatiseerde toegang wordt verkregen. Hierover schrijft de MvT dat met rechtstreeks geautomatiseerde toegang een online en *real-time*-verbinding tussen de dienst en de verstrekkende persoon of instantie bedoeld wordt. Daarbij kan de dienst de gegevens die deze nodig heeft voor een goede taakuitvoering, zonder menselijke tussenkomst aan de kant van de verstrekkende persoon of instantie, opvragen en verstrekt krijgen. Deze toegang zou met name van belang zijn in de gevallen waarbij het voorzienbaar is dat in het kader van een goede taakuitvoering het wenselijk is dat de diensten structureel de beschikking hebben over (actuele) gegevens die bij een persoon of instantie beschikbaar zijn. In verband met het vereiste uit het EVRM dat bevoegdheden voldoende kenbaar en voorzienbaar moeten zijn, wordt hier een expliciete wettelijke basis voor opgenomen, zegt de MvT (p.184). Een alternatief voor rechtstreekse geautomatiseerde toegang is het integraal verstrekken van geautomatiseerde gegevensbestanden door de bevraagde. Deze praktijk zal, volgens de toelichting, vaak aan de orde zijn, indien men op dergelijke gegevensbestanden specifieke vormen van data-analyse (zie artikel 47), zoals het doorzoeken op profielen of naar patronen – al dan niet in combinatie met andere bestanden – wil toepassen. Dit soort bewerkingen dienen vanwege privacy- en beveiligingsaspecten idealiter binnen het afgeschermde ICT-domein van de diensten zelf plaats te vinden. (MvT, p. 27).

Het integraal verstrekken van geautomatiseerde bestanden biedt de mogelijkheid te voorkomen dat de gegevensverwerker inzicht krijgt in hetgeen de dienst zoekt. Dat maakt het in zeker opzicht minder belastend voor de gegevensverwerker, omdat deze niet kennis hoeft te nemen van de specifieke personen waarin de diensten geïnteresseerd zijn. Het kan daarmee ook bijdragen aan de privacybescherming van betrokkenen, die immers geraakt kunnen worden door beslissingen die de gegevensverwerker (mogelijk ook onderbewust) neemt vanuit de wetenschap dat veiligheidsdiensten in deze betrokkene geïnteresseerd zijn. De mogelijkheid van rechtstreekse geautomatiseerde toegang maakt de uitvoering van de bevoegdheid efficiënter, als de diensten structureel beschikking willen krijgen over gegevens bij een bepaalde verwerker.

Daar staat tegenover dat geautomatiseerde toegang ook grote aanvullende privacyrisico’s oplevert, die verder gaan dan het ‘handmatig’, al dan niet op structurele basis, opvragen van gegevens. Dit is gelegen in het feit dat een belangrijke natuurlijke drempel wegvalt: bij het opvragen van gegevens bij een

derde, heeft de derde weet van de bevraging, en kan zij eventueel weigeren als zij de bevraging volstrekt disproportioneel of evident onjuist vindt (bijvoorbeeld als zij een foutief kenmerk of persoonsverwisseling in de bevraging constateert); dit biedt een zekere vorm van natuurlijk tegenwicht dat ook een normerend effect heeft op de bevragingen door de diensten (die hierdoor immers een prikkel hebben om niet volstrekt disproportionele of onjuiste bevragingen te doen). Deze natuurlijke drempel valt weg wanneer geautomatiseerd toegang wordt verleend. Daar komt bij dat geautomatiseerde toegang het element van het vernetwerken van informatie (de eerste waarschuwingsvlag van de WRR) versterkt, omdat gegevens die voor allerlei andere doeleinden worden verwerkt automatisch beschikbaar komen voor de diensten.

Het toezicht op de omvang van aldus verzamelde gegevens is bijzonder lastig, ook wanneer gebruik gemaakt wordt van een filter waarmee een eerste selectie automatisch plaatsvindt en alleen de informatie die past bij het target wordt doorgegeven. Bovendien ontstaan meer mogelijkheden voor grootschalige verwerking, met name bij het gebruik van generieke identiteiten om informatie uit bestanden te filteren, waarmee slechts beperkt gericht informatie gezocht wordt. De CTIVD heeft dit ook benoemd als een aandachtspunt en is geen voorstander van het gebruik van generieke identiteiten in het selectieproces, vanwege het grote privacyrisico.

Omdat met de toepassing van deze bevoegdheid veel risico’s optreden, is het noodzakelijk hier in strengere waarborgen te voorzien. Er ontbreekt echter enige vorm van waarborg om toe te zien dat de uitoefening daadwerkelijk noodzakelijk en proportioneel is, wat des te problematischer is omdat de enige natuurlijke drempel – potentieel tegenwicht door de gegevensverwerker – wegvalt. Omdat zelfs het algemene normeringskader van art. 23-24 niet van toepassing is, is het op basis van het wetsvoorstel mogelijk om eenieder te verzoeken rechtstreekse toegang te verlenen tot alle mogelijke gegevens voor onbepaalde tijd; maar ook al zou dat algemene normeringskader, zoals hierboven geconcludeerd, van toepassing worden op de algemene bevoegdheid, dan volstaat dat niet om de privacyrisico’s van lid 3, de geautomatiseerde toegang, te compenseren. Juist de potentieel grote omvang van de hoeveelheid gegevens die met deze bevoegdheid verkregen kan worden noopt ertoe extra zorgvuldig te zijn in de afweging om gegevens van derden te verkrijgen op geautomatiseerde wijze. Het verwerken van gegevens over meer personen dan alleen targets zal gezien de aard van de bevoegdheid immers meer regel dan uitzondering zijn.

Daarom zijn voor de uitoefening van de algemene bevoegdheid in de vorm van artikel 22 lid 3 zwaardere eisen nodig qua toestemming, duur en omvang. Voor rechtstreekse, geautomatiseerde toegang is ten minste toestemming op het niveau van het diensthoofd nodig, zolang de bevraging in andere opzichten (qua duur en omvang) beperkt is. Zodra de geautomatiseerde toegang echter omvattender is – in de vorm van databanken die gegevens over heel veel burgers bevatten, of bijzonder gedetailleerde gegevens, dan wel als de toegang structureel voor langere tijd is – zou de toestemming eerder op het niveau van de minister moeten liggen. Bovendien zou in deze gevallen ook sprake moeten zijn van onmiddellijk toezicht door de CTIVD, om te kunnen toetsen of er niet teveel informatie over anderen dan targets verkregen wordt en of de inzet en de duur van de toepassing van de

bevoegdheid inderdaad noodzakelijk en proportioneel is voor de uitvoering van de wet.

### *5.1.4 Bewaartermijn informanten*

Een aanvulling ten opzichte van art 17 Wiv 2002 is lid 5. Dit lid is in het huidige artikel 17 Wiv 2002 niet opgenomen en gaat over de bescherming van informanten. Lid 5 bepaalt dat gegevens die een natuurlijke persoon identificeren die op heimelijke wijze meegewerkt heeft aan het verstrekken van gegevens ingevolge lid 1 30 jaar na de beëindiging van de medewerking worden vernietigd. Het betreft hier dus de gegevens over informanten van de diensten. Hierover zegt de MvT dat menselijke bronnen absolute geheimhouding wordt toegezegd en gegevens omtrent deze personen nimmer (ook niet na overlijden) ter beschikking van derden mogen worden gesteld. In het wetsvoorstel is gekozen voor een langere termijn waarna de gegevens dienen te worden vernietigd, namelijk 30 jaar, dan in de Wet politiegegevens het geval is (in casu 10 jaar). Bij de keuze voor een langere termijn speelt met name een rol dat tegenover de plicht om de identiteit van betrokkene geheim te houden ook de plicht bestaat om, als naar aanleiding van zijn werkzaamheden voor een dienst bij betrokkene (alsnog) klachten ontstaan, deze zo goed mogelijk daarin bij te kunnen staan en hulp te kunnen bieden (MvT, p. 28).

30 jaar is een erg lange bewaartermijn, die is gebaseerd op de redenering dat de gegevens ook nodig kunnen zijn om een informant later te kunnen beschermen indien zich problemen voordoen naar aanleiding van haar rol als informant. De regeling is vergelijkbaar met de regeling voor politie-informanten in de Wet politiegegevens. In die regeling is een termijn van 10 jaar vastgesteld. De MvT noemt de voorgestelde termijn van 30 jaar voldoende ruim in het licht van praktijkervaringen, maar het blijft onduidelijk waarom dan voor 30 jaar (en niet bijvoorbeeld 10, 15 of 20 jaar) wordt gekozen; voorbeelden van gevallen waarin de beschikbaarheid na 25 jaar nog relevant is, ontbreken. Aangezien er een groot belang (en een grote verantwoordelijkheid) is om de identiteit van informaten geheim te houden en dus ook te voorkomen dat gegevens dus ook op welke wijze dan (via hackers, klokkenluiders of nalatige medewerkers) kunnen lekken, lijkt eerder een kortere bewaartermijn aangewezen dan een zo lang mogelijke termijn. De beste bescherming tegen datalekken is immers het vernietigen van gegevens. Het belang van beschikbaarheid van gegevens om de betrokkene bij klachten te helpen, zal ook afnemen met het verstrijken van de tijd.

In dat licht verdient het aanbeveling om een aanzienlijk kortere bewaartermijn te hanteren, dan wel om veel scherper de noodzaak te onderbouwen waarom de gegevens nog tot 30 jaar na dato beschikbaar zouden moeten blijven.

## 5.2 Open source intelligence (OSINT)

### *5.2.1 Inleiding*

Het vergaren van informatie uit open bronnen wordt vaak aangeduid als *open source intelligence* (OSINT). Het is uit de aard der zaak een belangrijke informatiebron van inlichtingen- en veiligheidsdiensten, die van oudsher naar de gangbare opvatting geen privacyinbreuk opleverde – het gaat immers om publiek toegankelijke gegevens, oftewel om gegevens waar iedereen, en dus ook de diensten, toegang toe kan verkrijgen. Met de komst van het Internet in het algemeen, en sociale media in het bijzonder, heeft OSINT echter een nieuwe dimensie gekregen, die het relevant maakt er apart aandacht aan te besteden.

Zoals het EHRM heeft opgemerkt, 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.[39] Daarom wordt ook de systematische verzameling van informatie over personen, ook wanneer deze uit publiek toegankelijke bronnen afkomstig is, beschouwd als een inbreuk op het recht op privacy. OSINT moet daarom ook voldoen aan de vereisten van art. 8 lid 2 EVRM.
In het wetsontwerp is er geen zelfstandige bepaling over het verzamelen en analyseren van gegevens uit openbare bronnen. Indirect zijn de volgende bepalingen van toepassing.

**Paragraaf 3.1. Algemene bepalingen**
Artikel 17

1. De diensten zijn bevoegd tot het verwerken van gegevens met inachtneming van de eisen die daaraan bij of krachtens deze wet of de Wet veiligheidsonderzoeken zijn gesteld.
2. De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken.
3. De verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze.
4. De gegevens die in het kader van de taakuitvoering van de diensten worden verwerkt, zijn voorzien van een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan de gegevens zijn ontleend.

**Paragraaf 3.2.2.9 Afwegingskader en verslaglegging**
Artikel 43 [cursivering toegevoegd]

1. De uitoefening van een bevoegdheid als bedoeld in paragraaf 3.2.2 is slechts geoorloofd, *indien de daarmee beoogde verzameling van gegevens niet of niet tijdig kan geschieden door raadpleging van voor een ieder toegankelijke informatiebronnen* of van informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend.
2. Indien is besloten tot het verzamelen van gegevens door uitoefening van een of meer bevoegdheden als bedoeld in paragraaf 3.2.2, wordt slechts die bevoegdheid uitgeoefend, die gelet op de omstandigheden van het geval, waaronder de ernst van de bedreiging van de door een dienst te beschermen belangen, mede in vergelijking met andere beschikbare bevoegdheden voor de betrokkene het minste nadeel oplevert.
3. De uitoefening van een bevoegdheid blijft achterwege, indien de uitoefening ervan voor betrokkene een onevenredig nadeel in vergelijking met het daarbij na te streven doel oplevert.
4. De uitoefening van een bevoegdheid dient evenredig te zijn aan het daarmee beoogde doel.

De Memorie van Toelichting besteedt geen zelfstandige aandacht aan het verzamelen of analyseren van data uit open bronnen als informatiebron van de diensten. Op drie indirecte verwijzingen na (die hier niet relevant zijn), staat alleen een passage over het monitoren van sociale media bij de toelichting over

[39] EHRM 4 mei 2000, Rotaru t. Roemenië, §43, later bevestigd in EHRM 25 mei 2011, Association "21 Decembre 1989" en anderen t. Roemenië, §168.

observatie (art. 25): ‘Echter ook anderszins kan sprake zijn van observatie. Zo is het regelmatig of continu raadplegen van hetgeen door een persoon op door hem gebruikte social media (twitter, Facebook e.d.) wordt geplaatst eveneens aan te merken als een vorm van (on line) observatie, waarvoor dus toestemming dient te zijn verkregen’ (p. 38). Onduidelijk is daarbij echter of dat slaat op het raadplegen van voor eenieder toegankelijke informatie op sociale media (dus gegevens waarbij het profiel ‘open’ staat), of op gegevens op een gesloten profiel, waarbij de gegevens verzameld worden door via een nepprofiel vriend of volger te worden van de te observeren persoon.[40]

### *5.2.2 Analyse en beschouwing OSINT*

Het feit dat gegevens online beschikbaar zijn, wil niet zeggen dat de persoonlijke levenssfeer niet geraakt wordt door het raadplegen, opslaan en verwerken van deze gegevens, zoals ook bevestigd door het EHRM. Evenmin betekent het feit dat veel mensen veel over zichzelf op Internet zetten, dat zij daarmee hun privacy opgeven. Veelal hebben ze daarbij nog steeds een zekere privacyverwachting, die samenhangt met de context waarbinnen de gegevens online worden gezet: men verwacht dat vrienden en volgers de informatie lezen, maar niet direct dat vijanden (zoals identiteitsdieven) of vreemden (zoals overheden) dat doen. Soms is een dergelijke verwachting naïef, maar soms ook, naar maatschappelijke maatstaven, gerechtvaardigd, omdat sociale relaties samenhangen met reële verwachtingen van contextuele integriteit.[41]

Bij OSINT worden veelal persoonsgegevens verwerkt, wat een inbreuk op de privacy oplevert – vooral, maar niet alleen, de opslag ervan en het gebruik bij beoordelingen over personen. Vaak zal die inbreuk gerechtvaardigd zijn, mits aan de eisen van artikel 8 lid 2 EVRM is voldaan. Bij de beoordeling of OSINT de toets van artikel 8 EVRM kan doorstaan, moet voorop worden gesteld dat OSINT, afhankelijk van de omvang en intensiteit, een aanzienlijke inbreuk op de privacy kan opleveren, ook al gaat het om publiek toegankelijke gegevens. De enorme hoeveelheid gegevens die op Internet beschikbaar zijn kunnen, in combinatie, een indringend beeld van iemands persoonlijke leven geven.[42] Daarbij moet in aanmerking worden genomen dat lang niet alle gegevens door personen zelf online worden gezet; veel gegevens worden publiek gemaakt door vrienden (of ‘vrienden’), familie en collega’s, of door overheden of andere instituties. Ook moet worden meegewogen dat het verzamelen van gegevens uit open bronnen tot grote hoogte geautomatiseerd kan worden (Google doet niet anders, en veiligheidsdiensten hoeven in dat opzicht niet veel voor Google onder te doen), waarbij de gegevens

---

[40] De CTIVD besteedt hier aandacht aan in Toezichtsrapport 39, aangevend dat ‘wanneer daadwerkelijk een gefingeerde identiteit of hoedanigheid wordt geconstrueerd, hetgeen verder gaat dan het enkele gebruik
van een alias’, dit moet worden beschouwd als de inzet van een agent, waarvoor de procedure van artikel 21 Wiv 2002 (dekmanteloperaties, art. 26 Wiv 20xx) geldt (CTIVD 2014b, p. 11). De MvT gaat niet in op deze problematiek; het zou wenselijk zijn als de MvT zou uitleggen of het standpunt van de CTIVD in dezen wordt overgenomen, en aan de hand van voorbeelden nader zou uitleggen waar de grens ligt tussen ‘het enkele gebruik van een alias’ en ‘het construeren van een gefingeerde identiteit of hoedanigheid’.

[41] Zie uitgebreid Nissenbaum 2010.

[42] Vergelijk in dit verband ook de overwegingen in de uitspraak van het Duitse Constitutionele Hof over Trojaanse politiepaarden (‘Bundestrojaner’), BVerfG 27 februari 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007, beschikbaar op http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, Engelse vertaling: http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html.

ook nog geautomatiseerd gefilterd, gecombineerd, opgepoetst en inzichtelijk gepresenteerd kunnen worden. Het gevolg hiervan is dat het Internet en sociale media een goudmijn van informatie vormen.

De daarmee gepaard gaande privacyrisico's zijn aanzienlijk, in de eerste plaats omdat een indringend beeld van iemands privéleven kan worden gevormd op basis van open bronnen. Daarnaast zijn de risico's ook aanzienlijk omdat het ontstane beeld ook vertekend of onjuist kan zijn (lang niet alles wat op Internet staat, is 'waar'), wat ertoe kan leiden dat de verkeerde personen in beeld komen bij de diensten en onderworpen worden aan nadere onderzoekshandelingen. Nu zijn fout-positieven inherent aan het werk van inlichtingen- en veiligheidsdiensten, die er zelf ook belang bij hebben het percentage fout-positieven zo klein mogelijk te houden (mits dat niet te veel ten koste gaat van het percentage fout-negatieven, dat wil zeggen de mensen die ten onrechte *niet* in beeld komen bij de diensten); maar dat doet niets af aan het privacyrisico voor degenen die als fout-positief toch onderwerp worden van onderzoek hoewel ze feitelijk geen bedreiging vormen voor de nationale veiligheid.

Dit betekent dat het gebruik van OSINT genormeerd dient te worden. De vraag is of de Wiv 20xx voldoende doet aan normering van OSINT. Onzes inziens is dat niet het geval, omdat het verzamelen van gegevens uit open bronnen niet wordt gezien als een bevoegdheid van de diensten, maar als een geïmpliceerde informatiebron die als zodanig geen normering behoeft. Dat blijkt uit artikel 43 lid 1, waarin het verzamelen van openbroninformatie als (te prefereren) alternatief voor het gebruik van een bevoegdheid uit paragraaf 3.2.2 – de bijzondere bevoegdheden – wordt gesteld, en uit artikel 22, dat als algemene bevoegdheid bepaalt dat de diensten zich voor het verzamelen van gegevens kunnen wenden tot bestuursorganen, ambtenaren en personen (maar niet tot 'het Internet' of andere open bronnen).[43] Het zelfstandig verzamelen van gegevens uit open bronnen wordt dus niet als bevoegdheid beschouwd.

Daarbij doen zich twee problemen voor. Ten eerste moeten privacyinbreuken bij wet voorzienbaar zijn. Zonder specifieke regeling voor OSINT is het minder voorzienbaar dat, en hoe, de diensten persoonsgegevens uit open bronnen verzamelen en gebruiken; waar dit stelselmatig gebeurt, en zeker als het ondersteund wordt door geautomatiseerde data-analyse, is het de vraag of de substantiële privacyinbreuk die dat met zich meebrengt, wel voldoende voor burgers voorzienbaar is. Voor het stelselmatig verzamelen en verwerken van data uit open bronnen door de politie, is er discussie of de algemene taakstelling van de politie (art. 3 Politiewet 2012) wel een afdoende wettelijke grondslag biedt; wat ons betreft is dat niet zo, als het gaat om het gedurende langere tijd, zeer gericht of breed, of met aanzienlijke automatisering verzamelen van gegevens over specifieke personen.[44] Een vergelijkbare redenering kan men geven voor de ivd's: biedt de algemene taakstelling van de diensten (art. 8 lid 2 en art. 10 lid 2) in combinatie met de algemene bepaling dat de diensten bevoegd zijn tot verwerking van gegevens (art. 17) wel een voldoende grondslag voor (stelselmatige) OSINT? Dat is niet

[43] Zie ook MvT, p. 32: 'kan het onder omstandigheden noodzakelijk zijn om (aanvullende) gegevens te kunnen verzamelen, die niet via de algemene bevoegdheid tot gegevensverzameling *of* uit open bronnen is [sic] te verkrijgen' (cursivering toegevoegd); gegevens kunnen, behoudens bijzondere bevoegdheden, dus worden verzameld hetzij via de algemene bevoegdheid van art. 22 hetzij uit open bronnen.
[44] Zie Koops 2012.

uitgesloten: anders dan bij de politie, waarbij de burger niet hoeft te verwachten (en in elk geval veelal niet zal verwachten) dat deze systematisch gegevens van het Internet verzamelt en combineert, ligt het bij inlichtingen- en veiligheidsdiensten voor de hand dat zij zich, uit de aard van hun werk, bezig houden met het stelselmatig monitoren van het Internet. Het zou de kenbaarheid ten goede komen als er een specifieke regeling werd getroffen voor OSINT, omdat dit veel duidelijker voor burgers is dan een impliciete bevoegdheid in te lezen in de algemene taakstelling van de diensten in artikelen 8 en 10.

Het tweede probleem is wezenlijker en noodzaakt in elk geval tot een expliciete bevoegdheidsregeling. Omdat OSINT niet als bevoegdheid wordt geregeld, maar als een soort natuurlijke informatiebron, wordt het verzamelen en verwerken van data uit open bronnen niet op dezelfde manier genormeerd als de overige dataverwerking door de diensten. De verwerking van data uit open bronnen moet voldoen aan de eisen van artikel 17: doelbinding (lid 2), wetsconform, behoorlijk en zorgvuldig (lid 3) en met een bronindicatie (lid 4). De verwerking hoeft echter niet te voldoen aan de eisen van artikel 43, dat slechts van toepassing is op gegevens verkregen met behulp van bijzondere bevoegdheden. Vanwege de mogelijke verwarring of de wettelijke eisen van proportionaliteit en subsidiariteit (expliciet vastgelegd in art. 43) wel of niet ingelezen moeten worden in het begrip ‘noodzakelijk (…) voor een goede uitvoering van deze wet’ van art. 17 lid 2, bestaat een risico dat OSINT toegepast zou kunnen worden zonder dat een expliciete proportionaliteits- of subsidiariteitstoets wordt uitgevoerd (zie hierover verder par. 4.1.3).

Daar komt bij dat de subsidiariteit van OSINT wel op een andere wijze is geregeld, namelijk in artikel 43 lid 1, dat aangeeft dat een bijzondere bevoegdheid alleen mag worden ingezet als open bronnen[45] niet volstaan. Dit komt erop neer dat de wet bepaalt dat het verzamelen van gegevens uit open bronnen *altijd*, per definitie, minder ingrijpend wordt geacht voor de privacy dan het verzamelen van gegevens met een bijzondere bevoegdheid. Dit ongeacht de hoeveelheid of het type informatie dat wordt verzameld, en ongeacht de bijzondere bevoegdheid.

Dit levert een hoog privacyrisico op, omdat als de diensten bepaalde informatie willen verkrijgen, ze altijd eerst moeten proberen deze informatie te verkrijgen door OSINT of het opvragen van gegevens bij derden. Dat kan gepaard gaan met grootschalige dataverzameling en -analyse, die veel meer informatie kan bevatten dan bijvoorbeeld een kortdurende observatieactie (art. 25) of een gerichte informatievraag aan een agent (art. 26). Bovendien kunnen bij gebruik van OSINT of algemene dataverzameling op basis van art. 22 ook makkelijk gegevens over andere personen terecht komen in de databanken van de diensten, die niet verzameld hoeven te worden bij inzet van een meer gerichte bijzondere bevoegdheid.

[45] Of ‘informatiebronnen waarvoor aan de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend’ (art. 43 lid 1). Ons is niet duidelijk wat hiermee wordt bedoeld; het wordt niet toegelicht in de MvT. Voor zover hiermee (mede) gedoeld wordt op bestanden waartoe de dienst rechtstreeks geautomatiseerde toegang heeft op basis van een verzoek ex artikel 22 lid 3, geldt daarvoor dezelfde redenering als wij hier voor OSINT geven: een dergelijke toegang is zeker niet per definitie altijd minder ingrijpend (in de zin van subsidiariteit en proportionaliteit) dan de inzet van bepaalde ‘bijzondere’ bevoegdheden.

Onzes inziens kan niet op voorhand worden gesteld dat OSINT of het verzamelen van bestaande gegevens bij derden altijd minder inbreuk op de privacy oplevert dan een bijzondere bevoegdheid; integendeel: dat is sterk contextafhankelijk. De absolute subsidiariteit die in artikel 43 lid 1 wordt gestipuleerd zou daarom moeten komen te vervallen, terwijl de algemene eisen van subsidiariteit en proportionaliteit van artikel 43 niet alleen op de bijzondere bevoegdheden, maar evenzeer op de algemene bevoegdheid en op het verzamelen van gegevens uit open bronnen van toepassing zouden moeten zijn—hetgeen zou moeten worden geëxpliciteerd in de toelichting bij artikel 17 (zie par. 4.1.3).

Ook valt niet in te zien waarom andere waarborgen van de algemene bepalingen (art. 23-24) en uit het afwegingskader (stoppen als het doel is bereikt (art. 44) en verslaglegging (art. 45)) beperkt zijn tot bijzondere bevoegdheden. Evenals bij de algemene bevoegdheid geldt dat de privacyinbreuk bij OSINT, potentieel groot is, en, afhankelijk van de uitvoering ervan, ingrijpender kan zijn dan bijvoorbeeld het onderzoek van plaatsen of het verzamelen van verkeersgegevens.

Het is begrijpelijk dat een simpele raadpleging van open bronnen – elke medewerker zal wel eens relevante informatie over personen op Internet zoeken – inherent is aan het werk van de diensten en bij incidenteel gebruik geen nadere normering behoeft; zodra echter de gegevensvergaring uit open bronnen een stelselmatig karakter krijgt – gericht zoeken naar informatie uit meerdere bronnen over een target op meer dan incidentele basis – ontstaat er wel een noodzaak tot nadere normering, vanwege de hierboven aangegeven privacyrisico's in combinatie met het noodzakelijkheidsvereiste van artikel 8 EVRM.

Daarom zou het wetsvoorstel een zelfstandige grondslag moeten bevatten voor het stelselmatig vastleggen van gegevens uit open bronnen, in de vorm van een bijzondere bevoegdheid die aan het algemene normeringskader voor bijzondere bevoegdheden (art. 23-24, 43-45) is onderworpen. Daarmee kunnen de subsidiariteit, proportionaliteit en noodzaak van deze vorm van gegevensverwerking expliciet worden gewaarborgd. Daarnaast zijn echter, zoals we hieronder voor de specifiekere vorm van het monitoren van sociale media aangeven (zie par. 7.1.5), zwaardere eisen nodig aan het toestemmingsniveau, de duur van uitoefening en (bij langere duur) toezicht tijdens de uitoefening wanneer het vastleggen van gegevens uit open bronnen over een lange periode plaatsvindt, wanneer met geautomatiseerde hulpmiddelen Internet-breed iemand in kaart wordt gebracht, of wanneer met nepprofielen de (semi-)besloten delen van sociale media worden gemonitord.

## 5.3 Geautomatiseerde data-analyse

### *5.3.1 Inleiding*

De diensten zijn op grond van artikel 47 van het wetsvoorstel bevoegd tot geautomatiseerde data-analyse. Deze vorm van het verwerken van gegevens is in de huidige maatschappij een veel gebruikte technologie en in het kader van Big Data is vaak een vorm van geautomatiseerde analyse nodig om informatie uit gegevens te halen of ten minste een selectie van gegevens te maken. Geautomatiseerde data-analyse vindt plaats in alle sectoren van de samenleving en ook inlichtingen- en veiligheidsdiensten passen de technologie in verschillende vormen toe.

**Paragraaf 3.3 Bijzondere bepalingen inzake geautomatiseerde data-analyse**
Artikel 47

1. De diensten zijn bevoegd om geautomatiseerde data-analyse toe te passen met betrekking tot:
   a. gegevens uit eigen geautomatiseerde gegevensbestanden,
   b. gegevens uit voor een ieder toegankelijke informatiebronnen,
   c. gegevens uit geautomatiseerde gegevensbestanden waartoe de diensten rechtstreeks geautomatiseerde toegang hebben, en
   d. gegevens uit door derden verstrekte geautomatiseerde gegevensbestanden.

2. Ten behoeve van de verwerking van de gegevens als bedoeld in het eerste lid kunnen de gegevens in ieder geval:
   a. op geautomatiseerde wijze onderling met elkaar worden vergeleken, dan wel in combinatie met elkaar worden vergeleken,
   b. worden doorzocht aan de hand van profielen, en
   c. worden vergeleken met het oog op het opsporen van bepaalde patronen.
3. Het bevorderen of treffen van maatregelen jegens een persoon uitsluitend op basis van de resultaten van een gegevensverwerking als bedoeld in het tweede lid, aanhef en onder b, is niet toegestaan.

De bevoegdheid tot geautomatiseerde data-analyse moet gezien worden in het licht van de algemene vereisten die in het wetsvoorstel zijn opgenomen om tot een zorgvuldige verwerking te komen (art. 17). Op grond van datzelfde artikel zijn de diensten bevoegd tot het verwerken van gegevens met behulp van geautomatiseerde data-analyse. Een expliciete wettelijke grondslag voor deze werkmethode ontbrak echter nog. In het wetsvoorstel is ervoor gekozen om deze te creëren in artikel 47 (MvT, p. 102). Deze regeling moet overigens ook in combinatie worden gezien met de regeling voor metadata-analyse (artikel 35 lid 1 onder b). Gegevensverwerking is de kernactiviteit van de inlichtingen- en veiligheidsdiensten. Aangezien het door de toegestane bronnen onvermijdelijk is dat ook gegevens over personen worden geanalyseerd die niet de aandacht van de diensten hebben, en die dus meegenomen kunnen worden in de geautomatiseerde analyse, geeft lid 5 van artikel 18 een wettelijke grondslag voor het verwerken van gegevens over deze personen ‘indien die gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden’ (MvT, p. 103).

In lid 3 van het artikel is bepaald dat het niet is toegestaan om uitsluitend op basis van resultaten van het doorzoeken van gegevens op basis van een profiel maatregelen jegens een persoon te bevorderen of treffen. Een profiel behelst veelal een samenstel van kenmerken die op basis van analyses of onderzoeken door de diensten zelf of door derden naar voren zijn gekomen. Het gaat hier om een dynamisch proces, waarbij gaandeweg profielen bijgesteld kunnen worden. Omdat het niet is toegestaan uitsluitend op basis van een dergelijke verwerking maatregelen te bevorderen of te treffen is met andere woorden vereist dat ook nog een menselijke afweging wordt gemaakt (MvT, p. 103).

### *5.3.2 Analyse en beschouwing geautomatiseerde data-analyse*

De bevoegdheid tot geautomatiseerde data-analyse is van toepassing op alle bronnen waar de diensten gegevens uit kunnen verkrijgen. Ook de wijze van analyseren is breed ingestoken. Er is een aantal voorbeelden opgenomen in lid 2 van het artikel, maar dit betreft een niet-limitatieve opsomming. Toekomstige wijzen van data-analyse zijn hiermee dus ook bij voorbaat afgedekt. Zowel een analyse waarbij gegevens vergeleken worden om verbanden of patronen te vinden als een analyse waarbij op basis van vooraf bepaalde profielen of kenmerken wordt gezocht is mogelijk.

Bij de bronnen waarop geautomatiseerde data-analyse mag worden uitgeoefend behoren ook open bronnen. De opmerkingen die hierboven ten aanzien van OSINT zijn gemaakt zijn dus eveneens van toepassing in dit verband. Daar komt als privacyrisico bij dat door geautomatiseerde data-analyse informatie zichtbaar wordt die niet zonder analysetechnieken is te herkennen, ook niet altijd door *intelligence*-specialisten. Bovendien kan de aldus gegenereerde informatie meer of minder juist zijn. Een algemene belangrijke kanttekening vanuit privacyperspectief bij profilering is dat dit kan leiden tot onterechte insluiting in bepaalde risicogroepen. Fout-positieven kunnen wel worden verminderd door zorgvuldige analyse en controle van gegevens door specialisten, maar zijn nooit volledig te vermijden. De gevolgen van een onterechte inclusie in een risicogroep (bijvoorbeeld iemand profileren als een potentiële jihadstrijder, terwijl deze feitelijk niet aan het radicaliseren is) kunnen zeer groot zijn, zowel voor de persoonlijke levenssfeer (als de op basis van het profiel ondernomen acties leiden tot interventies in diens sociale leven) alsook voor de effectiviteit van de diensten (als door de interventies iemand sociaal wordt uitgesloten en daardoor juist alsnog gaat radicaliseren).

Gezien de grote impact die het verbinden van gevolgen aan profilering door de inlichtingen- en veiligheidsdiensten kan hebben is bijzondere zorgvuldigheid geboden. Bovendien is het als gevolg van het type technologie en de databronnen waarop deze wordt toegepast inherent dat ook gegevens over (vele) personen die niet de aandacht van de diensten hebben worden verwerkt en geanalyseerd. Dit is erkend als probleem door deze categorie personen op te nemen in artikel 18 lid 5. Hoewel hiermee een wettelijke basis gecreëerd wordt, is daarmee niet gezegd dat ook voldaan is aan de andere vereisten die het EHRM stelt, zoals het vereiste van voorzienbaarheid in combinatie met proportionaliteit en subsidiariteit (zie daarover par. 4.2.2).

De inbreuk op de persoonlijke levenssfeer kan bij de toepassing van geautomatiseerd data-analyse in dezelfde zin aan de orde zijn als bij metadata-analyse (art. 35). Niet voor niets verwijst art. 35 (in lid 1 onder b en lid 4) naar art. 47 om het type gegevensverwerking aan te duiden. Het valt niet in te zien waarom bij metadata-analyse een intrinsiek snellere of grotere inbreuk op de privacy kan plaatsvinden dan bij geautomatiseerde data-analyse van andere typen gegevens. Weliswaar kunnen metadata bijzonder veel blootgeven over iemands persoonlijke levenssfeer (vandaar ook de relatief zware eisen van art. 35), maar dat geldt evenzeer voor andere databronnen (denk bijvoorbeeld aan financiële gegevens, aankoopgegevens, reisgegevens). Het feit dat de bron en het type gegevens verschillen, is in dit opzicht minder van belang dan het feit dat er in beide situaties grote hoeveelheden gegevens bij elkaar worden gestopt en daaruit met behulp van slimme algoritmes nieuwe informatie wordt gegenereerd. Daarom zou de normering

van geautomatiseerde data-analyse hetzelfde moeten zijn als bij metadata-analyse het geval is, wat betekent ministeriële toestemming vooraf.[46]

Tot slot kan nog worden gewezen op het algemene punt dat de MvT nauwelijks ingaat op hedendaagse en voorzienbare toekomstige technische ontwikkelingen. De regeling en toelichting lijken vooral uit te gaan van aloude vormen van *data mining* in grote bestanden. Het voorstel spreekt van het vergelijken van gegevens, het toepassen van profielen en het afleiden van patronen, alsof dit drie verschillende analysemethoden zijn. In feite zal bij de analyse van de diverse gegevensstromen steeds vaker gebruik worden gemaakt van machinaal leren, een vorm van kunstmatige intelligentie die zich niet tot dit soort statische onderscheidingen laat reduceren. De kern van machinaal leren is het vermogen van een computersysteem om de omgeving (hier datastromen) waar te nemen en de eigen prestaties (het afleiden van relevante patronen) voortdurend te verbeteren op basis van hernieuwde waarneming. Dat betekent dat gevonden patronen niet als statische profielen worden toegepast maar voortdurend worden getest, aangevuld en afgestemd, op basis van vergelijkingen in wiskundige zin, of liever op basis van wiskundige functies die permanent kunnen worden bijgesteld of zelfs gemuteerd om betere resultaten te verkrijgen. Daarbij kunnen zowel metadata als inhoudelijke analyse een rol spelen en kan data uit verschillende bronnen tot nieuwe inzichten leiden. De idee dat machinaal leren beter werkt als men meer data verzamelt is onjuist. Technisch gezien is het belangrijker om de juiste afwegingen te maken bij het ‘trainen’ van de desbetreffende algoritmes, waarbij het doel juist is om op basis van enkele datapunten relevant gedrag te kunnen voorspellen.

Het wetsvoorstel biedt volstrekt geen inzicht welke uitwerking machinaal leren zal hebben bij de uitoefening van de bevoegdheid van artikel 47, met name in het licht van het (zelf)lerende vermogen van algoritmes en de daarmee gepaard gaande toenemende moeilijkheid om te beoordelen op basis waarvan uitkomsten van geautomatiseerde data-analyses tot stand komen. De bovengeschetste risico’s van geautomatiseerde analyses worden versterkt door de opkomst van machinaal leren. De Memorie van Toelichting zou hier dan ook expliciet aandacht aan moeten besteden.

### *5.3.3 Geautomatiseerde beslissingen*

Lid 3 van het voorgestelde artikel 47 geeft een beperking in lijn met artikel 42 Wbp, inhoudende het verbod op geautomatiseerde beslissingen. Een geautomatiseerde gegevensverwerking op zich mag geen grond zijn voor het nemen van een beslissing waaraan rechtsgevolgen zijn verbonden of dat de persoon in aanmerkelijke mate treft. Volgens de MvT betekent dit dat altijd een menselijke afweging is vereist. Het is echter wel de vraag hoe dit uitwerkt en wat de reikwijdte van het ‘bevorderen of treffen van maatregelen’ is. Men mag aannemen dat dit ook, en vooral, het inzetten van nadere bevoegdheden gericht op een persoon betreft, maar dat wordt niet expliciet benoemd. Het is niet duidelijk of het ook minder directe maatregelen betreft, zoals het nader onderzoeken van (bepaalde aspecten van) een persoon op basis van open bronnen, of het vastleggen van een profiel in een bestand met een bepaalde markering (bijvoorbeeld dat een persoon aan een bepaald profiel voldoet). Aangezien ook dit type handelingen uiteindelijk effect kan hebben op hoe de diensten een bepaalde persoon behandelen, zouden ook deze

[46] Zoals ook aangeven door de CTIVD in haar reactie op het wetsontwerp, zie CTIVD 2015c, p. 49.

onder de bepaling moeten vallen. Dit zou nader uitgewerkt moeten worden in de toelichting.

Hoewel het vereisen van menselijke tussenkomst een logische en gewenste benadering is, blijft hier wel een groot risico bestaan dat te gemakkelijk op de uitkomsten van geautomatiseerde data-analyse en in het bijzonder het matchen van profielen voortgebouwd wordt. Er is immers een match gevonden op basis van een vooraf opgesteld profiel. Het in twijfel trekken van een dergelijke match of ten minste constateren dat iemand die aan een profiel voldoet geen aandacht van de diensten behoeft, lijkt misschien eenvoudiger dan het in werkelijkheid zal zijn. Niet alleen wordt er vaak vertrouwd op de uitkomst van een computerbewerking omdat het lijkt dat het om een objectieve 'berekening' gaat (waarbij wordt miskend dat de uitkomst afhangt van de input en van het algoritme, die beiden niet neutraal of onbevooroordeeld hoeven te zijn); ook wordt het steeds moeilijker om te beoordelen hoe de uitkomst van geautomatiseerde data-analyse tot stand is gekomen, vanwege de complexiteit en obscuriteit van algoritmes (onder andere door de opkomst van machinaal leren). Het is daarom de vraag of, en in welke gevallen, de uitkomst van geautomatiseerde data-analyse als zodanig in twijfel zal worden getrokken. Veeleer zal er eerder een aanleiding in een match gevonden worden om wat nader onderzoek te verrichten met degene die aan het profiel voldoet als specifieke target. Het is niet duidelijk welke omvang dit nadere onderzoek zou moeten hebben om te kunnen spreken van het treffen van maatregelen 'uitsluitend op basis van' geautomatiseerde data-analyse. Enige richting voor de interpretatie van de vereiste menselijke tussenkomst wordt wel gegeven in het voorstel voor de Algemene Verordening Gegevensbescherming. Artikel 20 van dit voorstel gaat over geautomatiseerde beslissingen en hierbij wordt aangegeven dat ook na menselijke tussenkomst het bevorderen en treffen van maatregelen ten aanzien van een specifieke persoon of specifieke personen niet alleen gegrond mag zijn op computationeel afgeleide profielen.[47]

Aangezien het gebruik van generieke identiteiten bij geautomatiseerde data-analyse niet wenselijk is en ervan uitgegaan moet worden dat de diensten met een specifiek doel een analyse op gegevens toepassen, zullen de profielen die op basis van lid 2 sub b worden gebruikt normaliter een aantal specifieke kenmerken bevatten, op grond waarvan het ook mogelijk is om gegevens over personen uit een grote dataset te selecteren. De kenmerken worden dan rechtstreeks gekoppeld aan de personen die op basis van het profiel uit de gegevensset naar voren komen. Het herkennen van personen als zijnde personen die aan het profiel voldoen kan daarom al een grote inbreuk op de persoonlijke levenssfeer opleveren. Deze inbreuk zal dus ook gelden voor personen die niet de aandacht van de diensten hebben, althans niet zouden moeten hebben, maar die als gevolg van de toepassing van de bevoegdheid van geautomatiseerde data-analyse ook in beeld komen. Vanwege het gevaar dat er onterecht wordt vertrouwd op de uitkomst van geautomatiseerde data-analyse, is het maar de vraag of het wetsontwerp voldoende rekening houdt met de gevolgen die fout-positieven in geautomatiseerde data-analyse kunnen hebben voor personen die onterecht in beeld komen.

Volgens de MvT houdt de bepaling in dat ook nog een menselijke afweging is vereist. In het artikel zelf is dit echter niet als zodanig benoemd. De bepaling laat de

[47] Toelichting bij Voorstel voor een Algemene Verordening Gegevensbescherming, versie Europees Parlement.

ruimte om op basis van de resultaten van genoemde analyse en willekeurig welke andere bron wel maatregelen jegens een persoon te bevorderen of treffen; letterlijk genomen kan dat dus ook betekenen dat wel maatregelen mogen worden getroffen op basis van twee of meer verschillende exercities van geautomatiseerde data-analyse, wat bijvoorbeeld ook verschillende metadata-analyse van communicatiegegevens op basis van artikel 35 zou kunnen omvatten. Dit kan niet de bedoeling van dit artikel zijn. Aanbevolen wordt dan ook om de formulering aan te passen zodat duidelijk is dat maatregel niet mogen worden getroffen of bevorderd louter gebaseerd op één of meer automatische verwerkingen. Daarnaast zou in de toelichting meer uitgewerkt moeten worden waaruit de menselijke tussenkomst zou moeten bestaan, om afdoende het risico te beperken dat te snel op de uitkomsten van geautomatiseerde data-analyse wordt vertrouwd.

## 5.4 Delen van gegevens met buitenlandse diensten

Samenwerking met buitenlandse diensten is van belang, omdat op deze wijze voor de nationale veiligheid van Nederland belangrijke informatie kan worden verkregen. In het metier van inlichtingen- en veiligheidsdiensten is immers bij de uitwisseling van informatie het beginsel van ‘quid pro quo’ (voor wat hoort wat) een belangrijk element: zonder wederkerigheid geen informatie (MvT, p. 135).

In paragraaf 6.2 van het wetsvoorstel is het (deels nieuwe) kader voor samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten opgenomen. Het betreft de bepalingen 76-78. Achtereenvolgens gaan deze artikelen over het aangaan van samenwerkingsrelaties met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen, het verstrekken van gegevens in het kader van een dergelijke samenwerkingsrelatie, en verzoeken tot technische of andere vormen van ondersteuning door diensten van andere landen.

### *5.4.1 Aangaan van samenwerkingsrelaties*

Artikel 76

1. De diensten zijn bevoegd tot het aangaan van samenwerkingsrelaties met daarvoor in aanmerking komende inlichtingen- en veiligheidsdiensten van andere landen.
2. Voorafgaand aan het aangaan van een samenwerkingsrelatie als bedoeld in het eerste lid weegt de dienst aan de hand van de criteria als bedoeld in het derde lid of kan worden overgegaan tot het aangaan van een samenwerkingsrelatie en, zo ja, wat de aard en intensiteit van de beoogde samenwerking kan zijn.
3. Bij de weging als bedoeld in het tweede lid worden in ieder geval de volgende criteria betrokken:
   a. de democratische inbedding van de dienst in het desbetreffende land;
   b. de eerbiediging van de mensenrechten door het desbetreffende land;
   c. de professionaliteit en betrouwbaarheid van de desbetreffende dienst.
4. Een samenwerkingsrelatie met een inlichtingen- en veiligheidsdienst van een ander land wordt pas aangegaan, indien daartoe door Onze betrokken Minister toestemming is verleend. Onze betrokken Minister kan de bevoegdheid tot het verlenen van toestemming mandateren aan het hoofd van de dienst. Van een verleende toestemming door het hoofd van de dienst wordt Onze betrokken Minister zo spoedig mogelijk geïnformeerd.

5. Het hoofd van de dienst draagt er zorg voor dat indien omstandigheden daartoe aanleiding geven de aard en intensiteit van de samenwerkingsrelatie met een inlichtingen- en veiligheidsdienst van een ander land opnieuw wordt gewogen. Het tweede tot en met vierde lid is van overeenkomstige toepassing.

Artikel 76 is op meerdere punten gewijzigd ten opzichte van de huidige wet (art. 59 Wiv 2002).

Allereerst wordt in artikel 76 de bevoegdheid tot het aangaan van samenwerkingsrelaties, waar tot nu toe wordt gesproken over het (minder intensief klinkende) onderhouden van verbindingen. In lid 2 en 3 wordt aangegeven dat voor een samenwerkingsrelatie kan worden aangegaan, in elk geval getoetst moet worden op democratische inbedding, de eerbiediging van mensenrechten en de betrouwbaarheid en professionaliteit van de buitenlandse dienst. Voor de beoogde samenwerking is toestemming van de minister vereist of gemandateerde toestemming van het diensthoofd. De samenwerking wordt opnieuw afgewogen als omstandigheden daartoe aanleiding geven.

Volgens de MvT wordt met de criteria op grond waarvan een afweging dient te worden gemaakt en het verdere wettelijke kader voor het aangaan van samenwerkingen met buitenlandse diensten invulling gegeven aan de rapporten van de CTIVD en de aanbevelingen van de commissie-Dessens. De criteria van lid 3 zijn gebaseerd op rapport 22A van de CTIVD.[48] Voor het kunnen maken van de bedoelde weging is het nodig de daarvoor benodigde informatie te verkrijgen. Volgens de MvT (p. 138) kunnen de diensten daarbij gebruik maken van informatie uit open bronnen of uit de signalen die zij hebben verkregen vanuit eerdere samenwerking of vanuit de bredere internationale inlichtingengemeenschap. Ook de mate van transparantie die een buitenlandse dienst geeft in haar taken, bevoegdheden en werkwijze is een belangrijke factor. In de MvT (p. 139) wordt dit verbonden aan een methodiek om vast te stellen in hoeverre diensten democratisch zijn ingebed en mensenrechten respecteren. Onvoldoende transparantie is een sterke contra-indicatie voor samenwerking (p. 139). Hoewel transparantie hier als hulpmiddel bij beoordeling wordt voorgesteld, is het ook intrinsiek een belangrijk criterium. Het is in dat licht aan te bevelen het zelfstandig in de wettekst op te nemen in lid 3 onder c.

De weging die in artikel 76 van het wetsvoorstel wordt voorgeschreven is van groot belang. De genoemde criteria zijn geschikt om een goede weging te maken. Voor de diensten is het van belang om een goede weging te maken, aangezien zij zelf ook benadeeld kunnen worden door samenwerking met een dienst die niet professioneel of betrouwbaar blijkt te zijn, of als de samenwerking in opspraak komt wegens schending van mensenrechten in het desbetreffende land. Een objectieve weging is daarbij essentieel. Er is echter ook ruimte voor politieke belangen in het wettelijk kader ingebouwd: ‘De huidige diffuse dreigingssituatie vereist soms contacten met diensten die niet aan alle eisen voldoen’ (MvT, p. 139). Er bestaat dus de mogelijkheid om, ook als uit de weging blijkt dat samenwerking met een dienst een risico vormt vanwege één of meer van de genoemde criteria, toch een samenwerking aan te gaan, met toestemming van de verantwoordelijke minister. Hoe dit in de praktijk uitwerkt zal uiteindelijk bepalen hoe groot de waarborgen zijn die nu in het wettelijk kader worden opgenomen. Indien er risico’s bestaan door het

[48] CTIVD 2009. Zie inmiddels ook CTIVD 2015B.

niet (volledig) voldoen aan de criteria maar toch een samenwerking wordt aangegaan, zal het politieke belang van de samenwerking tussen landen zwaarder kunnen wegen dan de risico's – niet alleen politiek, maar juist ook voor de bescherming van mensenrechten – die uit de samenwerking voort kunnen komen. Het is in die zin maar de vraag welke invulling zal worden gegeven aan de genoemde criteria.

Edward Snowden heeft laten zien hoe de samenwerking tussen de VS en buitenlandse inlichtingendiensten bij grootschalige surveillance-programma's gepaard gaat met aanzienlijke inbreuken op de privacy. De Amerikaanse wetgeving discrimineert 'between the protections afforded by the US constitution to US citizens, and everybody else',[49] wat de privacybescherming beïnvloedt van de personen van wie data worden doorgegeven vanuit de EU naar de VS. Onlangs heeft het Europees Hof van Justitie onderzocht of de 'safe harbour'-beginselen en de daaraan gerelateerde Frequently Asked Questions van het Amerikaanse Department of Commerce een passend niveau van bescherming bieden.[50] Het Hof herhaalde zijn vaste standpunt dat de 'protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary',[51] en dat 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life'.[52] Momenteel zijn drie procedures aanhangig bij het EHRM, waar de klagers stellen dat de generieke surveillance door de Britse inlichtingendienst, GCHQ en de ongeclausuleerde samenwerking van deze dienst met de Amerikaanse NSA een ongerechtvaardigde inbreuk maken op hun recht op privacy.[53] Dit onderstreept de noodzaak van een kader voor samenwerking dat gebaseerd is op naleving van mensenrechten, transparantie en de rechtsstaat.

Gezien de inbreuken op de persoonlijke levenssfeer die de inlichtingendiensten van de Verenigde Staten blijken te maken, en zoals deze via Snowden naar buiten zijn gekomen, kan inmiddels redelijkerwijs niet langer zonder meer geconcludeerd worden dat er bij samenwerking tussen Nederlandse en Amerikaanse inlichtingendiensten sprake is van een democratische inbedding, transparantie en naleving van mensenrechten vanuit het perspectief van het EVRM. Of deze conclusie ook door de diensten getrokken zou worden op basis van artikel 76 valt te bezien.[54] Zelfs indien dat het geval zou zijn, is het niet te verwachten dat de minister dit als doorslaggevend zal beschouwen in de beslissing al dan niet toestemming voor samenwerking te verlenen. De privacyrisico's die voortvloeien uit

[49] Caspar Bowden (2013), *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Report for the European Parliament, p. 20.
[50] EHJ 6 oktober 2015, Schrems (C-362/14) ECLI:EU:C:2015:650.
[51] EHJ 6 oktober 2015, Schrems (C-362/14) ECLI:EU:C:2015:650, §92.
[52] EHJ 6 oktober 2015, Schrems (C-362/14) ECLI:EU:C:2015:650, §94.
[53] Bureau of Investigative Journalism and Alice Ross vs. the United Kingdom, App. Nr. 62322/14, ingediend 11 september 2014; Joint application under Article 34, Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v the United Kingdom, App. No. 58170/13; Ten human rights organisations (the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v UK, nog geen aanvraagnummer beschikbaar.
[54] De Memorie van Toelichting (p. 137) noemt in navolging van de commissie-Dessens wel de 'discussies over de NSA', maar gaat niet in op de vraag tot welke conclusie kennis van de handelwijze van de NSA in het licht van deze criteria zou kunnen of moeten leiden.

de mogelijkheid om, ondanks risico's en een beoordeling die negatief uitpakt, toch een samenwerking aan te gaan kunnen dan ook aanzienlijk zijn. Om die privacyrisico's enigszins binnen de perken te houden, zal extern en politiek toezicht nodig zijn, maar vooral ook intern tegenwicht binnen de diensten, die zich door een cultuur van tegenspraak steeds zouden moeten afvragen of een specifieke handeling binnen een samenwerkingsverband wel te verantwoorden is.

Ook zal lid 5 in dit verband een belangrijke rol moeten spelen, dat het diensthoofd een zorgplicht oplegt om samenwerking te heroverwegen als daar aanleiding toe is. De MvT (p. 140) merkt daarbij op dat het een continu proces is om naar aanleiding van gewijzigde omstandigheden (positief of negatief) of voortschrijdend inzicht samenwerking te herzien. Het zou wenselijk zijn om in de wettekst explicieter tot uitdrukking te brengen dat het heroverwegen van samenwerking een doorlopend proces is. De formulering 'indien omstandigheden daartoe aanleiding geven' zou kunnen suggereren dat heroverweging alleen nodig is wanneer er iets gebeurd is – een incident, een rechtszaak, een rapport, een klokkenluideralarm –, terwijl het juist ook kan gaan om weinig zichtbare, graduele ontwikkelingen. Het is maar de vraag of gewijzigde 'omstandigheden' tijdig ontdekt worden als er niet actief de vinger aan de pols wordt gehouden. Dat bergt een privacyrisico in zich dat een samenwerking langer doorloopt dan verantwoord is. In dat licht zou lid 5 duidelijk moeten maken dat samenwerkingsverbanden *periodiek*, dan wel wanneer er door omstandigheden specifieke aanleiding toe is, heroverwogen moeten worden.

### *5.4.2 Verstrekking van gegevens en ondersteuning aan buitenlandse diensten*

Artikel 77

1. In het kader van een samenwerkingsrelatie als bedoeld in artikel 76 kunnen aan de desbetreffende dienst van een ander land gegevens worden verstrekt ten behoeve van door deze instanties te behartigen belangen, voor zover:

a. deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en

b. een goede taakuitvoering door de diensten zich niet tegen verstrekking verzet.

2. Voor zover de verstrekking van gegevens als bedoeld in het eerste lid betrekking heeft op ongeëvalueerde gegevens, vindt de verstrekking niet eerder plaats dan nadat Onze betrokken Minister daarvoor toestemming heeft verleend.
3. Op de verstrekking van gegevens als bedoeld in het eerste lid zijn de artikelen 51, 55 en 56 van overeenkomstige toepassing.
4. In het kader van een samenwerkingsrelatie als bedoeld in artikel 76 kunnen voorts op een daartoe schriftelijk verzoek aan de desbetreffende dienst technische en andere vormen van ondersteuning worden verleend ten behoeve van door deze instanties te behartigen belangen, voor zover:
   a. deze belangen niet onverenigbaar zijn met de belangen die de diensten hebben te behartigen, en
   b. een goede taakuitvoering door de diensten zich niet tegen de verlening van de desbetreffende vorm van ondersteuning verzet.

(…)

Artikel 77 regelt de verstrekking van gegevens en het verlenen van technische en andere vormen van ondersteuning aan buitenlandse collega-diensten ten behoeve van deze buitenlandse diensten. Hiervoor gelden dezelfde waarborgen als in de huidige wet (art. 59 Wiv 2002), behalve dat voor het verstrekken van

‘ongeëvalueerde’ gegevens (waarmee vooral gedoeld wordt op ’grote hoeveelheden (bulk)’, MvT, p. 107) toestemming van de minister nodig is (lid 2). Bij de verstrekking van gegevens aan buitenlandse diensten wordt (als wij de spaghetticonstructie juist lezen) de voorwaarde gesteld dat de ontvangende dienst de gegevens niet aan anderen mag verstrekken (art. 77 lid 3 j$^{o}$ 51 lid 2 j$^{o}$ 48 lid 1 onder d).

**Geëvalueerde gegevens (lid 1)**
De gegevens die verstrekt kunnen worden aan buitenlandse diensten betreffen primair gerichte gegevens waar al een analyse op heeft plaatsgevonden. De gegevens dienen immers betrekking te hebben op een specifiek doel. Dat doel dient vooraf beoordeeld te worden opdat er geen strijdigheid optreedt met de taken of belangen van de Nederlandse diensten. Hiervoor wordt, voor zover wij zien, geen toestemming vereist in de wet. Dat zou de MvT moeten motiveren en nader toelichten; wij nemen tenminste aan dat het niet de bedoeling is dat individuele medewerkers gebeld kunnen worden door een bevriende collega bij een buitenlandse dienst om wat gegevens op te sturen, en daar dan zelfstandig over zouden kunnen beslissen.

Het ontbreken van een toestemmingsvereiste lijkt ons problematisch, ook waar het gaat om gerichte en geëvalueerde gegevens, omdat het maar de vraag is of de verstrekking van deze gegevens verenigbaar is met het doel waarvoor ze door de Nederlandse diensten zijn verzameld. (Het gaat bij lid 1 immers niet om gegevens die op verzoek van de buitenlandse dienst met inzet van een bevoegdheid worden verzameld – zie daarover leden 4-6 – maar om gegevens die al aanwezig zijn bij de diensten.) De wet stelt hier geen concrete doelbindingseis. Artikel 17 lid 2 is van toepassing maar dat stelt slechts dat de verwerking, in casu de verstrekking, voor een bepaald doel moet geschieden, niet dat dit doel verenigbaar moet zijn met het oorspronkelijke doel waarvoor te verstrekken gegevens zijn verzameld.

Verder is de afweging voor verstrekking generiek, op het niveau van de belangen die diensten in het algemeen hebben te behartigen, niet in concreto op het niveau van het belang bij de te verstrekken gegevens. Lid 1 stelt dat deze algemene belangen van de buitenlandse diensten niet onverenigbaar moeten zijn met die van de Nederlandse dienst (sub a), terwijl het niet aannemelijk is dat de andere eis, namelijk dat de goede taakuitvoering van de Nederlandse dienst zich niet tegen verstrekking verzet (sub b) een toetsing aan doelbinding inhoudt. Uit de wetssystematiek lijkt daarom te volgen dat door de Nederlandse diensten verzamelde en geëvalueerde gegevens aan buitenlandse diensten verstrekt mogen worden, ook als het doel waarvoor de buitenlandse diensten de gegevens willen gebruiken, afwijkt van het doel waarvoor de gegevens in Nederland zijn verzameld. Als er geen nieuwe grondslag wordt gevonden voor de doelafwijkende verstrekking, is dat in strijd met de beginselen van gegevensbescherming. Het verstrekken van gegevens kan een belangrijk en specifiek, nieuw doel dienen, maar dat moet dan wel opnieuw worden gelegitimeerd. Op dit punt wreekt zich het ontbreken van een toestemmingsvereiste. Het wetsontwerp zou daarom moeten eisen dat de verstrekking alleen plaatsvindt met toestemming op het niveau dat nodig was voor de oorspronkelijke verzameling van de gegevens. Mogelijk is het niet altijd duidelijk op basis van welke bevoegdheid concrete gegevens zijn verzameld. Het is dan praktischer om de toestemmingeis van artikel 77 leden 5 en 6 ook van toepassing te verklaren op de gegevensverstrekking van lid 1.

Een ander zeer groot privacyrisico in de regeling betreft de spaghettikoppeling van artikel 77 aan artikel 55, dat in lid 2 een uitzondering biedt voor in art. 49 lid 1 onder d beschreven instanties, waarmee buitenlandse diensten worden aangeduid. Deze verwijzing betekent dat aan buitenlandse diensten ook gegevens mogen worden verstrekt 'waarvan de juistheid redelijkerwijs niet kan worden vastgesteld of die meer dan 10 jaar geleden zijn verwerkt, terwijl ten aanzien van de desbetreffende persoon sindsdien geen nieuwe gegevens zijn verwerkt' (art. 55 lid 1 j$^{o}$ lid 2). Weliswaar moeten de mate van (on)betrouwbaarheid en ouderdom bij de verstrekking worden gemeld (art. 55 lid 3), maar dat neemt niet weg dat onbetrouwbare en sterk verouderde gegevens kennelijk aan buitenlandse diensten verstrekt mogen worden. Dit levert grote privacyrisico's op voor betrokkenen over wie (mogelijk) onbetrouwbare of sterk verouderde gegevens kunnen worden verstrekt. Dit kan er bijvoorbeeld aan bijdragen dat zij op *no fly*-lijsten terecht komen, langdurig opgehouden worden op vliegvelden, of zelfs op basis van metadata-analyses doelwit worden van drone-aanvallen. Weliswaar zijn er geen concrete indicaties dat door Nederland verstrekte gegevens dergelijke gevolgen hebben, maar evenmin zijn er indicaties dat het uitgesloten is dat door Nederland verstrekte gegevens bijdragen aan dergelijke toepassingen. Evenals bij ongeëvalueerde gegevens (zie onder, waarmee de gegevens in art. 55 lid 1 een sterke verwantschap hebben maar vermoedelijk qua definitie niet mee samenvallen) lijkt ons een verstrekking van dergelijke gegevens onder de gegeven voorwaarden nauwelijks te rechtvaardigen. Het gaat immers om gegevens die hoogstwaarschijnlijk niet relevant zijn of waarvan de relevantie (vanwege de onbetrouwbaarheid) niet kan worden vastgesteld, en waarvan niet kan worden gecontroleerd op welke manier de buitenlandse dienst er gebruik van zal maken – de Nederlandse waarborgen zijn daarop niet van toepassing. Onzes inziens zouden deze gegevens daarom uitgesloten moeten worden van verstrekking aan buitenlandse diensten. Aangezien deze redenering evenzeer opgaat voor andere gevallen van verstrekking aan buitenlandse diensten (dus buiten samenwerkingsverbanden om), zou artikel 55 lid 2 onder a zou daarom integraal moeten komen te vervallen.

**Ongeëvalueerde gegevens (lid 2)**

Alvorens tot verstrekking over te gaan moeten de diensten beoordelen of de verstrekking noodzakelijk en proportioneel is. In het bijzonder is terughoudendheid geboden bij het verstrekken van ruwe gegevens of ruwe onderzoeksresultaten, zoals op grond van lid 2 mogelijk is. Een waarborg in het is dat toestemming van de minister is vereist voor het verstrekken van ongeëvalueerde gegevens. Een beoordeling op relevantie door de Nederlandse diensten heeft dan nog niet plaats gevonden. Met een dergelijke verstrekking wordt een buitenlandse dienst in staat gesteld zelf gegevens te beoordelen op hun relevantie voor de eigen taakuitvoering.[55] Waar de Nederlandse wet eisen stelt aan de termijn waarbinnen gegevenssets op relevantie moeten worden beoordeeld, althans als deze verkregen zijn door interceptie of binnendringen in computers (zie par. 4.6.3) – en bij verstrekking op basis van artikel 77 lid 2 zal het vaak om gegevens uit bulkinterceptie gaan – is het maar de vraag of de buitenlandse dienst ook een dergelijke termijn hanteert, en vooral of deze niet-onderzochte, of niet relevant bevonden, gegevens ook tijdig vernietigt. Het ligt daarom voor de hand om bij een dergelijke verstrekking ook de voorwaarde te stellen dat de gegevens binnen een bepaalde termijn onderzocht worden en na afloop van deze termijn alleen relevant

[55] Zie ook CTIVD 2015b, p. 30.

bevonden gegevens verwerkt mogen worden. Op zo'n voorwaarde valt natuurlijk moeilijk toe te zien; dat is overigens ook een probleem bij de spaghetticonstructievoorwaarde dat de gegevens niet doorverstrekt mogen worden – het ziet er op papier mooi uit maar valt niet of nauwelijks te controleren (behalve a contrario als uit een incident blijkt dat het toch gebeurd is; dat moet dan in elk geval aanleiding zijn de samenwerking te heroverwegen).

Minder terughoudendheid spreekt echter uit een passage uit de MvT:

> 'Overigens wordt opgemerkt dat de toestemming ook betrekking kan hebben op meerdere opeenvolgende verstrekkingen van vergelijkbare aard, zonder dat dit per geval dient te worden verleend. Dat is met name van belang voor de uitwisseling van dergelijke gegevens in het kader van specifieke internationale samenwerkingsverbanden.' (p. 141-2)

Kennelijk is lid 2 dus niet alleen bedoeld voor incidentele aanvragen, maar ook voor structurelere vormen van verstrekking van (bulk)gegevens die nog niet door de diensten zelf zijn geëvalueerd, in het kader van 'specifieke internationale samenwerkingsverbanden'.[56] Het feit dat voor verstrekkingen binnen dergelijke verbanden kennelijk ook een eenmalige generieke toestemming van de minister mogelijk is, kleedt de waarborg aanzienlijk uit.

Het verstrekken van ruwe of ongeëvalueerde gegevens aan buitenlandse diensten betekent een zeer groot privacyrisico, te meer omdat het vaak zal gaan, zoals de MvT aangeeft, om bulkbestanden. Deze gegevensverzamelingen zullen vaak vele personen betreffen en specifiek ook vele personen die niet de aandacht van de diensten hebben (vgl. daarover par. 4.2 en 8.3.2). Integrale verstrekking van deze gegevens, die niet op relevantie zijn onderzocht, is naar ons oordeel in beginsel niet subsidiair en disproportioneel, in elk geval waar het bulkdata betreft. Er is immers nauwelijks of geen controle mogelijk op hoe de buitenlandse diensten omgaan met de gegevens, en vooral met de bijvangst van data die niet relevant zijn voor het doel waarvoor ze (door de Nederlandse dienst) verzameld waren. De enige borging is dat de buitenlandse dienst, als onderdeel van de samenwerkingsrelatie, beoordeeld is geweest op professionaliteit en betrouwbaarheid en op naleving van mensenrechten. Dat zijn noodzakelijke voorwaarden om de privacyrisico's van verstrekking van bulkgegevens enigszins in te dammen, maar geen voldoende voorwaarden. De buitenlandse dienst kan bijvoorbeeld uiterst professioneel de gegevens voor andere doeleinden gebruiken dan waarvoor ze zijn verstrekt, of alle gegevens, ook van niet-relevante personen, op uiterst betrouwbare wijze 30 jaar bewaren en daar zeer professionele Big Data-analyses op loslaten. Ook betekent de beoordeling ex art. 76 dat een land in het algemeen de mensenrechten voldoende beschermt om een samenwerking mee aan te gaan, niet dat in alle gevallen de mensenrechten worden gerespecteerd; evenmin betekent het dat dezelfde standaard (bijvoorbeeld art. 8 EVRM) wordt toegepast in een ander rechtssysteem. Buitenlandse diensten zijn niet altijd gebonden aan dezelfde waarborgen als in de Nederlandse Wiv zijn opgenomen, en vallen ook niet altijd onder het EVRM.

[56] Hiermee wordt mogelijk gedoeld op samenwerkingsverbanden als Nine Eyes, waarbij Nederland naar verluidt is aangesloten, aldus https://en.wikipedia.org/wiki/Five_Eyes#Future_enlargement (geraadpleegd 1 december 2015).

Dit blijkt ook uit de zaak-Schrems, waarbij het Europees Hof van Justitie verwees naar de Mededeling van de Europese Commissie[57] waarin werd vastgesteld dat

> 'the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security'[58]

en dat wetgeving die beperkingen stelt aan het recht op privacy

> 'is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.'[59]

Weliswaar gaat het hier om gegevens die (veelal in commerciële relaties) vanuit de EU naar de VS worden overgedragen binnen de Safe Harbour, en niet om verstrekking door Europese inlichtingendiensten aan Amerikaanse collega-diensten, maar de vaststelling dat de Amerikaanse wetgeving onvoldoende waarborgen kent waardoor het onrechtmatig is dat gegevensverzamelingen in handen van de Amerikaanse diensten komen 'without any differentiation, limitation or exception being made in the light of the objective pursued' geldt evenzeer voor de verstrekking van ongeëvalueerde bulkgegevens onder artikel 77 lid 2.

Daar komt bij dat de wet de mogelijkheid open lijkt te laten om ook ongeëvalueerde gegevens te verstrekken binnen samenwerkingsverbanden die niet aan alle criteria voldoen maar die om politieke redenen toch zijn goedgekeurd. Artikel 77 lid 2 sluit niet uit dat ongeëvalueerde gegevens worden verstrekt aan 'risicodiensten' – de term waarmee de MvT 'diensten die niet aan alle eisen voldoen' of 'diensten die de mensenrechten onvoldoende respecteren' aanduidt waarmee mogelijk toch samengewerkt wordt als het belang van samenwerking zwaarder weegt (MvT, p. 139-140). Dat lijkt ons een onaanvaardbaar risico voor de verstrekking van ongeëvalueerde gegevens.

De verstrekking van dergelijke gegevens is een aantasting van de essentie van het recht op privacy. Hier ontstaat een onvoorzienbaarheid in normatieve zin, aangezien Nederlandse ingezetenen de verwerkingen van ongeëvalueerde gegevens door buitenlandse diensten niet hoeven te voorzien, en ook niet kunnen voorzien, omdat er geen invloed is op, noch kennis van, de wetgeving in andere landen. De democratische waarborg voor wat de buitenlandse diensten met gegevens mogen doen, ontbreekt. Indien een samenwerking met een buitenlandse dienst is overeengekomen, past het vanuit het oogpunt van de grote privacyrisico's,

[57] *Communication from the European Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final.
[58] EHJ 6 oktober 2015, Schrems (C-362/14) ECLI:EU:C:2015:650, §90.
[59] EHJ 6 oktober 2015, Schrems (C-362/14) ECLI:EU:C:2015:650, §93

de democratische legitimering en de benodigde rechtsstatelijke waarborgen om niet de gegevens ongeëvalueerd te verstrekken, maar namens of gezamenlijk met die dienst de gegevens binnen de Nederlandse diensten primair te analyseren met het oog op het doel van de buitenlandse dienst waarvoor de samenwerking met betrekking tot de te verstrekken gegevens wordt gezocht. Op die wijze kan eerst een selectie gemaakt worden en kunnen niet-relevante gegevens vernietigd worden. Daarmee wordt voorkomen dat een buitenlandse dienst de beschikking krijgt over gegevens over personen die niet de aandacht van die buitenlandse dienst hebben en worden alleen gegevens verstrekt die passen bij het doel waarvoor de gegevens worden verstrekt.

**Technische en andere vormen van ondersteuning (leden 4-6)**
Artikel 77 biedt verder de bevoegdheid tot het op verzoek van buitenlandse diensten bieden van technische en andere vormen ondersteuning aan deze diensten. De MvT legt niet echt uit wat hieronder wordt verstaan. Het zou helpen als de MvT enkele voorbeelden geeft en aangeeft of de aanbeveling uit CTIVD-rapport 22A om alle vormen van ondersteuning (zoals trainingen) onder het formele bereik van dit artikel te brengen,[60] met dit artikel wordt overgenomen. Duidelijk is wel dat het vooral ook inhoudt dat de Nederlandse diensten hun bevoegdheden ook ten behoeve van een buitenlandse dienst kunnen inzetten. Vanzelfsprekend zijn daarbij de bijbehorende vereisten en waarborgen voor de inzet van die bevoegdheden van toepassing (MvT, p. 142).

Voor het verlenen van technische en andere vormen van ondersteuning is op basis van zowel de huidige als de nieuwe wet toestemming van de minister vereist (art. 77 lid 5 verwijst hierbij overigens naar lid 3; hier zal lid 4 bedoeld zijn). Deze toestemming kan onder de Wiv 2002 alleen worden gemandateerd aan het hoofd van de dienst indien sprake is van een verzoek met spoedeisend karakter. De Wiv 20xx staat mandatering aan het diensthoofd in het algemeen toe, omdat de CTIVD heeft opgemerkt ‘dat het enkele feit dat een bijzondere bevoegdheid wordt ingezet in het belang en ter ondersteuning van een buitenlandse dienst een verhoging van het toestemmingsvereiste naar het niveau van de minister niet *in alle gevallen* noodzaakt’ (MvT, p. 142, onder verwijzing naar CTIVD-rapport 22A). De mogelijkheid tot het mandateren van de bevoegdheid tot verlenen van toestemming wordt in het wetsvoorstel dus verruimd ten opzichte van de Wiv 2002. Dat valt te billijken gezien de argumentatie van de CTIVD[61] en het feit dat voor de inzet van een bevoegdheid in elk geval het desbetreffende toestemmingsvereiste van de bevoegdheid geldt. Een belangrijke toevoeging in het wetsontwerp (lid 6) is ook dat indien er risico’s zijn verbonden aan de dienst van een ander land (wanneer de beoordeling conform artikel 76 lid 2 niet onverkort positief is), de toestemming wel altijd moet worden verleend door de minister. Dat is een belangrijke toevoeging, die terecht ook in de wettekst zelf wordt opgenomen, gezien de extra privacyrisico’s die ondersteuning in die situaties met zich meebrengt.

Dat neemt niet weg dat de regeling niet in alle opzichten rekening houdt met de privacyrisico’s die gemoeid zijn met ondersteuning van buitenlandse diensten, omdat de mate van controle over wat er met de resultaten in het buitenland gebeurt veel lager is dan de mate van controle over resultaten die voor de eigen taakuitoefening worden gebruikt.

[60] CTIVD 2009, p. 32.
[61] CTIVD 2009, p. 33.

Ten eerste is belangrijk dat bij de afweging die aan die toestemming vooraf gaat, ook de overweging betrokken wordt dat het gaat om inzet voor een buitenlandse dienst, met navenant minder controle op wat er met de gegevens gebeurt dan als de bevoegdheid voor de taakuitoefening van de diensten zelf zou worden ingezet. Daarom moet de noodzaak van inzet van de bevoegdheid extra scherp worden beoordeeld en moet het privacybelang in deze afweging, vanwege het gebrek aan controle, zwaar wegen. Het is belangrijk dat de CTIVD kan controleren dat de afweging ook daadwerkelijk rekening houdt met de extra privacyrisico's van verstrekking aan het buitenland, zodat in de motivering van de toestemming hier expliciet aandacht aan zal moeten worden besteed. De toelichting zou dit expliciet moeten aangeven.

Ten tweede ontbreekt bij de inzet van ondersteuning een verwijzing naar de waarborgen van artikel 51, 55 en 56. Mogelijk wordt impliciet verondersteld dat als de ondersteuning, in de vorm van inzet van bevoegdheden, resultaten oplevert die aan de buitenlandse dienst worden geleverd, dit geldt als een verstrekking van gegevens ex artikel 77 lid 1, maar dat is allerminst duidelijk uit de systematiek van het artikel en blijkt ook geenszins uit de toelichting. Het is niet begrijpelijk dat genoemde waarborgen wel worden gesteld bij verstrekking van reeds aanwezige gegevens, maar niet bij inzet van bevoegdheden om nieuwe gegevens te verzamelen voor de buitenlandse dienst. Artikel 51, verstrekking onder voorwaarde van niet-doorverstrekking, is dan misschien een papieren waarborg, maar wetssystematisch hoort dit in elk geval ook van toepassing te zijn op resultaten die via de technische ondersteuning worden verkregen. Artikel 55 is niet relevant waar het om verouderde gegevens betreft, maar wel voor zover het gaat om inzet van bevoegdheden die gegevens opleveren waarvan de betrouwbaarheid niet kan worden gecontroleerd; dergelijke gegevens zouden niet moeten kunnen worden verstrekt. Artikel 56, de plicht om aantekening te houden van de verstrekking, is mutatis mutandis ook van belang bij ondersteuning. Daarom zou artikel 77 lid 3 ook van toepassing moeten worden op lid 4.

Ten derde bestaat er een zeker privacyrisico dat deze bevoegdheid politiek-strategisch wordt ingezet in het kader van de 'quid pro quo'-praktijk. De diensten zouden internationale samenwerkingsverbanden ook als U-bocht kunnen gebruiken om waarborgen in hun eigen wet te omzeilen. Wij hebben geen aanwijzingen dat U-bochtconstructies feitelijk plaatsvinden, maat het gaat om een duidelijk aanwezig risico. Het is moeilijk om dat risico af te dekken door externe normering (in de wet, in het toezicht), al kan de CTIVD door de inzet van controlebevoegdheden proberen er zicht op te krijgen of dit risico zich in de praktijk manifesteert.[62] De normering zal vooral intern moeten zijn: door een cultuur van tegenspraak, waarbij men elkaar bevraagt en kritische vragen durft te stellen, en door het ontwikkelen van een intern moreel kompas bij de diensten door doorlopende training, discussiebijeenkomsten en ethische reflectie op de uitvoeringspraktijk.

### *5.4.3 Verzoek tot ondersteuning aan buitenlandse diensten*

Waar artikel 77 de mogelijkheid geeft om ondersteuning aan buitenlandse diensten te bieden, regelt artikel 78 de mogelijkheid om ondersteuning aan buitenlandse diensten te vragen.

[62] Vgl. CTIVD 2014b, p. 32-33.

Artikel 78

1. De diensten zijn in het kader van een goede taakuitvoering bevoegd tot het doen van een verzoek om technische en ander vormen van ondersteuning aan inlichtingen- en veiligheidsdiensten van andere landen, indien daarvoor overeenkomstig het bepaalde in dit artikel toestemming is verleend.
2. Indien het verzoek, bedoeld in het eerste lid, strekt ter ondersteuning bij de uitoefening van een bijzondere bevoegdheid, waarvoor toestemming is verleend, wordt de toestemming voor het verzoek om ondersteuning verleend door degene die ingevolge het bij of krachtens artikel 24 van deze wet bepaalde, bevoegd is tot het verlenen van toestemming voor de uitoefening van de desbetreffende bijzondere bevoegdheid.
3. Indien het verzoek om ondersteuning als bedoeld in het eerste lid het verrichten van een handeling betreft die overeenkomt met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3, is hetgeen bij of krachtens deze paragrafen ter zake is bepaald, van overeenkomstige toepassing.
4. In afwijking van het bepaalde in het tweede en derde lid, wordt, ingeval de verlangde ondersteuning niet in overeenstemming is met de aard en intensiteit van de samenwerkingsrelatie met de desbetreffende inlichtingen- en veiligheidsdienst van een ander land, zoals vastgesteld naar aanleiding van de weging als bedoeld in artikel 76, de toestemming voor het verzoek om ondersteuning verleend door Onze betrokken Minister.
5. Een verzoek om ondersteuning als bedoeld in het derde lid kan geen betrekking hebben op het verrichten van handelingen die niet overeenkomen met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3 van deze wet.

(…)

De bevoegdheid tot een verzoek om ondersteuning uit artikel 78 van het wetsvoorstel is nieuw. Samenwerking tussen diensten is belangrijk en wederkerig, en daarom is een regeling tot een dergelijke bevoegdheid nuttig. De wettelijke basis is daarbij welkom.

Vanuit het oogpunt van privacyrisico's is hierbij vooral lid 5 van belang, dat een belangrijke beperking kent in de zin dat alleen ondersteuning verzocht mag worden voor uitoefening van bijzondere bevoegdheden die de Nederlandse diensten zelf hebben. De MvT zegt hierover:

> 'Met deze regeling wordt aldus voorkomen dat men in de verzoeken om ondersteuning treedt buiten de bijzondere bevoegdheden die in de wet (limitatief) aan de diensten toekomen.' (p. 144)

> 'Het betreft een limitatieve opsomming van bijzondere bevoegdheden; de inzet van (inlichtingen)middelen die niet terug te herleiden zijn tot een van deze bevoegdheden is dan ook niet geoorloofd. [voetnoot] Zie ook artikel 78, vijfde lid, van het wetsvoorstel, waar het gaat om het doen van verzoeken van ondersteuning door de AIVD en de MIVD *aan* buitenlandse collega-diensten waar het gaat om de uitoefening van bijzondere bevoegdheden (of handelingen die daarop zijn terug te herleiden).' (p. 37).

Indien een buitenlandse dienst meer of andere bevoegdheden heeft, mag van die aanvullende bevoegdheden dus geen gebruik gemaakt worden in het kader van een onderzoek van de Nederlandse diensten. Onduidelijk is hierbij overigens waarom de bepaling beperkt is tot de bijzondere bevoegdheden; het suggereert dat buitenlandse diensten niet mag worden verzocht om gegevens op te vragen bij derden (vergelijkbaar met de 'algemene' bevoegdheid). Wetssystematisch valt dat moeilijk in te zien, en ook voor privacyrisico's maakt het niet op voorhand verschil of data in het buitenland via de 'algemene' of een bijzondere bevoegdheid worden ingewonnen, dat hangt immers van de concrete situatie af. Ons voorstel om de 'algemene' en de bijzondere bevoegdheden samen te nemen zou het mogelijk maken om ook verzoeken tot gegevensbevraging te kunnen doen op basis van artikel 78 j$^{o}$ artikel 22, wat naar wij aannemen (zonder tegenargumenten in de MvT) ook wel de bedoeling van de wetgever zal zijn.

De beperking dat een verzoek binnen de reikwijdte van de (bijzondere) bevoegdheden van de Nederlandse diensten moet vallen is van groot belang. Juist hiermee moet het privacyrisico van U-bochtconstructies worden afgedekt (het via een omweg verkrijgen van gegevens die de diensten zelf niet mogen verzamelen). Ook wordt hiermee, als het goed is, de mogelijkheid van het witwassen van informatie voorkomen, dat wil zeggen dat als diensten informatie in handen hebben gekregen op een manier die niet in overeenstemming met de Nederlandse wet is, via een gericht verzoek aan een buitenlandse dienst de informatie via die weg opnieuw probeert te verkrijgen maar nu met de buitenlandse dienst als legitieme bron.

Deze risico's worden geadresseerd door artikel 78 lid 5, maar het is de vraag of dat voldoende is. De toelichting spreekt in algemene termen van 'de bijzondere bevoegdheden', zonder in te gaan op de vraag welke waarborgen daarop van toepassing zijn. De toelichting over lid 5 is daarmee bijzonder minimalistisch; het wekt de suggestie dat het vooral gaat om de vraag of een buitenlandse dienst een bevoegdheid inzet die de AIVD of MIVD ook heeft, zonder in te gaan op de voorwaarden waaronder die bevoegdheid kan worden ingezet. De Nederlandse diensten mogen tappen, hacken en metadata-analyses uitvoeren, dus mogen ze dat ook vragen aan buitenlandse diensten. Dat gaat volledig voorbij aan de vraag in hoeverre deze specifieke bevoegdheden door de diensten van een ander land onder minder stringente voorwaarden kunnen worden uitgeoefend.

Nu is het misschien de bedoeling dat dit door het voorgestelde lid 3 wordt afgedekt, aangezien dat bepaalt dat bij verzoeken om een handeling die naar de Nederlandse wet onder een bijzondere bevoegdheid valt, 'hetgeen bij of krachtens [paragrafen 3.2.2, 4.2 en 4.3] ter zake is bepaald, van overeenkomstige toepassing' is. Hierover zegt de MvT:

> 'Concreet betekent dit, dat als de AIVD of MIVD aan een buitenlandse dienst een verzoek wil doen om bijvoorbeeld de telecommunicatie van een persoon in het desbetreffende land te intercepteren, daarvoor de regeling voor de toepassing van de bijzondere bevoegdheid tot het aftappen van telecommunicatie dient te worden toegepast. Dat betekent dat in dit voorbeeld er een gemotiveerd verzoek om toestemming aan de minister dient te worden voorgelegd.' (p. 143).

Onzes inziens kent de regeling aanzienlijke lacunes. Ten eerste is er een wetstechnisch bezwaar (dat vanwege de resulterende rechtsonzekerheid ook duidelijk privacyconsequenties heeft). Lid 5 beoogt kennelijk om duidelijk te maken dat men niet mag vragen om inzet van bevoegdheden die de Nederlandse diensten niet hebben. Maar dat is niet wat er in lid 5 staat. De formulering luidt: 'Een verzoek om ondersteuning als bedoeld in het derde lid kan geen betrekking hebben op het verrichten van handelingen die niet overeenkomen met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3 van deze wet.' Dat is nogal logisch: het derde lid is immers beperkt tot een verzoek dat het 'verrichten van een handeling betreft die overeenkomt met de uitoefening van een bijzondere bevoegdheid als bedoeld in de paragrafen 3.2.2, 4.2 en 4.3'. Lid 5 legt dus, door de beperking tot verzoeken 'om ondersteuning als bedoeld in het derde lid', in andere bewoordingen uit wat er al in lid 3 staat. Dat is overbodig, omdat de formulering van lid 3 op zich duidelijk genoeg is (althans voor juristen, hoewel niet voor de gemiddelde burger). Lid 5 zou juist moeten gaan over verzoeken die *niet* verzoeken als bedoeld in lid 3 betreffen, en dus eerder moeten verwijzen naar verzoeken als bedoeld in het *eerste* lid.

Ten tweede bestaat er een lacune in de van toepassingverklaring van waarborgen. Lid 3 stelt dat bij verzoeken om inzet tot (het buitenlandse equivalent van) een bijzondere bevoegdheid hetgeen bij of krachtens paragrafen 3.2.2, 4.2 en 4.3 ter zake is bepaald, van overeenkomstige toepassing is. Daarin staan de nodige waarborgen (waaronder art. 23-24 en 43-45 en soms specifieke waarborgen in bevoegdheidsbepalingen zelf), maar lang niet alle. Dat betekent dat de waarborgen in artikelen 17-21 (algemene regels over dataverwerking), paragraaf 3.2.3 (notificatie), art. 47 lid 3 (geen geautomatiseerde beslissingen), en paragraaf 3.5 (vernietiging van gegevens) kennelijk niet van overeenkomstige toepassing zijn. Mogelijk zijn niet al deze waarborgen in alle gevallen relevant voor verzoeken tot buitenlandse ondersteuning, maar het is in elk geval onbegrijpelijk dat de algemene bepalingen (par. 3.1) niet van overeenkomstige toepassing zouden zijn.

Verder blijft het ook wat onduidelijk wat 'van overeenkomstige toepassing' in dit verband inhoudt. Het voorbeeld van ministeriële toestemming bij een interceptieverzoek is duidelijk. Maar wat betekenen bijvoorbeeld de onderzoeksplichten zoals in artikel 30 lid 9 dat gegevens 'zo spoedig mogelijk op hun relevantie voor het onderzoek worden onderzocht'? Is het de bedoeling dat, naar 'overeenkomstige toepassing', deze selectie door de buitenlandse dienst gebeurt en dat alleen relevant bevonden gegevens aan de Nederlandse worden doorgegeven? Dat zou naar de geest van deze bepaling, en voor de privacybescherming van buitenlanders die als bijvangst in verzamelde gegevens zitten, belangrijk zijn, maar het is onduidelijk of dat de strekking is van artikel 78 lid 3. Ook is onduidelijk naar welke maatstaven de overeenkomstig toegepaste bepalingen moeten worden geïnterpreteerd. Zo mag een bevoegdheid niet worden toegepast als die voor betrokkenen een onevenredig nadeel oplevert ten opzichte van het beoogde doel (art. 43 lid 3). Wordt dat beoordeeld naar wat in Nederland evenredig wordt geacht, of in het desbetreffende buitenland? Als een handeling van een dienst tot gevolg heeft dat iemand haar baan verliest (bijvoorbeeld omdat de werkgever moet meewerken aan een Internettap of als informant wordt betrokken), is dat ingrijpend. Voor een zwaarwegend doel kan dat evenredig zijn naar Nederlandse maatstaven, omdat hier een relatief goed socialezekerheidsstelsel bestaat. In sommige landen kan baanverlies echter veel ingrijpender gevolgen hebben voor iemands bestaan. Los van de vraag welke maatstaf van toepassing is

(waarover de MvT zwijgt), is het ook moeilijk toe te passen: voor de Nederlandse dienst is het bij het doen van een verzoek moeilijk in te schatten wat de gevolgen voor betrokkenen kunnen zijn van de gevraagde handeling, terwijl het voor de buitenlandse dienst moeilijk is in te schatten wat het gewicht is van de gevraagde medewerking – beide zijn niet alleen sterk contextafhankelijk maar ook mede cultureel en sociaal bepaald.

Een vergelijkbaar punt is dat de verwijzing naar de genoemde paragrafen ook beperkt is, omdat deze niet verwijst naar het stelsel van waarborgen als geheel. De *checks and balances* bij de uitvoering van bevoegdheden zijn een precair samenstel tussen waarborgen vooraf (zoals toestemming), waarborgen tijdens uitvoering (zoals doelbinding) en waarborgen achteraf (toezicht). De balans tussen die waarborgen kan in het buitenland anders zijn, bijvoorbeeld een lichtere vorm van toestemming vooraf, die wordt gecompenseerd door zwaar toezicht achteraf, of omgekeerd. In het verlengde daarvan moet ook worden opgemerkt dat de regeling van een bevoegdheid in het buitenland moeilijk op waarde is te schatten door de Nederlandse diensten (en ook voor de toezichthouder). Een wettelijke bepaling moet in de context van het gehele systeem worden gelezen, en daarnaast ook in de wetshistorische, sociale en culturele context worden geïnterpreteerd. Dat vergt specialistenwerk en uitvoerige analyses, waarvan aan te nemen valt dat de capaciteit daarvoor niet (in voldoende mate) aanwezig is bij de diensten. Zo heeft de regeling van interceptie door de Amerikaanse en Britse diensten geleid tot zeer omvangrijke rapporten door nationale onderzoekscommissies om het waarborgenstelsel in kaart te brengen en te waarderen.

Al met al valt het nauwelijks te overzien of een verzoek door de AIVD of MIVD tot bijvoorbeeld interceptie aan buitenlandse diensten ‘treedt buiten de bijzondere bevoegdheden die in de wet (limitatief) aan de diensten toekomen’, omdat de Nederlandse diensten weliswaar een bevoegdheid tot interceptie hebben, maar de reikwijdte van interceptiehandelingen in het buitenland, op basis van de desbetreffende buitenlandse bevoegdheid en met inachtneming van het daarop van toepassing zijnde stelsel van waarborgen (of het gebrek daaraan), moeilijk te bepalen valt.

Dit levert een aanzienlijk risico op, namelijk dat de toets aan de vraag of bij verzoeken ex artikel 78 buiten Nederlandse bevoegdheden wordt getreden (op basis van lid 3 en de beoogde strekking van lid 5), alleen maar simplistisch benaderd zal worden door verzoeken te beperken tot handelingen die in abstracto overeenkomen met Nederlandse bevoegdheden – interceptie, observatie, binnendringen in computers, enzovoorts – *zonder* te kijken naar de manier waarop, en de voorwaarden waaronder, deze handelingen in het buitenland in concreto zullen worden uitgevoerd. Hoewel dat enigszins begrijpelijk is vanwege de complexiteit, is het zeer onwenselijk vanuit het oogpunt van privacyrisico’s. Waar de buitenlandse wetgeving of uitvoeringspraktijk minder waarborgen kent of lagere eisen stelt dan de Nederlandse, zal veelal een grotere privacyinbreuk mogelijk zijn dan naar de Nederlandse wet geoorloofd is. Mocht dat de bedoeling van de wetgever zijn, dan moet dat expliciet in de MvT worden aangegeven, met motivering waarom dit aanvaardbaar wordt geacht. Mocht het niet de bedoeling zijn – en vanuit het oogpunt van adequate privacybescherming zou dat niet de bedoeling mogen zijn – dan zouden de regeling en toelichting veel dieper op de problematiek moeten ingaan op de waarborgen die van toepassing moeten zijn bij buitenlandse taakuitoefening op Nederlands verzoek.

Daarbij moet in elk geval overwogen worden om het instemmingsvereiste op te hogen tot ten minste het niveau van het diensthoofd. In de huidige regeling is, volgens lid 4, (terecht) ministeriële instemming vereist als een handeling wordt gevraagd van ‘risicodiensten’, maar voor landen met een ‘reguliere’ samenwerking vindt toestemming plaats op het niveau dat in Nederland geldt. Dat wil zeggen dat voor bepaalde, ‘lichte’ bevoegdheden ondergemandateerde medewerkers toestemming kunnen verlenen om inzet van een dergelijke bevoegdheid aan een buitenlandse dienst te verzoeken (lid 2). Vanwege de complexiteit van het vergelijken van bevoegdheden en het inschatten van de mate waarin bij de uitvoering in het buitenland voldaan wordt aan de voorwaarden en waarborgen die bij uitvoering in Nederland zouden gelden, is het raadzaam om bij verzoeken op basis van artikel 78 ook voor ogenschijnlijk eenvoudige handelingen toestemming van het diensthoofd te vragen. Het is overigens opvallend dat het wetsontwerp een aanzienlijk lichter toestemmingsregime hanteert voor verzoeken tot inzet van een bevoegdheid aan buitenlandse diensten dan voor verzoeken aan de Nederlandse zusterdienst; artikel 74 lid 3 vereist immers toestemming van de minister voor verzoeken tot ondersteuning van AIVD aan MIVD en omgekeerd. In dat opzicht past het meer om in artikel 78 voor verzoeken aan buitenlandse diensten tot inzet van een bijzondere bevoegdheid altijd toestemming van de minister te eisen, die hooguit kan worden gedelegeerd aan het diensthoofd voor kleinschalige handelingen die alleen inzet van lichte bevoegdheden vergen.

Daarnaast kan bijvoorbeeld ook gedacht worden aan een verplichting tot het opnemen van de, op basis van het Nederlandse waarborgenstelsel geldende, beperkingen in de gedetailleerde beschrijving van het verzoek aan de buitenlandse dienst, die deze dienst bij de uitvoering van het verzoek in acht moet nemen. Ook kan de buitenlandse dienst gevraagd worden om bij het leveren van de resultaten aan de Nederlandse dienst schriftelijk te verklaren dat de in het verzoek gestelde eisen en beperkingen in acht zijn genomen. Weliswaar zullen dergelijke beperkingen op papier niet altijd de nodige normerende werking hebben op de uitvoering, en de naleving is moeilijk te controleren, maar het zou in elk geval bijdragen aan bewustwording bij de uitvoerders van het belang om grenzen in acht te nemen, alsook aan de mogelijkheid voor de toezichthouder om enige greep te krijgen op de uitvoering van verzoeken die op basis van artikel 78 worden gedaan. Daarbij zal het ook van belang zijn dat de CTIVD enige capaciteit heeft om de toezichthouder in staat te stellen in te schatten of de samenwerkingspartners, zeker ook bij samenwerking op verzoek van Nederland, niet alleen in abstracto (de toets van art. 76) maar ook in concreto (bij handelingen volgend uit art. 78) de mensenrechten voldoende naleven.

# 6 Lichamelijke privacy

Onder lichamelijke privacy verstaan we de privacy in relatie tot het lichaam van een natuurlijke persoon, oftewel de lichamelijke integriteit zoals die wordt gewaarborgd door artikel 11 Gw. In dit verband is het relevant om de voorgestelde regeling van het DNA-onderzoek te bekijken. Deze regeling maakt strikt genomen geen inbreuk op artikel 11 Gw: er wordt geen lichaamsmateriaal afgenomen (bijvoorbeeld wangslijm), zodat het lichaam niet fysiek wordt geraakt, terwijl de fysieke aantasting van het lichaam veelal als criterium wordt gehanteerd om te spreken van een inbreuk op de lichamelijke integriteit. De regeling omvat onderzoek aan voorwerpen waarop celmateriaal achterblijft, bijvoorbeeld een koffiebekertje, glas of tandenborstel, waaruit een DNA-profiel kan worden afgeleid. Niettemin behandelen we het wel in dit hoofdstuk over lichamelijke privacy, omdat het wel gaat om de verwerking van celmateriaal, dat alle genetische informatie over de persoon bevat, zodat hier de informationele privacy nauw verweven is met de lichamelijke privacy.

## 6.1 Inleiding

In artikel 28 wordt het verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen geregeld, ten behoeve van het vaststellen van de identiteit van een persoon. Het is daarmee een bijzondere vorm van het onderzoek aan voorwerpen ter vaststelling van de identiteit (art. 27 lid 1 onder c), dat vanwege de bijzonderheid van DNA-onderzoek zelfstandig wordt geregeld.

---

**Artikel 28**

1. De diensten zijn bevoegd tot het verrichten van DNA-onderzoek op basis van celmateriaal op voorwerpen ten behoeve van het vaststellen van de identiteit van een persoon. Onder vaststellen van de identiteit wordt in dit artikel mede verstaan de verificatie van de identiteit van een persoon. Het DNA-onderzoek vindt plaats door vergelijking van DNA-profielen.
2. De in het eerste lid bedoelde bevoegdheid mag slechts worden uitgeoefend, indien door Onze betrokken Minister daarvoor op een daartoe strekkend verzoek schriftelijk toestemming is verleend aan het hoofd van de dienst.
3. Het verzoek om toestemming, bedoeld in het tweede lid, wordt gedaan door het hoofd van de dienst en bevat in aanvulling op hetgeen is bepaald in artikel 24, zesde lid:
   a. gegevens betreffende de identiteit van de persoon ten aanzien van wie de uitoefening van de bevoegdheid wordt verlangd, voor zover deze bekend zijn;
   b. een nauwkeurige omschrijving van het celmateriaal waaraan het onderzoek wordt verricht alsmede de wijze waarop dit is verkregen.
   (…)

---

Het onderzoek aan voorwerpen ter vaststelling van de identiteit van een persoon bestaat al in de Wiv 2002 (art. 22 lid 1 aanhef en onder c). In de praktijk wordt dit artikel geïnterpreteerd als mede omvattende het onderzoek van celmateriaal dat achterblijft op voorwerpen om een DNA-profiel te maken. Die interpretatie wordt gedeeld door de CTIVD, die daarbij constateert dat art. 22 Wiv 2002 wel een voldoende grondslag biedt om het profiel te vergelijken met elders opgeslagen profielen (zoals de forensische DNA-databank), maar niet om een eigen DNA-

databank in te richten.[63] Het huidige artikel dient ertoe om de daarmee 'geconstateerde gebreken in de wetgeving ter zake' te adresseren (MvT, p. 44). Voordat we ingaan op het voorstel een eigen DNA-databank op te richten (zie onder, par. 6.6), bespreken we eerst de privacyimplicaties van het DNA-onderzoek in de voorgestelde regeling zelf.

## 6.2 Algemene beschouwing over DNA-onderzoek ter vaststelling van de identiteit

De interpretatie dat DNA-onderzoek reeds besloten zou zijn in art. 22 Wiv 2002 is twijfelachtig. Zoals de CTIVD opmerkt, wordt in de Memorie van Toelichting bij de Wiv 2002 alleen het voorbeeld gegeven van vingerafdrukken op een plastic bekertje,[64] maar nergens wordt DNA-onderzoek genoemd. Ten tijde van de totstandkoming van de Wiv 2002 was het DNA-onderzoek volop in ontwikkeling, en de wetgever heeft rond de eeuwwisseling het DNA-onderzoek in strafzaken uitvoerig geregeld.[65] In 1999 wees de Hoge Raad het tandenborstel-arrest, in een zaak waarin de politie onder andere tandenborstels bij een huiszoeking in beslag had genomen om daaraan DNA-onderzoek te kunnen doen.[66] Dit is precies de casus waarop het onderzoek aan voorwerpen met het oog op vaststelling van de identiteit betrekking heeft. Hoewel het arrest van later datum is dan de MvT bij de Wiv 2002, was het ook in 1997 al genoegzaam bekend dat tandenborstels DNA-materiaal bevatten, en het zou voor de hand hebben gelegen dat, als de wetgever beoogde dat ook de inlichtingen- en veiligheidsdiensten voorwerpen moeten kunnen wegnemen om DNA-onderzoek aan celmateriaal op die voorwerpen te kunnen doen, dit dan ook met zoveel woorden in de toelichting bij de wet verduidelijkt zou zijn. Verder is, voor zover wij hebben kunnen nagaan, in de latere behandeling van de Wiv 2002, ook na het tandenborstel-arrest en in de periode dat de wetgever het strafrechtelijk DNA-onderzoek wijzigde (mede met het oog op de casus uit het tandenborstel-arrest), niet gesteld dat art. 22 Wiv 2002 ook DNA-onderzoek omvat. Gezien de ingrijpendheid van DNA-onderzoek – dat ingrijpender is dan vingerafdrukkenonderzoek – vereist het een expliciete basis in de wet, en het is twijfelachtig of het huidige artikel 22 wel voldoende expliciet is, nu de wetgever wel vingerafdrukken maar niet DNA-onderzoek heeft genoemd bij de totstandkoming van de wet.

Het is een relevante vraag of het DNA-onderzoek wel of niet onder de huidige wet valt. Wanneer dit niet het geval is, is de voorgestelde regeling een voorbeeld van wetgeving die de praktijk volgt in plaats van andersom, met codificatie van een in de praktijk gegroeide handelwijze (zie par. 2.3.1). Ook elders wekt de MvT wel de suggestie dat artikel 28 meer een kwestie is van expliciet wettelijk regelen van wat al toegestaan is, waar gesteld wordt dat het gaat om het repareren van 'gebreken in de wetgeving', een formulering die meer suggereert dat de wetgeving onbedoelde lacunes heeft dan dat het gaat om het aanpassen van de wetgeving om te voldoen aan behoeften uit de praktijk waarin de huidige wet simpelweg niet voorziet. De toelichting zou explicieter moeten maken dat het hier gaat om een substantiële uitbreiding van bevoegdheden, zeker waar het het opzetten van een DNA-databank betreft.

---

[63] CTIVD (2015a), p. 11.
[64] *Kamerstukken II* 1997/98, 25 877, nr. 3, p. 36.
[65] Zie *Kamerstukken II* 1998-1999, 26 271, nrs. 1-3, resulterend in *Stb*. 2001, 335 en de regeling van de DNA-databank in het Besluit DNA-onderzoek in strafzaken, *Stb*. 2001, 400.
[66] HR 29 juni 1999, *NJ* 2000, 10 m.nt. 'tH.

De privacyrisico's van DNA-onderzoek op basis van op voorwerpen gevonden celmateriaal zijn in zichzelf niet zeer ingrijpend, zolang het celmateriaal enkel wordt onderzocht om een DNA-profiel te genereren dat met een elders beschikbaar profiel kan worden vergeleken. In die zin levert wat in de huidige wet – al dan niet terecht – wordt ingelezen, en wat in het voorgestelde art. 28 leden 1-3 expliciet wordt geregeld, geen groot privacyrisico op. Er wordt hierbij geen inbreuk gemaakt op de lichamelijke integriteit om het celmateriaal te verkrijgen, terwijl de informatie die wordt verkregen beperkt is: een DNA-profiel maakt het mogelijk om met grote waarschijnlijkheid vast te stellen of het celmateriaal behoort bij een bepaalde persoon (als van die persoon een DNA-profiel beschikbaar is), maar er kan weinig informatie uit worden afgeleid over de persoon (behalve het geslacht, maar we mogen aannemen dat kennis daarover al beschikbaar is bij de diensten).[67] Voorwaarden zijn wel dat het DNA-onderzoek uitsluitend wordt gebruikt om een DNA-profiel te maken (en niet voor het afleiden van persoonskenmerken uit het genetische materiaal), dat dit DNA-profiel uitsluitend wordt gebruikt om de identiteit van een target vast te stellen, en dat het celmateriaal en DNA-profiel worden vernietigd als eenmaal het doel van identificatie is bereikt. Zodra het biologische materiaal of het DNA-profiel langer wordt bewaard, ontstaat een risico dat dit op een later tijdstip ook voor andere doeleinden kan worden gebruikt.

Hoewel de privacyrisico's bij dit type DNA-onderzoek (indien beperkt tot het enkele vaststellen van de identiteit) niet zeer ingrijpend zijn, bestaat er wel een klein risico dat er fouten worden gemaakt, wat consequenties kan hebben voor derden. In enkele gevallen leidt contaminatie in het onderzoek echter tot foute interpretaties (zoals het 'fantoom van Heilbronn', waarin een vrouwelijke seriemoordenaar werd gezocht totdat bleek dat de wattenstaafjes waarmee DNA-materiaal was verzameld gecontamineerd uit de fabriek waren gekomen[68]). Belangrijker is dat fouten in interpretatie kunnen worden gemaakt: het voorwerp waaraan DNA-onderzoek wordt gedaan, kan ook materiaal van anderen dan de beoogde target bevatten. Het zal afhangen van mate van de zekerheid over de koppeling tussen het voorwerp en de beoogde persoon of dergelijke interpretatiefouten voldoende kunnen worden uitgesloten. De diensten zullen alert moeten zijn op de mogelijkheid dat het voorwerp ook nog sporen van anderen kan bevatten. In de meeste gevallen zal, als het om een spoor van een ander gaat en het profiel een treffer oplevert in een DNA-databank, vrij snel vastgesteld kunnen worden dat het om een andere persoon gaat. Niettemin blijft het risico dat de verkeerde persoon in beeld komt bestaan, zeker als het gaat om een kring van personen met veelal dezelfde kenmerken. Het (kleine maar niet denkbeeldige) risico van interpretatiefouten valt niet in de wet te ondervangen; het komt aan op de professionaliteit van de diensten en hun alertheid om tunnelvisies te voorkomen, iets wat met organisatorische maatregelen (zoals training en een interne cultuur van tegenspraak) zal moeten worden ondervangen.

Wetstechnisch valt overigens wel een kanttekening te plaatsen bij artikel 28 lid 3 onder a: het is wat merkwaardig om bij een bevoegdheid die mede als doel heeft de identiteit van een (kennelijk) niet-bekende persoon te achterhalen (dus naast gevallen van verificatie), te eisen dat het verzoek om toestemming 'gegevens

[67] Hooguit kunnen statistische uitspraken worden gedaan over de etnische afkomst op basis van het DNA-profiel, zoals gesteld door EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §76. De betrouwbaarheid van de uitspraken is niet bijzonder groot. In elk geval is het de diensten niet toegestaan om gegevens over ras te verwerken (art. 18 lid 3) en de wet stelt expliciet dat er geen persoonskenmerken uit het DNA-materiaal mogen worden afgeleid.
[68] Zie https://en.wikipedia.org/wiki/Phantom_of_Heilbronn (geraadpleegd 1 december 2015).

betreffende de identiteit van de persoon' bevat, 'voor zover deze bekend zijn'. Meestal zal immers juist daarover niets, of niet genoeg, bekend zijn – anders is het onderzoek immers niet nodig. Wat vermoedelijk bedoeld is, is dat de (qua identiteit onbekende maar fysiek in beeld zijnde) persoon op wie het verzoek betrekking heeft, zo nauwkeurig mogelijk wordt omschreven. Daarom zou een formulering als 'een zo nauwkeurig mogelijke aanduiding van de persoon' meer waarborgen bieden dat het verzoek zo specifiek mogelijk op de bedoelde persoon betrekking heeft dan 'gegevens betreffende de identiteit' (die immers ontbreken).

De privacyrisico's worden, zoals gezegd, wel aanzienlijk groter als het DNA-onderzoek zich richt op het afleiden van persoonskenmerken uit het celmateriaal; daarvoor is geen noodzaak aanwezig bij de diensten, en het wetsvoorstel beperkt zich dan ook terecht tot het enkele doel van vaststelling van de identiteit.[69] Tegelijk zijn de privacyrisico's ook aanzienlijk groter als het celmateriaal of DNA-profiel wordt bewaard nadat de identiteit is vastgesteld, en dit wordt wel mogelijk gemaakt in het wetsvoorstel. Dit roept vragen op over de noodzaak hiervan en de waarborgen, die we hieronder uitwerken (zie par. 6.5 en 6.6). Eerst is het echter nodig om nog nader het precieze doel van de voorgestelde regeling te analyseren, omdat het zich niet beperkt tot het enkele vaststellen van de identiteit van onbekende personen.

## 6.3 Het doel van DNA-onderzoek

Het doel van onderzoek aan voorwerpen ter vaststelling van de identiteit van een persoon is eenvoudig: vaststellen wie de persoon is aan de hand van een voorwerp waarop deze sporen heeft achtergelaten. In die zin heeft art. 28 Wiv 20xx een duidelijk doel – hetzelfde als art. 27 lid 1 onder c, maar dan, vanwege de grotere privacyinbreuk, zelfstandig geregeld. Ook als men de interpretatie volgt dat art. 22 Wiv 2002 geen grondslag biedt voor dit type DNA-onderzoek, en het dus om een uitbreiding gaat, valt de noodzaak van deze regeling te begrijpen: DNA-onderzoek is inmiddels mogelijk op minieme hoeveelheden celmateriaal, en biedt daarom, zeker gezien de grote betrouwbaarheid, een belangrijke aanvulling op het vaststellen van de identiteit aan de hand van vingerafdrukken. De relatief lichte extra inbreuk op de privacy ten opzichte van vingerafdruk (mits beperkt tot het enkele vaststellen van de identiteit, zie par. 6.2) kan daarbij de noodzakelijkheidstoets van art. 8 EVRM zeker doorstaan.

De voorgestelde regeling beperkt zich echter niet tot het minimum noodzakelijke voor het doeleinde van het vaststellen van de identiteit van een persoon aan de hand van een voorwerp. Het gaat in feite om een hybride regeling, waarbij twee verschillende situaties van DNA-onderzoek aan de orde zijn, die in het wetsontwerp en de toelichting door elkaar lopen. Dat blijkt uit de volgende passage:

> 'Het DNA-onderzoek vindt plaats door vergelijking van DNA-profielen. Deze vergelijking kan plaatsvinden aan de hand van DNA-profielen die bij

[69] Daaronder wordt ook verificatie van de identiteit verstaan, in gevallen waarin er twijfel bestaat of de veronderstelde identiteit van een target wel klopt. Dat levert geen aanvullende privacyrisico's op, omdat het vergelijkbaar is met de situatie waarin de identiteit van een target onbekend is. Wel beïnvloedt de reeds beschikbare kennis over de identiteit de invulling van het noodzakelijkheidsvereiste: naarmate de twijfel over de identiteit groter is, zal DNA-onderzoek sneller voldoen aan de vereisten van subsidiariteit en proportionaliteit. Hierop zal de toezichthouder moeten (blijven) toezien, zoals ook gedaan in CTIVD (2015a).

externe (binnen- en buitenlandse) instanties berusten, zoals aan de hand van de DNA-profielen opgenomen in de DNA-databank voor strafzaken, maar ook aan de hand van DNA-profielen die men zelf verwerkt en voor (toekomstige) vergelijking opslaat. Het vastleggen van DNA-profielen door de diensten zelf is noodzakelijk, omdat de vergelijking van de DNA-profielen die voor diensten zijn vastgesteld met DNA-profielen die bij externe instanties zijn vastgelegd, niet altijd een resultaat opleveren; niet alle targets van de dienst hebben immers een strafrechtelijk verleden en zijn in verband daarmee in de DNA-databank voor strafzaken opgenomen. Vergelijking met DNA-profielen die de diensten zelf hebben vastgelegd moet dan ook tot de mogelijkheden behoren om anderszins tot vaststelling of verificatie van de identiteit te komen. Zo heeft de AIVD recent in het kader van internationale samenwerking tegen terrorisme de beschikking gekregen over de DNA-profielen van een aantal zelfmoordterroristen, die echter geen hit opleverde in de DNA-databank voor strafzaken. Indien het toch Nederlandse targets zijn, maar geen strafrechtelijk verleden hebben, dan zitten zij immers ook niet in de DNA-databank voor strafzaken. De kans op een hit wordt dan vergroot indien de dienst zelf van uitreizende targets DNA-profielen heeft opgeslagen waarmee kan worden vergeleken.' (MvT, p. 47)

Hier worden twee verschillende scenario's op één hoop gegooid:

1. De dienst wil de identiteit van een persoon vaststellen die fysiek in beeld is bij een agent of informant, waarvan de identiteit *op dit moment* onbekend of onvoldoende zeker is. Om te weten wie deze persoon is, wordt een voorwerp waarvan duidelijk is dat daarop sporenmateriaal van deze persoon is achtergebleven (een koffiekopje, bierglas, tandenborstel) meegenomen en onderzocht op celmateriaal. Het daaruit afgeleide DNA-profiel wordt vergeleken met een beschikbare databank, waarbij een treffer de gezochte identiteit van de persoon oplevert. Dit levert identificatie op als de identiteit onbekend was, en verificatie als er wel aanwijzingen waren over de identiteit maar er nog onvoldoende zekerheid bestond dat dat ook de echte identiteit was.
2. De dienst wil in de toekomst sporen kunnen identificeren van mensen van wie *op dit moment* de identiteit voldoende bekend is, maar waarbij men verwacht dat het *in de toekomst* nodig kan zijn om deze te moeten kunnen identificeren aan de hand van een DNA-profiel. Met name gaat het om de mogelijkheid om toekomstige zelfmoordterroristen te kunnen identificeren aan de hand van DNA-onderzoek. Omdat niet alle zelfmoordterroristen in beschikbare forensische DNA-databanken zitten, wil de dienst een eigen databank opzetten waarin DNA-profielen van 'uitreizende targets' worden opgenomen. Zo wordt de kans vergroot dat zelfmoordterroristen aan de hand van de eigen databank in de toekomst kunnen worden geïdentificeerd.

Het gaat hier om verschillende scenario's waar verschillende behoeften aan ten grondslag liggen. Ten onrechte doet het wetsontwerp het voorkomen alsof het tweede scenario voortvloeit uit het eerste. Dat is niet het geval. De 'uitreizende targets', oftewel personen van wie vermoed wordt dat zij een verhoogd risico lopen om te radicaliseren en, al dan niet na een Syriëreis, een zelfmoordaanslag te plegen, zullen veelal bekend zijn bij de diensten. Het gaat meestal om jongeren die voor een zekere periode worden gevolgd en die met naam en toenaam bekend zijn, of waarvan in elk geval met reguliere middelen de identiteit eenvoudig kan worden vastgesteld. Voor potentiële Syriëgangers en radicaliserende jongeren zal het niet

nodig zijn om DNA-onderzoek te doen aan voorwerpen om hun identiteit vast te stellen of te verifiëren. Als hun DNA-profiel via DNA-onderzoek aan voorwerpen wordt gegenereerd, zal dat uitsluitend, of in elk geval hoofdzakelijk, zijn om ze in de databank op te nemen met het oog op toekomstige identificatie van een zelfmoordterrorist. Daarom zal art. 28 lid 1 op deze categorie personen niet van toepassing zijn.

Mocht bedoeld zijn om voor dit scenario lid 1 wel van toepassing te verklaren door de clausule dat ook verificatie van identiteit hieronder valt, en het dus gaat om potentiële zelfmoordterroristen van wie de identiteit reeds bekend is, dan is dat een misleidende toepassing van het DNA-onderzoek als bedoeld in art. 28 lid 1 – dat ziet immers op scenario 1, niet op scenario 2. Het 'verifiëren' van de identiteit is niet noodzakelijk in deze gevallen. Als het de bedoeling is dat ook DNA-onderzoek mogelijk is bij personen van wie de identiteit reeds voldoende bekend is (of waarvan de identiteit ook met minder ingrijpende middelen kan worden vastgesteld), met het doel om *toekomstige* identificatie mogelijk te maken, en aldus de eigen databank van potentiële zelfmoordterroristen te vullen, dan vergt dat een zelfstandige regeling, waarvan de toelichting ook expliciet de noodzaak zou moeten motiveren, omdat de noodzaak hiertoe in de huidige toelichting volstrekt niet wordt aangetoond (zie nader hieronder, par. 6.6).

De conclusie is dat de twee verschillende scenario's in de voorgestelde regeling en in de toelichting veel scherper uit elkaar moeten worden getrokken, waarbij de noodzaak voor elk van beide scenario's afzonderlijk moet worden aangetoond.

### 6.4 Doelbinding en verstrekking aan derden

Artikel 28 lid 4 regelt doelbinding maar biedt tegelijkertijd de mogelijkheid van verdere verwerking, mits daarvoor een nieuwe grondslag wordt verkregen in de vorm van toestemming van de Minister:

> 4. De resultaten van een DNA-onderzoek mogen uitsluitend worden verwerkt voor het onderzoek ten behoeve waarvan de toestemming is verleend. Elk verdere verwerking is slechts toegestaan, indien daarvoor toestemming is verkregen van Onze betrokken Minister. Het verzoek om toestemming wordt gedaan door het hoofd van de dienst en bevat in aanvulling op hetgeen in artikel 24, zesde lid, is bepaald:
>    a. een nauwkeurige omschrijving van de beoogde verdere verwerking;
>    b. voor zover het de verstrekking van de resultaten van het DNA-onderzoek aan een derde betreft, welke derde het betreft.

Met 'resultaten van een DNA-onderzoek' wordt hierbij niet gedoeld op de aldus vastgestelde identiteit, maar het DNA-profiel, blijkens de toelichting ('Gebruik van DNA-profielen in het kader van andere onderzoeken van de dienst of bijvoorbeeld ter verstrekking aan een andere instantie, vergt altijd een afzonderlijke en op die verdere verwerking toegespitste toestemming van de voor de desbetreffende dienst verantwoordelijke minister', MvT, p. 48). Het is goed voor de privacybescherming dat de verdere verwerking, inclusief verstrekking aan derden, wordt begrensd door de eis daarvoor toestemming op ministerieel niveau te verkrijgen.

Verstrekking aan derden, zoals buitenlandse diensten of Nederlandse justitie, levert echter wel een privacyrisico op, omdat de beschikkingsmacht uit handen wordt gegeven. Wet noch toelichting geven aan of er eisen (kunnen of moeten) worden gesteld bij de verstrekking van een DNA-profiel aan derden. Dat levert een risico op dat het profiel vervolgens door de derde in een databank wordt bewaard, mogelijk voor zeer lange tijd of voor zeer verschillende doeleinden, wat in strijd kan zijn met de eisen van het EVRM.[70] Het is onduidelijk waarom dat mogelijk zou moeten zijn. De wet of toelichting zou duidelijk kunnen maken dat bij het verstrekken eisen kunnen worden gesteld aan het gebruik, waarbij met name gestipuleerd zou kunnen worden dat het profiel wel mag worden gebruikt voor vergelijking met een ander profiel of met een databank (dat zal immers meestal het doeleinde van verstrekking zijn), maar niet in een databank mag worden opgenomen. Met name bij verstrekking van een DNA-profiel aan justitie zou dat een belangrijke voorwaarde moeten zijn, tenzij er termen zijn om het profiel wel in de justitiële databank op te nemen conform de regeling in strafvordering en het DNA-besluit.

Ook zou de wet of toelichting duidelijk kunnen maken dat verstrekking aan derden alleen mogelijk is als het doel niet door vergelijking van DNA-profielen door de dienst zelf kan worden gedaan. In gevallen waarin de derde identificatiegegevens zoekt bij een DNA-profiel van een spoor van een onbekend persoon (bijvoorbeeld een bij een zelfmoordaanslag omgekomen persoon), is het voor de privacybescherming beter als deze derde het DNA-profiel van het spoor aan de dienst verstrekt om een vergelijking te maken, waarbij de dienst kan antwoorden of deze persoon bekend is en zo ja, wie het betreft, dan dat de dienst zelf DNA-profielen aan de buitenlandse dienst verstrekt.

## 6.5 Bewaartermijn celmateriaal

Het celmateriaal kan uitsluitend worden gebruikt om een DNA-profiel te genereren en moet dan binnen drie maanden worden vernietigd:

> 5. Door de diensten vergaard celmateriaal ten behoeve van een onderzoek als bedoeld in het eerste lid wordt binnen drie maanden na het DNA-onderzoek vernietigd. Van de vernietiging wordt een verslag gemaakt.

De Memorie van Toelichting licht dit als volgt toe: ‘Indien met betrekking tot het celmateriaal DNA-onderzoek heeft plaatsgevonden, dient dit materiaal zo spoedig mogelijk doch uiterlijk binnen drie maanden na het onderzoek te worden vernietigd. Een zo kort mogelijke vernietigingstermijn is met name aangewezen, nu het bewaren van celmateriaal als drager van genetische en gezondheidsinformatie, in bijzondere mate inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer van personen die het betreft. Aangezien de vernietiging van het celmateriaal op een gecontroleerde wijze dient plaats te vinden, waarbij ook de aanwezigheid van de forensisch expert van de dienst is vereist, is vernietiging niet altijd direct na het onderzoek mogelijk; om die reden is een termijn van maximaal drie maanden opgenomen. Van de vernietiging dient een verslag te worden gemaakt.’ (MvT, p. 48)

Hieruit spreekt het belang het celmateriaal niet langer dan absoluut noodzakelijk te bewaren, om het risico zoveel mogelijk te beperken dat het in de tussentijd voor

[70] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk.

andere doeleinden kan worden misbruikt (door de diensten of door derden die er onrechtmatig toegang toe krijgen). Toch is het onduidelijk waarom het celmateriaal nog tot drie maanden na het onderzoek zou moeten kunnen worden bewaard. De termijn gaat in vanaf het moment dat uit het celmateriaal het DNA-profiel is afgeleid. De enige reden die de MvT om het materiaal niet terstond te vernietigen, is dat de forensische expert van de dienst erbij aanwezig moet zijn en die niet altijd direct beschikbaar is. Daarbij wordt niet toegelicht waarom de forensische expert van de dienst aanwezig moet zijn (en bijvoorbeeld niet een forensische expert van het NFI of een ander forensisch instituut waar het DNA-onderzoek zelf plaatsvindt, waar per definitie ook forensische experts aanwezig zijn, die mogelijk ook in staat zijn toe te zien op gecontroleerde vernietiging en daarvan een verslag te maken). Ook wordt niet toegelicht waarom het tot drie maanden kan duren dat de forensische expert van de dienst aanwezig kan zijn; wellicht is er sprake van drukke agenda's, een deeltijdfunctie of vakantieperiodes, maar het is moeilijk te begrijpen waarom privacyrisico's moeten worden gelopen om uitsluitend praktische en intern-organisatorische redenen. Als er meer fundamentele redenen zijn voor deze termijn van drie maanden, dan zou de MvT die beter voor het voetlicht moeten brengen; anders zou een termijn van twee weken of een maand meer aangewezen zijn.

Verder valt het aan te bevelen om de urgentie van vernietiging meer in de wettekst zelf naar voren te laten komen. Nu bepaalt lid 5 dat het materiaal 'binnen drie maanden' vernietigd moet worden, terwijl de toelichting veel scherper is: 'zo spoedig mogelijk doch uiterlijk binnen drie maanden'. Voor de rechtszekerheid is het van belang om deze scherpere formulering in de wettekst zelf op te nemen.

### 6.6 Een eigen DNA-databank

De ingrijpendste uitbreiding van bevoegdheden betreft het oprichten van een eigen DNA-databank bij de diensten:

> 6. Het door of ten behoeve van de dienst vervaardigde DNA-profiel wordt voor ten hoogste vijf jaren bewaard en daarna vernietigd. Op een daartoe strekkend verzoek van het hoofd van de dienst aan Onze betrokken Minister kan de bewaartermijn telkens voor ten hoogste vijf jaren worden verlengd. Artikel 24, zesde lid, is van overeenkomstige toepassing.
> 7. Bij algemene maatregel van bestuur worden in ieder geval regels gesteld voor het verwerken van DNA-profielen, waaronder begrepen de inrichting, het beheer en de toegang tot deze gegevens, en celmateriaal. De voordracht voor een krachtens de eerste volzin vast te stellen algemene maatregel van bestuur wordt niet eerder gedaan dan vier weken nadat het ontwerp aan beide kamers van de Staten-Generaal is overgelegd.

Voorgesteld wordt een DNA-databank bij de diensten in te richten waarin alle door de diensten gegenereerde profielen worden opgeslagen voor vijf jaar, of zoveel langer als nodig wordt geacht, waarbij geen absolute bovengrens aan de bewaartermijn wordt gesteld.

Het opslaan van DNA-profielen maakt inbreuk op de privacy, minder dan de opslag van DNA-materiaal maar meer dan de opslag van vingerafdrukken.[71] Er zijn specifieke risico's verbonden aan opslag van DNA-profielen. Het EHRM benadrukt

[71] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk.

dat DNA-profielen ook kunnen worden gebruikt voor verwantschapsonderzoek, zodat niet alleen de persoonlijke levenssfeer van betrokkenen in het geding is, maar ook van hun familie. Bovendien kunnen hierdoor verwantschapsrelaties (of het ontbreken daarvan) worden vastgesteld waarmee de betrokkenen of hun familie onbekend zijn.[72] De MvT zegt niets over verwantschapsonderzoek en laat daarmee de mogelijkheid open dat de identiteit van targets ook kan worden vastgesteld op basis van verwantschapsonderzoek; anders dan bij het afleiden van persoonskenmerken wordt deze techniek immers niet expliciet uitgesloten in de toelichting. Ook stelt het EHRM dat de vermoedelijke etnische afkomst op basis van het DNA-profiel zou kunnen worden vastgesteld;[73] het is de vraag of het afleiden van etnische afkomst voldoende betrouwbaar is, en sowieso is dit niet toegestaan voor de diensten,[74] maar aangezien het profiel beschikbaar is (ook voor derden, en potentieel voor hackers) valt het risico van deze privacyinbreuk niet volledig uit te sluiten.

Een ander risico is ‘function creep’, het geleidelijk uitbreiden van de functionaliteit van een systeem voor andere doeleinden dan waarvoor het oorspronkelijk is opgezet. Dit is een reëel risico, met name omdat het bestaan van een DNA-databank bij de inlichtingen- en veiligheidsdiensten, zeker als daar potentiële jihadstrijders of zelfmoordterroristen in zitten, aantrekkelijk is om ook voor opsporingsdoeleinden te gebruiken. Het feit dat de databank er is, maakt het makkelijker om, in een incidenteel geval maar ook structureel door de wet aan te passen, om het mogelijk te maken voor justitie om ook in de databank van de diensten te kijken als zij een spoor van een onbekende dader hebben. Het in het leven roepen van een databank bij de diensten bergt dan ook een zeker risico in zich dat een ‘schaduw-databank’ ontstaat ter aanvulling op de forensische databank, die in de toekomst voor steeds meer doelen gebruikt wordt (zoals ook de functionaliteit van het forensische DNA-onderzoek de afgelopen decennia steeds is uitgebreid). Dat zal (op dit moment) niet de bedoeling zijn, maar de ervaring leert dat databanken die eenmaal zijn opgericht, er in de politieke werkelijkheid om ‘vragen’ om ook voor andere doeleinden te worden gebruikt, zeker als er prominente aanslagen worden gepleegd en de politiek daadkracht wil tonen. Hoewel uitdrukkelijke uitspraken in de MvT dat zulke uitbreiding van de functionaliteit van de databank niet de bedoeling is, kunnen helpen om dit risico enigszins te beperken, hebben die uitspraken weinig waarde in een toekomstige politieke discussie. De beste manier om dit risico in te perken, is om geen databank op te richten. Omgekeerd betekent dit dat de noodzaak om de databank op te richten des te sterker moet worden aangetoond, wil het risico van *function creep* gerechtvaardigd zijn.

Het EHRM eist dat de opslag van profielen proportioneel is in relatie tot het doel van de verzameling van het profiel en beperkt in bewaartermijn.[75] Op deze punten voldoet het wetsontwerp niet. Er wordt niet duidelijk gemaakt waarom het opzetten van een eigen DNA-databank *noodzakelijk* is in een democratische samenleving. De enige reden die de MvT geeft is dat opslag nuttig is met het oog op het in de toekomst kunnen identificeren van toekomstige zelfmoordterroristen. Deze redengeving schiet om twee redenen te kort.

[72] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §75.
[73] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §76.
[74] Zie noot 67.
[75] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §107.

Ten eerste is nut niet hetzelfde als noodzaak. Het wordt niet gemotiveerd wat het precieze belang is van identificatie van zelfmoordterroristen. Het is evident dat identificatie wenselijk is, maar of het ook een 'pressing social need' oplevert, zou nader moeten worden gemotiveerd. Ook wordt niet duidelijk gemaakt hoe groot de kans is dat bij een zelfmoordaanslag aangetroffen lichaamsmateriaal op basis van de eigen databank geïdentificeerd kan worden, en dus ook niet hoe groot de verwachte meerwaarde van een DNA-databank is. Daar komt bij dat deze categorie personen vastgesteld wordt op basis van risicotaxatie, waarbij het uit de aard der zaak gaat om personen die nog niet eerder een zelfmoordaanslag hebben gepleegd. Die categorie is vergelijkbaar met de categorie verdachten in het strafrecht, en niet met de categorie veroordeelden. Van de laatsten is het opslaan in een DNA-databank breed geaccepteerd; bij de eersten past echter grotere terughoudendheid om deze in een databank op te slaan. Niet voor niets heeft het EHRM duidelijke grenzen gesteld aan het bewaren in een databank van niet-veroordeelde personen in de zaak-S. en Marper.[76] In dat licht is het twijfelachtig of het proportioneel is om DNA-profielen van *potentiële toekomstige* zelfmoordterroristen in een databank op te slaan, zeker voor een (telkens verlengbare) termijn van vijf jaar. Verder worden er ook geen alternatieve mogelijkheden besproken om identificatie in dergelijke gevallen te verkrijgen. Er kunnen bijvoorbeeld aanwijzingen zijn om wie het mogelijk gaat, en kan het veelal mogelijk zijn dat de familie – die ook een groot belang heeft bij identificatie – op vrijwillige basis DNA-materiaal afstaat, waarbij een partiële treffer (op ongeveer de helft van de meetpunten) voldoende bewijs oplevert van de identiteit. Het betreft dan een relatief lichte privacyinbreuk (verwantschap tussen twee concrete profielen vaststellen of uitsluiten, vergelijkbaar met een ouderschapstest), die niet problematisch is als er sprake is van vrijwilligheid en het celmateriaal en het profiel alleen voor dit doeleinde worden gebruikt (en vervolgens worden vernietigd). Een dergelijk alternatief zal niet in alle gevallen mogelijk zijn, maar aangezien een eigen DNA-databank nooit alle zelfmoordterroristen uit Nederland zal bevatten (het valt immers niet altijd op voorhand te voorspellen, en ook zal het niet bij iedere 'afreizende target' die wel in beeld is, lukken om DNA-materiaal te pakken te krijgen voordat deze afreist), zullen de diensten sowieso alternatieve mogelijkheden moeten ontwikkelen. Al met al wordt de noodzaak van een DNA-databank volstrekt onvoldoende onderbouwd.

Ten tweede gaat het om een zeer specifieke groep. Op basis van de MvT ligt de behoefte voor toekomstige identificatie niet bij alle targets van wie de identiteit vastgesteld wordt op basis van DNA-onderzoek aan een voorwerp – het hierboven geschetste scenario 1 – maar specifiek voor een subgroep van targets, namelijk potentiële zelfmoordterroristen. Als daarvoor het aanleggen van een databank al nodig zou zijn (wat dus nog aangetoond zou moeten worden), dan zou de databank beperkt moeten worden tot deze specifieke groep. In het kader van de voorzienbaarheid bij wet, alsook voor de proportionaliteit en subsidiariteit, is het belangrijk dat privacyinbreuken beperkt zijn tot een zo nauw mogelijk omschreven groep. Het is disproportioneel om alle targets van wie de diensten een DNA-profiel hebben gegenereerd, in een databank op te slaan, als het hoofddoel van de databank is om toekomstige zelfmoordterroristen te kunnen identificeren. De databank zou dan ook (nogmaals, als de noodzaak ervan wordt aangetoond) beperkt moeten zijn tot de specifieke categorie voor wie de databank bedoeld is.

[76] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §125.

Voor de omschrijving daarvan kan bijvoorbeeld aangesloten worden bij de omschrijving in het strafrecht die het beste aansluit bij de desbetreffende categorie potentiële zelfmoordterroristen (bijvoorbeeld werving voor de gewapende strijd, of voorbereiding van moord met een terroristisch oogmerk). De beperking tot deze categorie zou bij voorkeur in de wet zelf moeten staan. Indien voorzienbaar is dat de noodzaak van toekomstige identificatie ook voor andere categorieën targets kan gaan spelen (daarvan zou de toelichting dan wel enige voorbeelden moeten geven om dit aannemelijk te maken), zou de beperking ook in de AMvB (op basis van lid 7) kunnen worden vastgelegd. Belangrijk is dan wel dat de voorhangprocedure van de AMvB verzwaard wordt. Nu bepaalt lid 7 dat de ontwerp-AMvB aan het parlement wordt voorgelegd, maar zonder de bepaling dat het parlement binnen een termijn van vier weken kan eisen dat het onderwerp of de inwerkingtreding bij wet wordt geregeld (de zware voorhangprocedure).

Naast de niet-aangetoonde noodzaak, is het ook twijfelachtig of de voorgestelde bewaartermijn proportioneel is in het licht van de privacyrisico's. Hoewel er na vijf jaar verlenging gevraagd moet worden met motivering van de noodzaak tot verlenging, bestaat de mogelijkheid om het profiel voor onbepaalde tijd te bewaren, zolang als het nodig wordt gevonden. Zolang de wet niet voorziet in bindend advies van een onafhankelijke toezichthouder, is er geen onafhankelijk toezicht op deze bewaarmogelijkheid. Het wetsvoorstel komt dan zeer dicht in de buurt bij de 'the blanket and indiscriminate nature of the powers of retention of the (…) DNA profiles of persons suspected but not convicted of offences' waarvan het EHRM in *S. en Marper* heeft vastgesteld dat dit in strijd is met het verdrag.[77]

Ook is het onduidelijk hoe de bewaartermijn wordt gehanteerd als een profiel op basis van lid 4 voor een ander doel wordt gebruikt. De bewaartermijn van het eerste doel loopt na vijf jaar af (als er geen grondslag is voor verlenging), maar het profiel kan niet worden vernietigd zolang de bewaartermijn voor het tweede doel nog loopt. Dat levert een risico op dat het profiel na afloop van de wettelijke bewaartermijn voor het specifieke doel waarvoor het profiel is opgeslagen, alsnog voor dat doel kan worden gebruikt. Mogelijk kan dit worden opgelost door de doelen met 'sticky policies' aan de profielen in de databank te verbinden en door organisatorische toegangsmaatregelen, maar zou dan wel adequaat moeten worden geregeld in de AMvB, met onafhankelijk toezicht.

Concluderend stellen we vast dat de noodzaak voor de oprichting van een DNA-databank bij de diensten niet is aangetoond. Er worden geen klemmende redenen aangevoerd die de privacyrisico's (waaronder verwantschapsonderzoek, gebruik voor andere doelen en door derden, en *function creep*) rechtvaardigen. Mocht er wel een 'pressing social need' zijn om toekomstige zelfmoordterroristen na de aanslag te kunnen identificeren, en dit doel aantoonbaar niet met andere middelen kunnen worden bereikt, dan moet de wet om DNA-profielen op te slaan beperkt worden tot deze specifieke groep. Daarbij zou dan ook de bewaartermijn nader moeten worden ingeperkt, met een absoluut maximum dat proportioneel is voor het doel van opslag voor deze specifieke groep.

[77] EHRM 4 december 2008, S. en Marper t. Verenigd Koninkrijk, §125.

# 7 Ruimtelijke privacy

Onder ruimtelijke privacy verstaan we privacy in relatie tot bepaalde plaatsen; de belangrijkste verschijningsvorm hiervan is van oudsher het huisrecht (art. 12 Gw). Ook bij andere besloten plaatsen (bijvoorbeeld bedrijven) wordt de privacy enigermate beschermd. Privacy in de publieke ruimte wordt tot nu toe niet als zodanig beschermd, maar met de toenemende mogelijkheden om mensen in de publieke ruimte langdurig en gedetailleerd te volgen, neemt ook de privacygevoeligheid van gedrag in het openbaar toe. Daarom is het bij ruimtelijke privacy niet alleen relevant om te kijken naar bevoegdheden in relatie tot woningen of besloten plaatsen, maar ook naar de observatiebevoegdheden in het algemeen.

Hoewel een computersysteem niet als zodanig een bepaalde 'plaats' is (met draagbare computers zijn computers juist in belangrijke mate plaatsonafhankelijk geworden), behandelen we het binnendringen in computers in dit rapport onder ruimtelijke privacy. Hoewel computersystemen ook samenhangen met informationele privacy en relationele privacy, hebben ze een belangrijke ruimtelijke dimensie, in de zin dat ze een ruimte op zichzelf vormen waar de persoonlijke levenssfeer zich in steeds belangrijker mate afspeelt. Niet voor niets wordt Internet vaak aangeduid als cyber*space*, een abstracte ruimte waarbinnen digitale en genetwerkte activiteiten worden uitgevoerd. De koppeling met ruimtelijke privacy en het huisrecht wordt daarnaast ook ingegeven door het feit dat de wetgever computervredebreuk (art. 138ab Sr) heeft vormgegeven naar analogie met, en geplaatst aansluitend op, huisvredebreuk (art. 138 Sr).[78]

## 7.1 Observatie en onderzoek van plaatsen

### *7.1.1 Inleiding*

Hier zijn drie artikelen relevant. Artikel 25 (observeren en volgen, zowel binnen als buiten besloten plaatsen) is ongewijzigd ten opzichte van de huidige wet (art. 20 Wiv 2002). Artikel 27 (onderzoek van plaatsen en voorwerpen) is in enkele opzichten gewijzigd ten opzichte van de bestaande bevoegdheid (art. 22 Wiv 2002). Voor ons is vooral relevant dat het huidige art. 22 lid 5 Wiv 2002 bepaalt dat de toestemming voor het doorzoeken van woningen verleend wordt voor ten hoogste drie dagen; deze bepaling keert niet terug, maar de beperking tot drie dagen blijft bestaan omdat een machtiging conform de Algemene wet op het binnentreden nodig is, die hooguit drie dagen geldig is (art. 6 lid 2 Awbi, een bepaling waarnaar de MvT in relatie tot deze artikelen (p. 39, 44-46) wel specifieker zou kunnen verwijzen). Artikel 42 biedt een steunbevoegdheid van toegang tot plaatsen; deze is gewijzigd ten opzichte van het bestaande artikel 30 Wiv 2002, hoofdzakelijk door toe te voegen dat plaatsen ook kunnen worden betreden om technische middelen te vervangen of te verwijderen.

[78] Vgl. ook BVerfG [Duits Constitutioneel Hof] 27 februari 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007, beschikbaar op http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, Engelse vertaling http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html, waarin een grondrecht op vertrouwelijkheid en integriteit van computersystemen wordt bepaald dat verankerd is in het huisrecht en het communicatiegeheim.

In de MvT wordt aangegeven dat voor artikel 25 de toestemming voor inzet van observatie- en registratiemiddelen binnen de woning alleen door de betrokken minister gegeven kan worden en geldig is voor ten hoogste drie maanden (p. 38-39). Om de apparatuur te plaatsen is, vanwege het heimelijke karakter, een machtiging nodig voor het binnentreden van de woning zonder toestemming van de bewoner. Deze machtiging wordt eveneens door de betrokken minister afgegeven, dan wel namens deze door het hoofd van de dienst. De machtiging voor binnentreden is drie dagen geldig, maar kan meerdere keren worden afgegeven gedurende de periode van observatie (p. 39).

Omdat het binnentreden in de woning zonder toestemming van de bewoner een inbreuk oplevert op artikel 12 Gw gelden ook de vormvereisten uit art 12(2) Gw, waaronder notificatie achteraf. Het belang van de nationale veiligheid kan zich echter onder omstandigheden tegen notificatie verzetten (art. 12(3) Gw). Artikel 27 en 42 van het wetsvoorstel en de Algemene wet op het binnentreden geven gezamenlijk uitwerking aan de grondwettelijke vereisten voor de inbreuk (MvT, p.194).

### *7.1.2 Algemene beschouwing over het huisrecht*

Gezien de ontwikkelingen op technologisch gebied is het belangrijk te kijken naar de impact van middelen om activiteiten binnen de woning te observeren en vast te leggen, zonder daadwerkelijk de woning te betreden. Het huidige artikel 12 Gw beschouwt het huisrecht als een bescherming tegen binnentreden (zonder toestemming) van de woning; dat was van oudsher de belangrijkste inbreuk op het huisrecht, omdat bewoners zich tegen andere bedreigingen—het van buiten naar binnen kijken—makkelijk zelf konden beschermen door de gordijnen dicht te doen. Dit is echter achterhaald, omdat bewoners zich veel moeilijker kunnen beschermen tegen de vele huidige (en toekomstige) technische mogelijkheden om van buitenaf te weten te komen wat er zich binnen de woning afspeelt—denk aan warmtebeeldkijkers (waarmee hennepplantages kunnen worden opgespoord, maar waarmee ook in zekere mate kan worden achterhaald hoeveel, en waar, personen zich in een woning bevinden), richtmicrofoons, chemische analyse van rioolafvoer en het aftappen van Internetverkeer (waarmee in het Internet der Dingen in toenemende mate ook huishoudelijke apparaten, zoals nu al de verwarming, worden aangestuurd). Ook via het opvragen van gegevens bij dienstverleners, zoals elektriciteitsbedrijven, kan het nodige inzicht worden verkregen over wat zich afspeelt binnen de woning, zeker als die een slimme meter heeft die met korte intervallen meet (waaruit leefpatronen en gebruik van apparatuur af te leiden valt).[79] Niet al deze technieken vallen onder observatie als bedoeld in art. 25 (voor opvragen van gegevens en aftappen, zie par. 5.1en hfd.8), maar relevant is wel, vanuit het oogpunt van ruimtelijke privacy, dat een beperking van het huisrecht tot het fysiek binnentreden in de woning te beperkt is.

Hoewel de grondwetgever dit punt, ondanks eerdere kritiek vanuit de literatuur,[80] nog niet heeft willen onderkennen, en art. 12 Gw vooralsnog formeel beperkt blijft tot bescherming tegen fysiek binnentreden, vraagt een adequate bescherming van privacy in de 21e eeuw dus om een ruimere opvatting van het huisrecht, namelijk

[79] Vgl. Cuijpers en Koops 2008.

[80] Koops, Van Schooten en Prinsen 2004. In beperkte mate ook Commissie-GDT 2000, p. 207 (betogend dat het met richtmicrofoons afluisteren van gesprekken in een woning zou moeten voldoen aan de vereisten van art.12 Gw van notificatie en het bij of krachtens wet aangewezen zijn van bevoegde functionarissen).

als een bescherming tegen het (zonder toestemming) kennisnemen van wat zich binnen de woning afspeelt. De (lagere) wetgever in formele zin mag zich op dit punt niet verschuilen achter een verouderde, 20e-eeuwse grondwetsbepaling en moet een effectieve bescherming van het huisrecht bieden die recht doet aan de technische mogelijkheden van de 21e eeuw. De nieuwe Wiv zou daarom in het algemeen, gezien het feit dat het huisrecht van oudsher een van de belangrijkste hoekstenen is van privacybescherming, een sterke bescherming moeten bieden tegen elke bevoegdheid waarbij kennis wordt genomen van wat zich binnen een woning afspeelt.

### *7.1.3 Algemene beschouwing over privacy in de publieke ruimte*

Van oudsher heeft men weinig (maar wel enige[81]) privacybescherming in de publieke ruimte, dat wil zeggen buiten besloten plaatsen die niet voor het publiek toegankelijk zijn. Daar was ook niet bijzonder veel behoefte aan, om twee redenen – beide inmiddels achterhaald.

Ten eerste vond het privéleven in behoorlijke mate plaats in besloten plaatsen, met name binnenshuis; de meest gevoelige privéactiviteiten deed men thuis, en de dingen die het meeste inzicht gaven in het persoonlijke leven, zoals papieren, foto's en boeken, bewaarde men binnenshuis. Dit is achterhaald, nu mensen hun privéleven bij zich dragen op smartphones dan wel beheren via de cloud, en daarmee ook meer privéactiviteiten uitoefenen terwijl zij zich in de openbare ruimte begeven – veel mensen gedragen zich op straat, in de trein of in het café alsof ze in een privébubbel zitten.

Ten tweede was er voorheen een behoorlijke natuurlijke drempel om mensen in de publieke ruimte te volgen; weliswaar is het zichtbaar wat iemand in de publieke ruimte doet, maar dat zijn momentopnamen. Voor een stelselmatig inzicht in iemands leven moet men de persoon voor langere tijd volgen. Vroeger kostte dat de nodige tijd en moeite, maar met de huidige technologische mogelijkheden is het veel eenvoudiger en goedkoper geworden om mensen te volgen. Dit was al zo bij de totstandkoming van de Wiv 2002, maar deze tendens heeft zich sindsdien nog sterker doorgezet, bijvoorbeeld door WiFi-tracking, (mobiele) miniatuurcamera's, drones en locatie-gebaseerde apps. Dit wordt versterkt door de opkomst van het Internet der Dingen en allerlei *smart city*-toepassingen waarmee via een netwerk van sensoren individuele en groepspatronen automatisch in kaart kunnen worden gebracht.

Daar komen nog twee ontwikkelingen bij, in de eerste plaats de opkomst van Big Data en profileringstechnologie. Op basis van grote hoeveelheden data, die allemaal uit de publieke ruimte verzameld kunnen zijn en op zichzelf nauwelijks informatief zijn, kunnen vergaande conclusies worden getrokken over iemands interessesfeer en privéleven. Met name locatiegegevens kunnen veel inzicht bieden in iemands privéleven; wanneer je iemand een paar weken lang continu traceert, ontstaat een tamelijk volledig beeld van een groot deel van iemands persoonlijke leven.[82] In de tweede plaats nemen de mogelijkheden tot identificatie toe, ook geautomatiseerd. Hoewel nu nog niet voldoende betrouwbaar, zal gezichtsherkenning binnen afzienbare tijd een dusdanig betrouwbare herkenning opleveren dat dit ook voor veiligheidsdiensten interessante toepassingen kan

[81] EHRM 24 juni 2004, Von Hannover t. Duitsland.
[82] Vgl. Tokmetzis 2013.

opleveren. Het hoeft daarbij niet te gaan om het herkennen van personen met 99,9% betrouwbaarheid – het automatisch herkennen van interessante personen of doelwitten, zowel op beeldmateriaal op Internet als in de fysieke ruimte, zou ook met 80% betrouwbaarheid al interessant kunnen zijn als startpunt van nader onderzoek. Voor de Wiv 20xx moet er in elk geval rekening mee worden gehouden dat de observatie- en registratiemiddelen van artikel 25 binnen 5 tot 10 jaar ook gezichtsherkenningstoepassingen zouden kunnen omvatten, wat de schaal en intensiteit van observatie in de openbare ruimte aanzienlijk kan vergroten ten opzichte van de huidige mogelijkheden.

Door deze ontwikkelingen is het privacyrisico van observatie en volgen veel groter geworden dan het in 2002 was, en zal dit in de nabije toekomst nog aanzienlijk groter worden. Hoewel de eerste tendens nog in zekere mate door burgers zelf kan worden beïnvloed (maar niet volledig, aangezien er een zekere sociale druk lijkt te bestaan om het privéleven 24/7 met anderen te kunnen delen, en dus ook in de openbare ruimte mee te nemen), kunnen burgers zich nauwelijks verweren tegen de tweede tendens. Het permanent gevolgd en herkend kunnen worden is feitelijk alleen te stoppen als men radicaal zijn mobiliteitsgedrag aanpast (en vooral veel thuis blijft) en bijvoorbeeld gezichtsbedekkende kleding gaat dragen in de openbare ruimte (iets wat in het huidige politieke klimaat niet bijzonder op prijs lijkt te worden gesteld). Bovendien zou men met dergelijk gedrag zeer afwijken van wat de gemiddelde burger doet, en daarmee juist boven komen drijven in data-gestuurde analyses waarmee risicoprofielen worden opgesteld. Dit betekent dat de kwetsbaarheid voor privacyinbreuken in de publieke ruimte dusdanig toeneemt, buiten de controle van burgers om, dat hiervoor meer juridische bescherming dan voorheen nodig is. Die juridische bescherming van privacy in de publieke ruimte zal ook in de Wiv 20xx moeten worden geboden, substantieel meer dan voor de Wiv 2002 nodig was.

### *7.1.4 Artikel 25: observeren en volgen*

Voortvloeiend uit de algemene beschouwingen hierboven, zijn er twee typen privacyrisico's bij artikel 25 die aandacht vergen.

1) *Observatie binnen woningen*.

Uit de algemene beschouwing over het huisrecht volgt dat dit niet beperkt moet zijn tot het fysiek binnentreden in de woning, maar ook van toepassing moet zijn op het van buiten naar binnen kijken (met welke technologische middelen dan ook) in de woning. Het gaat daarbij niet om indirecte waarnemingen, waarbij conclusies kunnen worden verbonden aan observatie van de buitenkant van de woning (bijvoorbeeld door te kijken wie naar binnen gaat), maar om directe waarnemingen, dat wil zeggen door observatie die door de muren van de woning heen gaat. Te denken valt aan richtmicrofoons, warmtebeeldkijkers, registratieapparatuur die elektromagnetische straling (zoals van babyfoons, draadloze webcams of draadloze domotica-apparatuur) opvangt, energieverbruiksgegevens doorgegeven door de slimme meter of chemische sensoren die registreren wat door het toilet wordt gespoeld.

Hoewel de tekst van de wet en de Memorie van Toelichting niet uitsluit dat ook deze vormen van 'van buiten naar binnen kijken' onder artikel 25 lid 2 vallen, is het allerminst duidelijk of dat zo bedoeld is. Formuleringen als '[i]ndien observatie- en registratiemiddelen (…) dienen te worden ingezet in woningen' (MvT, p. 38) lijken eerder te wijzen op een fysieke interpretatie van het huisrecht,

namelijk dat alleen toestemming van de Minister nodig zou zijn wanneer technische hulpmiddelen in de woning worden geplaatst. Volgens ons is een dergelijke fysieke interpretatie van het huisrecht niet langer gerechtvaardigd, nu de muren en gordijnen van het huis burgers niet langer feitelijk kunnen beschermen tegen technologische pottenkijkers. De toelichting, en bij voorkeur ook de tekst van de wet zelf, zou ondubbelzinnig duidelijk moeten maken dat ook voor de inzet van observatie- en registratiemiddelen die buiten de woning blijven maar waarmee activiteiten binnen de woning worden geobserveerd of geregistreerd, toestemming van de Minister behoeven. Het huisrecht moet, in andere woorden, technologieneutraal worden geïnterpreteerd en dezelfde bescherming bieden, onafhankelijk van welke technologie wordt gebruikt om kennis te nemen van wat zich binnen de woning afspeelt.

2) *Observatie en volgen buiten woningen*.
In het licht van de algemene beschouwing over privacy in de publieke ruimte is de vraag gerechtvaardigd of de Wiv 20xx wel voldoende waarborgen kent voor het volgen (in ruime zin) van personen in de publieke ruimte. De tekst van artikel 25 mag dan niet veranderd zijn, de praktische uitwerking daarvan is dat wel. Alleen voor het observeren binnen woningen is toestemming van de Minister nodig; daarbuiten volstaat de toestemmingsregeling van artikel 23, wat inhoudt dat de toestemming door het hoofd van de dienst kan worden gemandateerd aan aan hem ondergeschikte ambtenaren. Ook aan de duur van observatie wordt geen harde limiet gesteld; elke drie maanden moet verlenging worden aangevraagd, met onderbouwing van de noodzaak daarvan, maar in beginsel kan observatie jaren duren. Waar observatie plaatsvindt door personen, zit er een natuurlijke drempel in de capaciteit van de diensten, maar waar observatie ook kan worden geautomatiseerd (waarbij medewerkers slechts in actie komen als de observatie tot een signaal leidt) bestaat geen natuurlijke drempel. Aangezien uit stelselmatige observatie van iemands gedrag in de publieke ruimte – ook gedurende een betrekkelijk korte periode van een of twee maanden – een indringend beeld kan ontstaan van iemands privéleven, zijn de huidige waarborgen te minimaal. Te overwegen valt een hoger toestemmingsvereiste in te voeren, dan wel een sterkere beperking aan de duur van observatie en volgen, of beide.

Ook zal toezicht *tijdens* de uitoefening van deze bevoegdheid belangrijk zijn, met name waar deze over langere tijd wordt ingezet, of met meerdere en verschillende hulpmiddelen tegelijkertijd, alsmede wanneer de observatie geautomatiseerd wordt uitgevoerd. Het gaat er daarbij om of uit de losse brokken gegevens, die elk op zich weinig zeggen, een dusdanig beeld ontstaat dat iemands persoonlijke leven duidelijk naar voren komt. Dit noemt men in de Verenigde Staten de mozaïektheorie: een hoopje losse, gekleurde steentjes zegt niets, maar een gestructureerde verzameling van deze steentjes in de vorm van een mozaïek kan heel veelzeggend zijn. Doorlopend en bindend toezicht (zie hfd. 9) is in dat licht niet alleen van belang voor observatie binnen de woning, maar evenzeer voor de inzet van observatie buiten de woning, gezien de hierboven beschreven technische ontwikkelingen, waarbij met name oog moet zijn voor het cumulatieve effect van de verzameling van informatie uit verschillende bronnen en met diverse hulpmiddelen.

Een ander aandachtspunt is dat de technologische mogelijkheden voor het observeren en volgen van personen inmiddels zo omvangrijk zijn, dat het de

vraag is of de privacyinbreuken van artikel 25 nog voldoende voorzienbaar zijn bij wet, nu de MvT niets zegt over de sterk toegenomen mogelijkheden van observatie in de openbare ruimte. De toelichting bij artikel 25 is vaag ('het gaat dan om volgmiddelen, plaatsbepalingapparatuur en registratiemiddelen') dan wel blijft steken in 20e-eeuwse technologie ('daarbij kan worden gedacht aan een verrekijker, foto- en video-apparatuur', p. 38). In hoofdstuk 9 van de Memorie van Toelichting ontbreekt een beschouwing over privacy in de publieke ruimte. Nergens wordt de burger duidelijk gemaakt dat de diensten nu of in de nabije toekomst ook bijvoorbeeld met camera's uitgeruste drones of gezichtsherkenning zullen kunnen gebruiken ter observatie. Het is begrijpelijk dat de toelichting geen gedetailleerd inzicht geeft in operationele observatietechnieken, maar voor de kenbaarheid van de privacyinbreuken zou het op zijn minst wenselijk zijn als de toelichting de burger op hoofdlijnen inzicht geeft in de *typen* observatiemiddelen die de diensten in de 21e eeuw ter beschikking staan. Het noemen van verrekijkers en foto- en videocamera's als voorbeelden is misleidend in een tijdperk waarin de diensten ook technieken als microdrones, WiFi-tracking, chemische sensoren en gezichtsherkenning ten dienste staan. Ook zou de toelichting de burger duidelijk moeten maken dat door combinatie van gegevens over iemands gedrag in de openbare ruimte een scherp beeld kan ontstaan van iemands privéleven.

### *7.1.5 Observatie van sociale media*

De Memorie van Toelichting merkt op dat ook het monitoren van sociale media onder observatie kan vallen: 'Zo is het regelmatig of continu raadplegen van hetgeen door een persoon op door hem gebruikte social media (Twitter, Facebook e.d.) wordt geplaatst eveneens aan te merken als een vorm van (on line) observatie, waarvoor dus toestemming dient te zijn verkregen.' (p. 38) Het is goed dat hier erkend wordt dat het monitoren van sociale media een privacyinbreuk is waarvoor toestemming nodig is. Een enkele opmerking in de toelichting volstaat echter niet om het monitoren van sociale media – en in bredere zin van via het Internet raadpleegbare gegevens – afdoende te normeren.

Onduidelijk is bijvoorbeeld of de opmerking slaat op het raadplegen van voor eenieder toegankelijke informatie op sociale media (dus gegevens waarbij het profiel 'open' staat), of op gegevens op een gesloten profiel, waarbij de gegevens verzameld worden door via een nepprofiel vriend of volger te worden van de te observeren persoon.[83] Het laatste is een aanzienlijk zwaardere inbreuk op de privacy; maar ook het eerste brengt al een potentieel groot privacyrisico met zich, zoals in par. 5.2 is aangegeven.

Bovendien suggereert de MvT hier dat alleen wat iemand zelf plaatst hieronder valt, niet wat anderen over de persoon plaatsen, terwijl dat even ingrijpend is of nog ingrijpender, omdat het informatie betreft waarover de persoon zelf geen controle heeft uitgeoefend. Verder ontbreekt een nadere uitleg wat 'regelmatig' en 'continu' betekenen. Mogelijk wordt hier iets soortgelijks mee bedoeld als met het begrip 'stelselmatig' in de opsporing, oftewel situaties waarbij observatie 'tot resultaat [kan] hebben dat een min of meer volledig beeld wordt verkregen van bepaalde aspecten

[83] De CTIVD heeft hierover een uitspraak gedaan (het construeren van een virtuele identiteit op sociale media betreft een dekmanteloperatie die moet voldoen aan de eisen van art. 21 Wiv 2002 (art. 26 Wiv 20xx), zie CTIVD 2014b, p. 11). De MvT gaat hier echter niet op in, zodat onduidelijk blijft hoe volgens de wetgever het gebruik van een nepprofiel of alias op sociale media onder de Wiv 20xx genormeerd wordt. Zie ook noot 40.

van iemands leven'.[84] Het gaat daarbij niet om een (enigszins) volledig beeld van het hele privéleven, maar om een (enigszins) volledige beeld van een deelaspect – bijvoorbeeld iemands sportleven, uitgaansleven of familieleven. Die drempel wordt al snel gehaald wanneer meer dan incidenteel iemand wordt gevolgd op sociale media. De MvT zou dit explicieter moeten maken. Mocht er een andere interpretatie bedoeld zijn, dan is het wenselijk dat de begrippen nader worden toegelicht, met voorbeelden van wat wel en niet onder 'regelmatig' of 'continu' wordt verstaan.

Daarmee is echter niet gezegd dat met toestemming voor observatie de privacyrisico's afdoende zijn geborgd. Een fundamenteel verschil tussen observatie in de fysieke ruimte en observatie van cyberspace is dat fysieke observatie toekomstgericht is: vanaf het moment van toestemming wordt gevolgd wat een persoon aan het doen is. Online observatie is niet alleen toekomstgericht (monitoren wat iemand vanaf het moment van toestemming op sociale media plaatst), maar omvat tegelijk ook het verleden: alle informatie die tot nu toe door de persoon, of door anderen over de persoon, op Internet is geplaatst. Dit geeft online observatie een principieel ander karakter dan observatie in de fysieke ruimte. Daarom zou observatie van sociale media niet ingelezen moeten worden in de algemene observatiebevoegdheid, maar een sui generis-bevoegdheid moeten zijn (als apart lid van artikel 25 of in een apart artikel, al dan niet gecombineerd met OSINT (zie par. 5.2)), met een op de specifieke privacyinbreuk toegesneden normering. Aangezien die privacyinbreuk potentieel groot is – vanwege de grote hoeveelheid beschikbare data, ook afkomstig van anderen, zowel in de toekomst als in het verleden – moet die normering uit meer bestaan dan toestemming ex artikel 23 en het algemene afwegingskader van artikelen 43-44. Zeker wanneer het monitoren over een langere periode plaatsvindt, of wanneer met geautomatiseerde hulpmiddelen Internet-breed iemand in kaart wordt gebracht, of wanneer met nepprofielen de (semi-)besloten delen van sociale media worden gemonitord, zijn zwaardere eisen nodig aan het toestemmingsniveau, de duur van uitoefening en (bij langere duur) toezicht tijdens de uitoefening.

### *7.1.6 Artikel 27: onderzoek van plaatsen (inclusief woningen) en voorwerpen*

Hiervoor geldt hetzelfde als hierboven reeds bij artikel 25 onder observatie binnen woningen is gesteld. Hoewel het doorzoeken van woningen normaal gesproken fysiek gebeurt, waarbij er dus sprake is van binnentreden, sluit de tekst van de wet, evenmin als de toelichting, niet uit dat het doorzoeken plaatsvindt met behulp van een technisch hulpmiddel zonder dat daarbij binnengetreden wordt. De toelichting zou duidelijk moeten maken hetzij dat het van buitenaf doorzoeken van een woning geen vorm is van doorzoeking als bedoeld in artikel 27 maar een vorm van observatie die valt onder artikel 25, hetzij dat het van buitenaf doorzoeken van een woning met een technisch hulpmiddel ook onder artikel 27 lid 3 valt en dus toestemming van de Minister behoeft.

### *7.1.7 Artikel 42: toegang tot plaatsen*

Op basis van artikel 42 hebben de diensten te bevoegdheid elke plaats te betreden om, onder andere, observatie- of afluisterapparatuur te plaatsen (of te vervangen of verwijderen). Dit is een steunbevoegdheid, waarbij de privacyinbreuk naar wij aannemen over het algemeen zal worden afgedekt door de privacywaarborgen bij de (regeling en uitoefening van de) doelbevoegdheid. Het betreden van plaatsen,

[84] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26-27.

met name de woning, levert echter ook een zelfstandige privacyinbreuk op. Het is onduidelijk of deze voldoende wordt afgedekt in de huidige regeling.

De Memorie van Toelichting geeft aan dat bij het binnentreden in woningen op basis van art. 42 een machtiging conform de Algemene wet op het binnentreden (Awbi) nodig is, die wordt afgegeven door de Minister of door het hoofd van de dienst (p. 39). Dit volgt ook uit artikel 42 lid 4 j$^{o}$ artikel 2 Awbi. Deze bevoegdheid kan niet worden gemandateerd aan ondergeschikte ambtenaren (MvT, p. 92). Enige verwarring is mogelijk door artikel 42 lid 2, dat stelt dat voor het betreden van plaatsen geen toestemming (als bedoeld in artikel 24, dus toestemming van Minister, diensthoofd of aangewezen ambtenaren) nodig is, terwijl voor het betreden van woningen wel toestemming nodig is. Kennelijk prevaleert in het laatste geval de Awbi jo artikel 42 lid 4 Wiv 20xx boven artikel 42 lid 2, en niet andersom, maar dat is uit de wettekst zelf niet duidelijk. Voor de privacybescherming zou het duidelijker zijn als artikel 42 lid 2 bepaalt dat voor het betreden van een woning ter uitoefening de bevoegdheid van lid 1 wel toestemming als bedoeld in artikel 24 nodig is, en dat lid 4 bepaalt dat deze toestemming niet kan worden gemandateerd.

Voorts is het de vraag waarom de machtiging voor het betreden van woningen ter uitoefening van artikel 42 niet voorbehouden is aan de Minister, maar ook door het diensthoofd kan worden gegeven. Voor het uitoefenen van doelbevoegdheden binnen woningen, zoals observatie of afluisteren, kan alleen de Minister toestemming geven. De MvT legt niet uit waarom dit anders is voor de steunbevoegdheid van het betreden van plaatsen. Het betreden van een woning zonder toestemming van de bewoner is als zodanig een ingrijpende inbreuk op de privacy, los van het feit of en hoe er vervolgens informatie wordt verkregen. Bovendien is het twijfelachtig of medewerkers die apparatuur plaatsen of verwijderen binnen een woning, zich volstrekt kunnen beperken tot dat plaatsen of verwijderen zelf, en verder hun ogen, oren en neuzen geheel dicht houden tijdens hun oponthoud in de woning. Op zijn minst zou het verschil in behandeling van het huisrecht gemotiveerd moeten worden in de toelichting, maar het ligt meer voor de hand om de toestemming bij artikel 42 evenals bij de doelbevoegdheden op ministerieel niveau te regelen waar het woningen betreft.

## 7.2 Binnendringen in computers

### *7.2.1 Inleiding*

**Paragraaf 3.2.2.6 Verkennen van en binnendringen in geautomatiseerde werken**

Artikel 30

1. De diensten zijn bevoegd tot:
   a. het verkennen van de technische kenmerken van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten;
   b. het al dan niet met gebruikmaking van een technische ingreep, valse signalen, valse sleutels, valse hoedanigheid of door tussenkomst van het geautomatiseerd werk van een derde, binnendringen in een geautomatiseerd werk.
2. Tot de bevoegdheid in het eerste lid, onder b, behoort tevens de bevoegdheid tot:
   a. het doorbreken van enige beveiliging;

b. het aanbrengen van technische voorzieningen teneinde versleuteling van gegevens opgeslagen of verwerkt in het geautomatiseerde werk ongedaan te maken;
c. het aanbrengen van technische voorzieningen in verband met de toepassing van de bevoegdheid als bedoeld in de artikelen 25, eerste lid, en 32, eerste lid;
d. het overnemen van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk.

3. De in het eerste lid bedoelde bevoegdheid mag slechts worden uitgeoefend, indien door Onze betrokken Minister daarvoor op een daartoe strekkend verzoek schriftelijk toestemming is verleend aan het hoofd van de dienst.
4. Het verzoek om toestemming, bedoeld in het derde lid, wordt gedaan door het hoofd van de dienst en bevat in aanvulling op hetgeen is bepaald in artikel 24, zesde lid, voor zover van toepassing, welke bevoegdheden als bedoeld in het tweede lid, bij de uitoefening van de in het eerste lid, onder b, bedoelde bevoegdheid worden toegepast.

(…)

---

Artikel 30 (binnendringen in computers[85]) is gewijzigd ten opzichte van het huidige artikel 24 Wiv 2002. In aanvulling op de bestaande bevoegdheid tot het binnendringen in geautomatiseerde werken, wordt aan de diensten de bevoegdheid toegekend tot *het verkennen van de technische kenmerken* van geautomatiseerde werken die op een communicatienetwerk zijn aangesloten (artikel 30, eerste lid, onder a). Deze bijzondere bevoegdheid heeft ten opzichte van de bevoegdheid tot het binnendringen in een geautomatiseerd werk (artikel 30, eerste lid, onder b) een ondersteunend karakter. (MvT, p. 52)

Als toevoeging ten opzichte van de huidige wet (2002) wordt in artikel 30 lid 1 onder b geregeld dat het binnendringen in een geautomatiseerd werk ook kan plaatsvinden met gebruikmaking van het geautomatiseerd werk van een derde. Het wordt in bepaalde situaties in het belang van de bescherming van de nationale veiligheid noodzakelijk geacht de diensten ook in staat te stellen om via geautomatiseerde werken van zogenoemde *non-targets* binnen te dringen in geautomatiseerde werken die bij doelwitten in gebruik zijn.

Ook lid 2 sub c is nieuw; het bepaalt dat tot het binnendringen van een geautomatiseerd werk tevens de bevoegdheid behoort tot het aanbrengen van technische voorzieningen in verband met toepassing (volgens MvT ‘ter ondersteuning’) van de bevoegdheid als bedoeld in de artikelen 25, eerste lid en 32, eerste lid (resp. observeren en aftappen technisch hulpmiddel).

In lid 3 is opgenomen dat de bevoegdheid uit artikel 30 lid 1 alleen mag worden uitgeoefend indien door de voor de desbetreffende dienst verantwoordelijke minister daarvoor op een daartoe strekkend verzoek schriftelijk toestemming is verleend aan het hoofd van de dienst. In het huidige artikel 24 Wiv 2002 wordt deze

[85] Wij hanteren in dit rapport de term computers, dan weet de lezer tenminste wat er bedoeld wordt. Het gebruik van de term ‘geautomatiseerd werk’ in het wetsontwerp is begrijpelijk, omdat aangesloten wordt bij de term uit het strafrecht en daarmee de interne consistentie van de Nederlandse wet wordt vergroot. Voor de kenbaarheid van de wet is het echter een ongelukkige, en inmiddels ook verouderd aandoende, term. De wetgever kan overwegen om de term ‘geautomatiseerd werk’ te vervangen door de term ‘computersysteem’, die in de Nederlandse vertaling van het Cybercrime-Verdrag wordt gehanteerd (*Trb.* 2004, 290).

toestemming nog verleend in overeenstemming met de minister dan wel, voor zover van toepassing, het hoofd van de AIVD. Het verzoek om toestemming dient te worden gedaan door het hoofd van de dienst (Wiv 20xx) en dient te voldoen aan de eisen van artikel 24 lid 6 van het wetsvoorstel.

### *7.2.2 Algemene beschouwing I: binnendringen in computers als zwaarste privacyinbreuk*

De bevoegdheid tot het binnendringen in computers en het vervolgens overnemen van gegevens daaruit bestaat al in de Wiv 2002. Nog afgezien van de voorgestelde uitbreidingen van de bevoegdheid (zie hieronder), is het belangrijk om te benadrukken dat de mogelijkheid tot het binnendringen in computers een steeds ingrijpender inbreuk op de privacy is geworden, en in de komende decennia ook zal worden, door socio-technische ontwikkelingen. Hoewel de computer bij de totstandkoming van de Wiv 2002 ook al een belangrijk onderdeel was van het persoonlijk leven van veel burgers, en een essentieel onderdeel van bedrijven en overheden, is het belang van de computer enorm toegenomen, vooral ook in het dagelijkse en privéleven van burgers. Waar foto's, muziek, boeken en administratie in 2002 nog grotendeels op fysieke dragers (papier, cd's) werden bewaard, staan deze nu veelal op computers of in de cloud. Mobiele telefoons waren in 2002 nog geen computers, maar de huidige smartphones—voor bijna iedereen tegenwoordig een onmisbaar onderdeel van het privéleven—zijn evenzeer computers als de pc, laptop en tablet dat zijn. Computers en smartphones bevatten anno 2015 aanzienlijk meer gegevens, zowel in kwantiteit (hoeveelheid) als in kwaliteit (nieuwe soorten informatie). De bevoegdheid tot het binnendringen in computers is daarom nog veel ingrijpender geworden dan deze in 2002 al was.

Dit blijkt ook uit het feit dat constitutionele hoven in het buitenland inmiddels grondwettelijke bescherming toekennen aan computers als de nieuwe 'plaats' waar een groot deel van het persoonlijke leven zich afspeelt. Duitsland kent een grondrecht op integriteit en vertrouwelijkheid van computers, dat ontwikkeld is juist in de context van het op afstand heimelijk binnendringen van computers door de overheid.[86] De specifieke privacybedreigingen van het binnendringen in computers, gegeven alle daarin beschikbare informatie, worden onvoldoende afgedekt door de grondwettelijke bescherming van het huis en communicatie, maar vergen een zelfstandige bescherming van computers op grondwettelijk niveau.[87] Ook in de Verenigde Staten is erkend dat smartphones (en naar men aanneemt ook tablets en laptops) inmiddels zoveel informatie bevatten dat zij niet vergelijkbaar zijn met oude typen objecten die informatie bevatten; in de context van aanhouding door de politie betekent dit dat het inbeslagnemen en onderzoeken van de smartphone altijd specifieke rechterlijke machtiging vooraf vergt.[88] Het Supreme Court legt in niet mis te verstane bewoordingen de privacyrisico's van het doorzoeken van een smartphone door de overheid uit:

'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

[86] BVerfG 27 februari 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007, beschikbaar op http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, Engelse vertaling: http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html..
[87] Ibid., §§166-206.
[88] *Riley v California*, 134 S.Ct. 2473 (2014).

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".'[89]

Het feit dat zowel Duitsland als de VS – landen die regelmatig verschillende opvattingen hebben over de mate waarin de overheid inbreuk mag maken op privacy – grondwettelijke bescherming toekennen aan computers, zou voor de Nederlandse (grond)wetgever aanleiding moeten zijn om computers te beschermen op minstens het beschermingsniveau dat in de grondwet wordt toegekend aan het huisrecht en de vertrouwelijkheid van middellijke communicatie. In gevallen waarin de overheid toegang kan krijgen tot alle informatie op computers, moet het beschermingsniveau zelfs *hoger* liggen dan de bescherming van huis of communicatie, gezien het feit dat computeronderzoek veel meer van het privéleven kan blootleggen dan een huiszoeking of telefoontap. Het huidige voorstel voldoet daar niet aan (zie par. 7.2.4).

### *7.2.3 Algemene beschouwing II: de reikwijdte van het computerbegrip*

Apparaten die van oudsher mechanische hulpmiddelen of hooguit gegevensdragers waren, zoals horloges, auto's en koelkasten, worden in toenemende mate computers; voor het ene apparaat (de auto) gaat dat sneller dan voor het andere (de koelkast), maar in de komende decennia zullen met de komst van het Internet der Dingen ook veel apparaten onder de definitie van computer vallen, en vanuit hun functionaliteit ook de nodige gegevens bevatten die interessant kunnen zijn voor de diensten. Vaak zullen dat privacygevoelige gegevens (en niet zelden bijzondere persoonsgegevens) zijn, zoals de locaties waar een auto geweest is, lichaamswaarden die vastgelegd zijn door een sport-app, of het voedingspatroon dat uit de inhoud van een koelkast blijkt.

Nu het begrip 'computer' een grote hoeveelheid aan apparaten omvat, gezien de ruime definitie van het begrip 'geautomatiseerd werk' (art. 80sexies Sr), is het de vraag of de inbreuk van het binnendringen in computers voldoende voorzienbaar bij wet is. Voor de burger zal het niet op voorhand duidelijk zijn op basis van de voorgestelde wet dat met artikel 30 ook de mogelijkheid bestaat dat haar slimme telefoon of horloge kan worden gehackt, en zeker niet dat ook de boordcomputer van de auto en andere slimme apparaten kunnen worden geïnfecteerd en op afstand overgenomen door de diensten. Op zijn minst zou de toelichting uitgebreider moeten aangeven hoe de voorgestelde bevoegdheid zich verhoudt tot het Internet der Dingen. Daarnaast moet de wetgever zich afvragen of het überhaupt wel de bedoeling is dat de diensten moeten kunnen binnendringen in apparaten die technisch onder de definitie van geautomatiseerd werk vallen maar functioneel een andere rol vervullen dan het type computers (zoals de pc, laptop, tablet of smartphone) waarvoor deze bevoegdheid primair bedoeld is. De risico's van het hacken van apparaten in het Internet der Dingen, zoals slimme energiemeters, thermostaten en boordcomputers van auto's, zijn aanzienlijk, en het is sterk de vraag of het noodzakelijk is om dergelijke apparaten te kunnen hacken om gegevens te verzamelen, die niet op een minder ingrijpende manier zouden kunnen worden verkregen.

### *7.2.4 Toestemming en toezicht*

Lid 3 vereist toestemming van de minister aan het hoofd van de dienst. Hiermee wordt de toestemming vooraf nu 'over de volle breedte (…) naar ministerieel niveau

[89] Ibid.

getild' (MvT, p. 54). Dit codificeert wat door de Ministers van BZK en Defensie in reactie op rapport nr. 38 van de CTIVD was aangekondigd en thans ook de praktijk is. Daarmee is voor de 'hackbevoegdheid' over de volle breedte het toestemmingsniveau naar ministerieel niveau getild en aldus voorzien in een extra waarborg, aldus de MvT (p. 54). Dit volgt ook een aanbeveling van de commissie-Dessens, om het toestemmingsvereiste voor binnendringen in computers en het toezicht op deze bevoegdheid in lijn te brengen met de tweede fase van het interceptieraamwerk. Een andere – maar hiermee samenhangende – aanbeveling van de commissie-Dessens, namelijk om de CTIVD onmiddellijk toezicht te laten houden op de lastgevingen, is echter niet overgenomen.[90]

Nu, zoals boven aangegeven, de computer (pc, tablet, smartphone) een steeds centralere rol inneemt in het privéleven, als de toegangspoort tot de informatie en contacten waarmee mensen hun leven vormgeven, vormt het binnendringen in computers de zwaarst denkbare[91] inbreuk op de privacy. De bevoegdheid hiertoe moet dan ook met het zwaarst mogelijke toezicht worden omkleed. De voorgestelde waarborgen voldoen daar niet aan. Er zit een discrepantie in het feit dat, in afwijking van het algemene stelsel van ministeriële toestemming, (vanwege grondwettelijke kaders) een voorafgaande rechterlijke toestemming nodig is voor het onderscheppen en openen van brieven en voor het onderscheppen van communicatie met een advocaat, terwijl voor het overnemen van alle gegevens op een computer – waaruit een veel indringender beeld kan ontstaan van iemands persoonlijke leven dan uit welk briefverkeer dan ook – geen rechterlijke toestemming wordt vereist. Naast de vormgeving van de toestemming vooraf, is het met name bij de onderhavige bevoegdheid moeilijk te begrijpen dat het wetsvoorstel niet de aanbeveling overneemt om onmiddellijke toetsing in te voeren tijdens de uitoefening van de bevoegdheid, te meer omdat het mogelijk is de bevoegdheid gedurende een langere periode (telkens verlengd) uit te oefenen. De wetgever moet aldus wezenlijk zwaardere eisen stellen dan momenteel voorgesteld aan de bevoegdheid tot het binnendringen in computers.

### *7.2.5 Het binnendringen in computers van derden (niet-doelwitten)*

Volgens de MvT hebben de diensten ook de bevoegdheid nodig om de computers van derden (*non-targets*) binnen te dringen:

> 'De technische realiteit leert dat targets over het algemeen veiligheidsbewust zijn, maar dat zich operationele kansen tot het benutten van zwakheden kunnen voordoen bij technische randgebruikers, zoals medehuurders van een bepaalde server, welke kunnen leiden tot het succesvol binnendringen van het geautomatiseerde werk van het target. Het wordt in het belang van de bescherming van de nationale veiligheid noodzakelijk geacht de diensten ook in dergelijke situaties in staat te stellen om via geautomatiseerde werken van zogenoemde *non-targets* binnen te dringen in geautomatiseerde werken die bij targets in gebruik zijn.' (MvT, p. 53)

Volgens de MvT moet de bevoegdheid tot binnendringen in computers dus ook kunnen worden ingezet tegen niet-doelwitten (*non-targets*), omdat de computers van de doelwitten zelf soms te goed beveiligd zijn om direct in door te dringen. De zwakheden van 'technische randgebruikers, zoals medehuurders van een bepaalde

[90] Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013), p.106-107.
[91] Althans totdat het technisch mogelijk wordt om tot het brein van mensen door te dringen en hersensignalen uit te lezen en te interpreteren.

server' zouden benut kunnen worden om dan alsnog de computer van het doelwit te kunnen hacken. Daarmee worden opmerkelijk weinig woorden gewijd aan een van de meest vergaande voorstellen in de Wiv 20xx. Waar het binnendringen in computers al de zwaarst denkbare bevoegdheid is (zie boven), valt het binnendringen in computers van personen die zelf niet onderwerp zijn van onderzoek door de diensten in de buitencategorie van privacyinbreuken.

Privacyinbreuken moeten bij wet zijn voorzien, wat onder meer inhoudt dat de categorieën personen die onderworpen kunnen worden aan de inbreuk gedefinieerd moeten worden.[92] Voor de zwaarste vormen van privacyinbreuken zullen deze categorieën des te nauwer omschreven moeten worden, bij voorkeur in de wet zelf en niet in lagere regelgeving, zeker niet alleen in een toelichting, en des te meer niet in de vorm van één in de toelichting genoemd voorbeeld. Burgers (en zeker degenen met een lager 'veiligheidsbewustzijn' dan doelwitten van de diensten) zullen niet voorzien dat hun zwakker beveiligde computers gehackt kunnen worden door de diensten om aldus door te dringen tot de computers van mensen in hun omgeving – huisgenoten, familieleden, vrienden of (fysieke of server-)buren. De term 'derde' in artikel 30 lid 1 onder b biedt in dat licht nauwelijks inzicht in de categorie personen van wie de computer kan worden gehackt; het kan iedereen betreffen, maar slechts weinig burgers zullen beseffen dat onder de frase 'door tussenkomst van het geautomatiseerd werk van een derde' hun eigen computer valt; men zal er vermoedelijk eerder van uitgaan dat hiermee computers van Internetaanbieders worden bedoeld. (Dat is des te sterker het geval nu het hacken ook kan plaatsvinden ter ondersteuning van andere bevoegdheden, zie punt 3 hieronder.) Ook is de term 'derde' op geen enkele manier onderscheidend om een bepaalde categorie personen aan te duiden, zoals bedoeld in *Weber en Saravia*.

Het is daarom twijfelachtig of een regeling waarbij ook computers van een niet scherp omschreven categorie 'derden' kunnen worden gehackt, de toets van voorzienbaarheid bij wet kan doorstaan. Dat ligt mogelijk anders als de categorie 'technische randgebruikers' wel nauw omschreven kan worden; in dat geval zou de wet dit moeten expliciteren. Daarbij zou dan bovendien een subsidiariteitseis wenselijk zijn in de wet, waarbij bijvoorbeeld lid 4 zou moeten stipuleren dat het verzoek om toestemming dient te motiveren dat het in het specifieke geval dringend noodzakelijk is dat de bevoegdheid wordt uitgeoefend ten aanzien van het geautomatiseerd werk van iemand uit de nader omschreven categorie niet-doelwitten.

Afgezien van de voorzienbaarheid is het ook twijfelachtig of het hacken van computers van derden de toets van noodzakelijkheid kan doorstaan. Het enkele in de MvT gestelde feit dat 'targets over het algemeen veiligheidsbewust zijn' (p. 53), levert nog geen 'pressing social need' op om de computers van willekeurige (dan wel een nauw omschreven categorie onverdachte) burgers te kunnen hacken. Zonder enige empirische onderbouwing (via een al dan niet vertrouwelijk onderzoek naar de mate waarin het veiligheidsbewustzijn van doelwitten het de diensten feitelijk onmogelijk maakt om in hun computers binnen te dringen) is er geen motivering dat het hacken van computers van derden – zoals gezegd een privacyinbreuk van de buitencategorie – daadwerkelijk noodzakelijk is in een democratische samenleving. De noodzaak van dit onderdeel van het voorstel zal

[92] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §95.

dan ook sowieso veel beter onderbouwd moeten worden. Onzes inziens moet dit onderdeel van het voorstel echter intrinsiek worden afgewezen, omdat het moeilijk voorstelbaar is dat het (kennelijke) feit dat doelwitten van de diensten hun computers over het algemeen goed beveiligen het noodzakelijk maakt om dan maar computers van onverdachte burgers te kunnen hacken.

*7.2.6 Het verkennen van technische kenmerken van computers*

Onder het verkennen van technische kenmerken wordt verstaan het door de AIVD en MIVD inzetten van technische toepassingen, zoals IP- en poortscansoftware en registratiemiddelen, waarmee inzicht kan worden verkregen in de kenmerken van computers. Op grond van deze kenmerken zijn de diensten in staat te duiden of een computer relevantie voor de nationale veiligheid heeft. Om veranderingen tijdig te kunnen onderkennen en steeds over een actueel beeld van op basis van concrete onderzoeksopdrachten van de diensten relevante delen van het digitale landschap te kunnen beschikken, zouden de AIVD en MIVD de verkennende bevoegdheid semi-continu inzetten. (MvT, p.52).

Het gaat hier om een steunbevoegdheid, die veelal zal voorafgaan aan het binnendringen van de computer zelf. In die zin zal bij de uitoefening van de bestaande hackbevoegdheid ook het nodige verkend zijn aan de binnen te dringen computers, en betreft het hier mogelijk eerder een expliciete regeling van wat voorheen al impliciet onder de bevoegdheid werd begrepen, dan een zelfstandige uitbreiding van de bevoegdheid. Zoals de MvT opmerkt gaat het bij het verkennen om een lichtere privacyinbreuk, omdat alleen de ‘uiterlijke kenmerken’ van de computer in beeld worden gebracht, en niet de inhoud ervan – het zijn ‘vrijelijk te onderkennen gegevens over technische eigenschappen, zoals het IP-adres, de beschikbaarheid van poorten en de functie van het werk, zoals mailserver of router’ (p. 52). Als zodanig levert dit dan ook geen groot privacyrisico op. Dat wordt enigszins anders nu de toelichting aangeeft dat de diensten de bevoegdheid ‘semi-continu’ zullen inzetten (let wel: de toelichting spreekt van ‘zullen’, niet ‘kunnen’). Deze semi-continue monitoring stelt de diensten ‘aldus in staat in het belang van de nationale veiligheid gericht, efficiënt en zorgvuldig in relevante geautomatiseerde werken binnen te dringen’ (p. 53). Dit betekent dat de schaal waarop computers verkend gaan worden, vermoedelijk aanzienlijk groter is dan voorheen (als men aanneemt dat de Wiv 2002 geen bevoegdheid omvat om semi-permanent het hele Internet af te struinen op zoek naar ‘interessante’ computers om binnen te dringen). Ook zal het door het semi-continu monitoren van potentieel interessante computers een drempelverlagend effect kunnen hebben op het daadwerkelijk uitoefenen van de hackbevoegdheid – men heeft immers sneller en eenvoudiger in beeld waar en hoe binnengedrongen zou kunnen worden. Volgens ons levert de steunbevoegdheid van het verkennen van technische kenmerken van computers als zodanig geen aanvullende inbreuk op de privacy op, maar het semi-continu scannen op hackbare computers doet dat wel. Feitelijk komt een dergelijke vorm van monitoring neer op stelselmatige observatie en zou dit tenminste aan de vereisten van die bevoegdheid moeten voldoen, inclusief het verkrijgen van specifieke toestemming van de Minister voor observatie (art. 25 lid 2) waar het gaat om het semi-continu scannen van computers die zich (mogelijk ook) in woningen bevinden. Daarnaast zou het voor de voorzienbaarheid bij wet, en als waarborg tegen al te omvangrijke semi-continue monitoring, wenselijk zijn dat het verzoek om toestemming, als geregeld in lid 4, een specificatie bevat van de beoogde reikwijdte van het verkennen (als bedoeld in het eerste lid onder a) (vergelijkbaar met de eis dat het verzoek een specificatie bevat van de modaliteiten van het binnendringen

conform het eerste lid onder b). Ook zal bij het toezicht op de uitoefening van bevoegdheden gecontroleerd moeten worden op welke schaal de technische kenmerken van computers zijn of worden gemonitord.

*7.2.7 Binnendringen als steunbevoegdheid voor andere bevoegdheden*

Computers, zoals laptops en desktop computers, zijn tegenwoordig vrijwel allemaal uitgerust met camera's en microfoons. Deze kunnen door het aanbrengen van bepaalde software op afstand worden geactiveerd en zo ingezet worden als een technisch hulpmiddel bij de uitoefening van bijvoorbeeld de bevoegdheid tot observatie (artikel 25, eerste lid) of het opnemen van de conversatie in een bepaalde ruimte (artikel 32, eerste lid). Artikel 30 lid 2 onder c staat het binnendringen toe ter ondersteuning van een andere bevoegdheid. Toestemming is vereist voor zowel deze doelbevoegdheden als voor het inzetten van de steunbevoegdheid van artikel 30 lid 1 b; deze kan in bepaalde gevallen gelijktijdig worden aangevraagd (MvT, p. 54).

Dit onderdeel is nieuw ten opzichte van de Wiv 2002. De huidige regeling sluit een dergelijke inzet echter niet uit, zodat het hier eerder gaat om een explicitering dan een uitbreiding (zoals de MvT, p. 51-52, ook suggereert). Mede omdat er zowel voor de steunbevoegdheid (het hacken) als de doelbevoegdheid (observatie, aftappen) een zelfstandige toestemming nodig is, levert dit als zodanig geen aanvullende privacyrisico's op. Niettemin is het wel relevant te bekijken of er door de combinatie – en de mogelijkheid om gelijktijdige machtiging te verkrijgen – niet in sommige gevallen eenvoudiger inbreuk op de privacy kan worden gemaakt. Te denken valt vooral aan het observeren of afluisteren binnen een woning, waarvoor van oudsher de noodzaak bestaat dat daarvoor (meestal) ingebroken moet worden in de woning om een technisch hulpmiddel te plaatsen, wat niet alleen zelfstandige autorisatie behoeft, maar ook een zekere natuurlijke drempel oplevert – het inbreken in een woning is een afbreukrisico omdat het kan worden ontdekt door het doelwit. Het inbreken in computers kan op afstand en is vaak minder makkelijk te ontdekken (afhankelijk van de technische vaardigheid van het doelwit). Het risico dat door het wegvallen van deze natuurlijke drempel de bevoegdheid vaker zal worden ingezet, lijkt ons niet bijzonder groot, aangezien het aanbrengen van malware in een computer ook de nodige tijd, zorg en expertise vereist, en dus ook een zekere natuurlijke drempel kent.

Wat wel een aanvullend privacyrisico oplevert, is de combinatie van de steunbevoegdheid met het voorstel om ook computers van derden te kunnen hacken (zie par.7.2.5). Hacken als steunbevoegdheid zou bijvoorbeeld ingezet kunnen worden om de conversatie van een doelwit van de diensten (die zijn computer zelf te goed beveiligt) af te luisteren via de microfoon op een computer van een niet-doelwit-huisgenoot, bijvoorbeeld in een studentenhuis. Ook kan de computer van de moeder van een doelwit worden gehackt om de Skype-conversaties die zij heeft met haar zoon af te luisteren. Evenals bij het hacken van computers van derden om via die weg door te dringen tot de computer van het doelwit (zie par. 7.2.5), is dit iets wat burgers volstrekt niet zullen (en ook niet zouden moeten hoeven) verwachten. Dit versterkt de vragen die hierboven reeds opgeworpen zijn over de voorzienbaarheid bij wet en over de noodzakelijkheid in een democratische samenleving.

*7.2.8 Ontsleutelplicht*

Leden 5 t/m 8 bieden een meer uitgewerkte regeling van de ontsleutelplicht bij binnendringen in computers dan het huidige art. 24 lid 3 Wiv 2002, waarin enkel een medewerkingsplicht is vermeld.

---

Artikel 30

(…) 5. De diensten zijn bevoegd zich te wenden tot degene van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk als bedoeld in het eerste lid met het verzoek alle noodzakelijke medewerking te verlenen tot het ontsleutelen van de gegevens door hetzij deze kennis ter beschikking te stellen, hetzij de versleuteling ongedaan te maken.

6. De bevoegdheid, bedoeld in het vijfde lid, mag slechts worden uitgeoefend indien door Onze betrokken Minister op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst.
7. Het verzoek om toestemming, bedoeld in het zesde lid, is schriftelijk en bevat in aanvulling op hetgeen is bepaald in artikel 24, zesde lid:
   a. gegevens betreffende de identiteit van de persoon aan wie de medewerking wordt verzocht;
   b. een omschrijving van het geautomatiseerde werk waarin de desbetreffende gegevens worden verwerkt of opgeslagen ten aanzien waarvan de medewerking wordt verlangd.
8. De persoon aan wie een verzoek als bedoeld in het vijfde lid wordt gericht is verplicht daaraan te voldoen.

---

Het voorstel regelt nu dus ook expliciet wat in de huidige wet slechts impliciet wordt verondersteld, namelijk dat de diensten om een dergelijke medewerking tot ontsleuteling kunnen verzoeken; dat is een nuttige verduidelijking. De medewerking blijft verplicht en niet meewerken blijft strafbaar, in artikel 132, met dezelfde straffen als het huidige art. 89 Wiv 2002. Nieuw is dat voor het verzoeken om ontsleuteling zelfstandige toestemming van de minister vereist is. Het feit dat de regeling aldus meer procedureel wordt ingekleed en meer waarborgen kent, verkleint het privacyrisico, en levert dus winst op voor de privacy.

Wel moet worden aangetekend dat de term ‘verzoek’ in deze bepaling een voorbeeld is van verhullend taalgebruik, aangezien de aangesprokene verplicht is om mee te werken, op straffe van maximaal twee jaar gevangenisstraf; het gaat dus om een bevel, en het zou duidelijker zijn als de wet dan ook die term zou hanteren.

Verder is het belangrijk om te benadrukken dat de vormgeving van de ontsleutelplicht, in de huidige wet en eveneens in het wetsontwerp, nog steeds een potentieel aanzienlijk privacyrisico oplevert. Het weigeren van medewerking wordt gesanctioneerd met een strafdreiging van maximaal twee jaar gevangenisstraf voor het opzettelijk weigeren, maar daarnaast ook met maximaal zes maanden gevangenisstraf voor niet-opzettelijk weigeren. Dat laatste is geen misdrijf maar een overtreding, wat betekent dat er geen sprake hoeft te zijn van verwijtbare schuld: bij overtredingen geldt in hoofdzaak de leer van het blote feit, de ‘pure gedraging’.[93] Feitelijk betekent dat een aanzienlijke risicoaansprakelijkheid voor vergeetachtigen (en wie van ons heeft nog nooit een wachtwoord vergeten?). Hoewel de regeling en

[93] Hazewinkel-Suringa-Remmelink 1994, p. 103. Degene die het blote feit pleegt kan eventueel wel een beroep doen op het leerstuk van afwezigheid van alle schuld.

strafdreiging onbekend zijn bij de gemiddelde (en naar wij aannemen ook ongemiddelde) burger, levert het in theorie wel een potentieel verkillend effect op voor het gebruik van versleuteling door burgers. In een tijdperk waarin het voor burgers steeds belangrijker wordt de bestanden op de computer te beveiligen (tegen phishers, hackers, identiteitsdieven, en buitenlandse veiligheidsdiensten), is het onwenselijk dat het niet-opzettelijk niet geven van een wachtwoord aan de diensten een strafbedreiging kent. Burgers die deze wet zouden kennen (en dat worden zij geacht te doen), zouden voor de zekerheid maar kunnen afzien om hun bestanden te beveiligen, dan wel hun wachtwoorden overal gaan noteren; dit levert vooral een veiligheidsrisico op, maar daarmee ook een privacyrisico.

Hoewel dit theoretisch is, moet wel onder ogen worden gezien wat de wettelijke regeling feitelijk behelst in haar combinatie van voorstellen. De diensten mogen in beginsel inbreken op de computer van de moeder van een doelwit om de gesprekken met hem te kunnen afluisteren (zie punt 1 en 3 hierboven); daarbij mogen zij ook gegevens uit de computer van de moeder overnemen (art. 30 lid 2 onder d) – bijvoorbeeld bestanden die de zoon daarop zet als hij zijn moeder bezoekt – en als deze versleuteld zijn, kunnen zij de moeder ‘verzoeken’ om het wachtwoord ter beschikking te stellen (art. 30 lid 5). Wanneer de moeder het wachtwoord vergeten heeft, of simpelweg niet heeft omdat het bestanden van de zoon betreft, kan zij voor zes maanden de gevangenis ingaan wegens het niet-opzettelijk niet-meewerken (art. 30 lid 8 j$^{o}$ art. 132 lid 1 j$^{o}$ lid 2 j$^{o}$ lid 3 onder b). Dit zal (hopelijk) een puur hypothetisch geval zijn, maar de wet sluit het niet uit, en dat geeft aan hoe ingrijpend de combinatie van verschillende voorstellen in beginsel kan uitwerken voor de privacy van elke burger, ook degenen die niet zelf voorwerp zijn van onderzoek door de diensten.

### *7.2.9 Onderzoekplicht en bewaartermijn*

Artikel 30

(…) 9. Gegevens verkregen door uitoefening van een bevoegdheid als bedoeld in het tweede lid, onder d, in verband met de uitoefening van de bevoegdheid, bedoeld in het eerste lid, onder b, worden zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven onderzocht. Gegevens, waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste twaalf maanden vernietigd.

Dit lid bepaalt dat gegevens die gekopieerd zijn uit gehackte computers zo spoedig mogelijk worden onderzocht op relevantie, waarbij niet-relevante gegevens, evenals nog niet op relevantie onderzochte gegevens, na maximaal 12 maanden moeten worden vernietigd. Dat is (voor de diensten) een relatief korte termijn, zodat dit een belangrijke waarborg biedt tegen misbruik of datalekken. Tegelijkertijd kan men zich afvragen hoe het mogelijk zou kunnen zijn dat gegevens na 12 maanden nog niet op relevantie onderzocht zijn, als de wet eist dat zij ‘zo spoedig mogelijk’ worden onderzocht op relevantie; als de wetgever daadwerkelijk rekening houdt met de mogelijkheid dat gegevens nog niet binnen 12 maanden onderzocht zijn, is de term ‘zo spoedig mogelijk’ in art. 30 lid 9 misleidend en zou een term als ‘zodra de diensten daaraan toekomen’ passender zijn. Het zou in elk geval nuttig zijn als in de toelichting een nadere precisering wordt gegeven wat precies onder ‘zo spoedig mogelijk’ wordt verstaan, en daarbij expliciet een uiterlijke termijn te geven

waarbinnen de gegevens onderzocht moeten zijn (hetgeen nu impliciet op 12 maanden wordt gesteld, een termijn die niet met de normale betekenis van de term ‘zo spoedig mogelijk’ te verenigen valt).

Ook valt niet in te zien waarom gegevens waarvan eenmaal is vastgesteld dat zij niet relevant zijn, überhaupt nog moeten worden bewaard. De MvT geeft hiervoor geen reden. Persoonsgegevenswetgeving vereist normaliter dat gegevens worden vernietigd zodra zij niet (meer) relevant zijn, tenzij bepaald is dat zij nog voor een ander doel (met een zelfstandige grondslag daarvoor) mogen worden bewaard. Indien beoogd is dat vergaarde gegevens, nadat is vastgesteld dat zij niet relevant zijn voor het doel van het onderzoek maar nog voordat zij zijn vernietigd conform lid 9, ook voor andere onderzoeken zouden mogen worden gebruikt, dan zou dat niet alleen in de toelichting maar ook in de wet zelf expliciet moeten worden geregeld. Aannemend dat dit niet beoogd is, zou moeten worden bepaald dat gegevens worden vernietigd zodra blijkt dat zij niet relevant zijn voor het onderzoek (zie ook par. 4.6.4).

# 8 Relationele privacy: bescherming van communicatie

De jurisprudentie van het EHRM ziet ten aanzien van bescherming van communicatie op communicatie per brief, telefoon[94] en e-mail, zowel thuis[95] als op het werk.[96] In Nederland geldt het brief-, telefoon- en telegraafgeheim (art. 13 Gw), dat momenteel aan herziening onderhevig is. Het herzieningsvoorstel stelt voor alle inhoud van middellijke communicatie, ongeacht met welk communicatiemiddel (post of enige vorm van telecommunicatie) deze wordt overgebracht, aan dezelfde eisen te onderwerpen. Het artikel ziet momenteel alleen op middellijke communicatie waarbij een derde belast is met het transport; in het voorgestelde gewijzigde artikel 13 zou dat ook kunnen gaan gelden voor derden belast met de opslag.

Artikel 13 van de Grondwet biedt (slechts) bescherming aan de inhoud van de communicatie. Verkeersgegevens ofwel metadata, die geen informatie geven over de inhoud maar slechts over de overdracht en de opslag van de communicatie, vallen momenteel buiten het bereik van artikel 13, en deze benadering van verkeersgegevens blijft gehandhaafd in het huidige wetsvoorstel. Deze gegevens worden wel beschermd door artikel 10 van de Grondwet en artikel 8 EVRM. Ook onmiddellijke communicatie (zoals het live gesprek) wordt niet door artikel 13, maar door artikel 10 Gw beschermd.

Bij een inbreuk op het recht op bescherming van de persoonlijke levenssfeer wegens het onderscheppen van communicatie wordt door het EHRM sterk gehecht aan het vereiste van voorzienbaarheid bij wet, waarbij expliciet ook eisen worden gesteld aan de kwaliteit van de wet in de vorm van waarborgen. Het betreft immers het inzetten van bevoegdheden waarbij heimelijk inbreuken worden gepleegd op een grondrecht. De inzet van bevoegdheden hoeft daarbij niet voorzienbaar te zijn in elk individueel geval, maar de wetgeving moet wel voldoende voor burgers inzichtelijk maken wat de consequenties van hun gedragingen kunnen zijn.[97] Met betrekking tot de toegankelijkheid betekent dit dat een burger een goede indicatie moet kunnen hebben van de regels die in concrete omstandigheden van toepassing zullen zijn op een bepaald geval. De wettelijke regels moeten daarom publiekelijk kenbaar zijn.[98] Overigens is het toegestaan om nadere regels omtrent de inzet van bevoegdheden, waarborgen tegen misbruik en een onafhankelijke klachtenprocedure in lagere wetgeving of in openbaar gemaakte instructies vast te leggen.[99]

Het EHRM heeft meermaals benadrukt dat ‘the existence of some legislation granting powers of secret surveillance […] is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the

[94] EHRM 6 september 1978, Klass t. Duitsland, §41.
[95] EHRM 24 april 1990, Kruslin t. Frankrijk, EHRM 24 april 1990, Huvig t. Frankrijk.
[96] EHRM 25 juni 1997, Halford t. Verenigd Koninkrijk; EHRM 3 juli 2007, Copland t. Verenigd Koninkrijk.
[97] ‘[T]he domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures’. EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §93.
[98] EHRM 26 april 1979, Sunday Times t. Verenigd Koninkrijk; EHRM 25 maart 1983, Silver en anderen t. Verenigd Koninkrijk, §87.
[99] EHRM 1 juli 2008, Liberty en anderen t. Verenigd Koninkrijk, §63.

prevention of disorder or crime'[100]. Dit betekent volgens het Hof echter niet een onbegrensde discretionaire bevoegdheid om mensen aan geheime surveillance te onderwerpen.[101] In Europese rechtspraak zijn randvoorwaarden vastgelegd om willekeur of misbruik van bevoegdheden te voorkomen en is ingegaan op de minimum waarborgen voor het onderscheppen van communicatie. De volgende aspecten moeten in formele wetgeving vastgelegd zijn:

'a. de aard van de gedragingen die tot een interceptiebevel kunnen leiden;
b. de categorieën van personen van wie communicatie kan worden onderschept;
c. een beperking van de duur van de interceptie;
d. de procedure die gevolgd moet worden voor het onderzoeken, gebruiken en opslaan van de verkregen gegevens;
e. de voorzorgsmaatregelen die moeten worden getroffen als de gegevens met derden worden gedeeld;
f. de omstandigheden waaronder gegevens moeten worden gewist of opnamen vernietigd.'[102]

Voor het onderscheppen van communicatie is door het EHRM bepaald dat voor meer algemene opsporingsactiviteiten, zoals bulkinterceptie, dezelfde vereisten gelden als voor gerichte interceptie.[103]

Het EHRM kijkt bij de mate van uitwerking van de wettelijke waarborgen ook naar de aard van de gegevens die verzameld worden. In *Uzun* werd bijvoorbeeld gekeken naar GPS-surveillance en werd meegewogen dat het verzamelen van locatiegegevens een beperktere inbreuk oplevert dan het onderscheppen van de inhoud van communicatie.[104] Ook wordt van oudsher gesteld dat het verzamelen van verkeersgegevens (wie met wie belt) een kleinere privacyinbreuk oplevert dan het onderscheppen van de inhoud van communicatie. Hierbij moet wel worden aangetekend dat steeds vaker de vraag wordt opgeworpen of dergelijke onderscheiden – die veelal gebaseerd zijn op het eind-20$^{e}$-eeuwse communicatielandschap[105] – nog wel valide zijn in het huidige tijdperk.[106] In dit hoofdstuk baseren we ons dan ook niet alleen op het bestaande juridische kader, zoals met name uitgewerkt door het EHRM, maar ook op huidige inzichten over de privacygevoeligheid van onderzoek van communicatie in het huidige telecommunicatielandschap.

In dit hoofdstuk gaan we niet in op het onderscheppen van brieven en post (art. 29 Wiv 20xx, dat grotendeels ongewijzigd is ten opzichte van art. 23 Wiv 2002), maar beperken we ons tot de bevoegdheden tot onderzoek van telecommunicatie. Dit omvat medewerkingsplichten voor communicatieaanbieders, gerichte interceptie en de bulkinterceptie.

[100] EHRM 6 september 1978, Klass t. Duitsland, §48.
[101] EHRM 6 september 1978, Klass t. Duitsland, §49.
[102] EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §95 (onze vertaling).
[103] EHRM 1 juli 2008, Liberty en anderen t. Verenigd Koninkrijk, §69.
[104] EHRM 2 september 2010, Uzun t. Duitsland.
[105] Weber en Saravia betrof bijvoorbeeld een zaak die in 1995 door klagers aanhangig was gemaakt bij het Duitse Constitutioneel Hof; ook Uzun betrof surveillance-activiteiten rond 1995.
[106] Zie over het onderscheid verkeersgegevens-inhoud bijvoorbeeld Koops & Smits 2014.

## 8.1 Medewerkingsplichten communicatieaanbieders

Er worden nieuwe eisen gesteld aan de informatie- en medewerkingsplicht van aanbieders van communicatiediensten. Naast een definitie van het begrip communicatieaanbieder betreft het deels nieuwe medewerkingsplichten, bij bulkinterceptie (artikel 36, 37 en 38); deels betreft het een wijziging van bestaande informatie- en medewerkingsplichten rond verkeersgegevens en abonneegegevens (artikel 39 en 40); en deels betreft het een nieuwe plicht tot medewerking bij ontsleuteling van berichten (artikel 41).

### *8.1.1 Definitie en reikwijdte van de medewerkingsplichten*

Allereerst is van belang dat de reikwijdte van de artikelen is uitgebreid ten opzichte van de Wiv 2002 van 'aanbieders van openbare telecommunicatienetwerken en -diensten (in de zin van de Telecommunicatiewet)' naar 'aanbieders van communicatiediensten'. Omdat niet meer wordt aangesloten bij de definitie uit de Telecommunicatiewet, wordt een zelfstandige definitie gegeven:

---

Artikel 31

In deze paragraaf en de daarop berustende bepalingen wordt verstaan onder:

a. aanbieder van een communicatiedienst: de natuurlijke of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst;
b. gebruiker: de natuurlijke persoon of rechtspersoon die met de aanbieder van een communicatiedienst een overeenkomst is aangegaan met betrekking tot het gebruik van die dienst of die feitelijk gebruik maakt van een zodanige dienst.

---

Deze definitie is dezelfde als die gehanteerd wordt in art. 126la Sv, gebaseerd op het Cybercrime-verdrag. Nu de reikwijdte wordt uitgebreid ten opzichte van de aanbieders die onder de Telecommunicatiewet vallen, is het enigszins verwarrend dat de wettekst verder nog wel de term 'telecommunicatie' blijft gebruiken. Dit dient vermoedelijk ter onderscheiding van het bredere begrip 'communicatie', dat zowel communicatie van persoon tot persoon (het zogenoemde 'live-gesprek') omvat als communicatie op afstand ('tele'-communicatie). De MvT geeft echter niet aan of voor de interpretatie van het begrip 'telecommunicatie' nog wel aangesloten moet worden bij de Telecommunicatiewet (die in hoofdstuk 13 de term 'telecommunicatie' gebruikt, maar daarbij beperkt is tot openbare telecomnetwerk en -diensten), dan wel bij de Grondwet (wat lastig is omdat het wetsvoorstel voor aanpassing van art. 13 nog niet is aangenomen en het daarmee niet zeker is welke invulling het begrip telecommunicatie in art. 13 krijgt), of dat dit begrip een zelfstandige invulling krijgt in de Wiv. Veel communicatieaanbieders bieden een scala aan diensten aan, en voor de rechtszekerheid is het belangrijk dat de MvT duidelijk maakt welke diensten uit hun aanbod onder het begrip 'telecommunicatie' vallen.

Met de definitie worden twee uitbreidingen beoogd ten opzichte van de huidige reikwijdte:

- ook aanbieders van hosting- en opslagdiensten vallen eronder; de MvT noemt in dat verband 'diensten als webhosting, opslag in de cloud en dergelijke' en 'webhostingdiensten en beheerders van websites' (MvT, p. 56-57); dit omvat

dus ook diensten van de informatiemaatschappij, die traditioneel buiten het wettelijke telecommunicatieregime vallen;
- ook besloten netwerken vallen eronder, waar het voorheen alleen openbare telecommunicatiediensten betrof (MvT, p. 57).

Het gaat hier om zeer ingrijpende uitbreidingen, niet alleen in de reikwijdte van de communicatie (en opgeslagen gegevens) die hiermee onderschept kunnen worden, maar ook in de verplichtingen die aan private partijen worden opgelegd om mee te werken met de diensten. De Memorie van Toelichting is echter tamelijk laconiek in het motiveren van deze uitbreidingen. Sommige diensten 'in de sfeer van elektronische communicatie' vallen mogelijk of duidelijk niet onder de reikwijdte van de Telecommunicatiewet, maar 'waarvan het wel noodzakelijk wordt geacht dat de gegevens die in dat kader worden verwerkt voor een goede taakuitvoering van de diensten beschikbaar moeten kunnen komen (…). Indien dergelijke diensten niet als een openbare telecommunicatiedienst kunnen worden aangemerkt, betekent dat de in dat kader verwerkte gegevens door de diensten uitsluitend op basis van vrijwillige medewerking kunnen worden verkregen.' (MvT, p. 56) Er wordt echter niet nader gemotiveerd *waarom* het noodzakelijk wordt geacht deze diensten te kunnen aftappen, noch *waarom* het problematisch is als dat alleen met vrijwillige medewerking van aanbieders zou kunnen. De toelichting (p. 57) noemt slechts dat deze voorstellen ook in het post-Madrid-voorstel waren opgenomen en legt verder alleen uit wat ermee wordt bedoeld. Hier wordt het post-Madrid-voorstel als retorische truc gehanteerd om te suggereren dat het (kennelijk) niet nodig is om de noodzaak van deze uitbreiding nog nader te motiveren (zie par. 2.3.2). In plaats van te verwijzen naar het post-Madrid-voorstel, zou de toelichting inhoudelijke argumenten moeten geven die de noodzaak van uitbreiding onderbouwen. Die argumenten zullen sterk moeten zijn, omdat het om ingrijpende uitbreidingen gaat.

**Opslagdiensten**

De uitbreiding tot aanbieders van opslagdiensten is enerzijds begrijpelijk, omdat deze diensten vaak nauw verweven zijn met communicatiediensten zoals webmail. Anderzijds ligt de uitbreiding echter minder voor de hand, omdat het bij opslagdiensten niet als zodanig om communicatie gaat. Niet voor niets maakt het Europese wetgevingskader juist een onderscheid tussen elektronische communicatiediensten (waarop de Tw ziet) en diensten van de informatiemaatschappij, waaronder webhosting en sociale media (waarop de Tw niet ziet).

De aansluiting bij de definitie in Sv is in dat opzicht ook enigszins problematisch, omdat die definitie niet expliciet het type diensten omvat dat het wetsontwerp in brede zin suggereert. Onder art. 126la Sv wordt wel als voorbeeld genoemd 'web-hosts',[107] maar niet cloud-opslagdiensten (die destijds als zodanig nog nauwelijks bestonden). Het is in het strafrecht nog geen uitgemaakte zaak dat cloud-opslag als zodanig onder de definitie van art. 126la valt. Onzes inziens is dat niet het geval, omdat het gedeelte van de definitie dat op opslagaanbieders betrekking zou hebben – 'die gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst' – de opslagfunctionaliteit ('verwerkt of opslaat') koppelt aan de communicatiefunctionaliteit ('een *zodanige* dienst (…) of (…) *die* dienst', cursivering toegevoegd). Met andere woorden, de definitie slaat

[107] *Kamerstukken II* 2004/05, 26 671, nr. 7, p. 24.

grammaticaal alleen op opslagdiensten voor zover deze plaatsvinden in het kader van een dienst die gebruikers de mogelijkheid biedt te *communiceren*.

Waar webhostingaanbieders diensten aanbieden die veelal bestaan uit of samenhangen met openbare communicatie (het publiceren van inhoud op Internetpagina's), dan wel met besloten communicatie (bijvoorbeeld in de vorm van een chatfunctionaliteit), gaan cloud-opslagdiensten veel meer gepaard met opslag van documenten en bestanden. Sommige cloud-opslagdiensten, zoals Dropbox, hebben (mede) een communicatieve functie, omdat ze gericht zijn op het online uitwisselen van bestanden of het gezamenlijk werken aan documenten in de cloud. Dit type cloud-diensten kan worden gezien als een functioneel equivalent van communicatiediensten (het overbrengen van berichten tussen personen). Andere cloud-opslagdiensten zijn echter gericht op het opslaan van de eigen bestanden (als reservedocumenten of om er vanuit verschillende plaatsen toegang toe te kunnen hebben). Deze diensten zijn geen functioneel equivalent van communicatiediensten, maar een nieuw type dienst dat het functioneel equivalent is van het opslaan van gegevens in een besloten omgeving. Traditioneel wordt dergelijke opslag beschermd door het huisrecht: de opslag van foto's, boeken, muziek, dagboeken en administratie vond tot recent plaats binnen het huis. Met digitalisering worden deze typen gegevens steeds meer in computers opgeslagen; aanvankelijk betrof dat nog steeds grotendeels opslag binnen het huis, waar de pc of externe gegevensdrager zich bevond. Met de opkomst van de cloud worden deze bestanden nu steeds meer extern opgeslagen, met een cloud-opslagdienst. Dat betekent dat dit type cloud-dienst niet moet worden benaderd vanuit het perspectief van bescherming van communicatie (art. 13 Gw) maar van het huisrecht (art. 12 Gw).

Wanneer de klassieke interceptiebevoegdheden, die betrekking hebben op telefonie en email, uitgebreid worden naar 'interceptie' van bestanden die van oudsher door het huisrecht beschermd worden maar die nu door gebruikers van cloud-opslagdiensten op afstand worden bewaard, betekent dit een enorme oprekking van het begrip 'communicatie'. Opgeslagen bestanden zijn immers niet vergelijkbaar met brieven, telefoontjes of emailberichten en vallen niet onder wat men over het algemeen onder 'communicatie' zal verstaan, namelijk de uitwisseling van berichten tussen verschillende personen. Bij cloud-opslag is er geen sprake van communicatie tussen personen, maar van bestandsbeheer van één persoon. Het feit dat dergelijk bestandsbeheer inmiddels mede via de telecommunicatie-infrastructuur plaatsvindt, waardoor bestanden die iemand extern opslaat onderweg onderschept kunnen worden, betekent niet dat we bestanden die op afstand worden bewaard nu onder het begrip 'telecommunicatie' zouden moeten laten vallen waarop de interceptiebevoegdheid van oudsher zijn toegesneden.

Dit is vooral van belang omdat het een uiterst ingrijpende uitbreiding betreft waar het gaat om bulkinterceptie. Als de bulkinterceptiebevoegdheden ook toegepast kunnen worden op dit type cloud-opslagdiensten, doordat het gegevensverkeer tussen gebruikers en hun externe opslagplaats in bulk kan worden onderschept, betekent dit feitelijk een functioneel equivalent van het door de diensten in bulk gegevens die in Nederlandse woningen liggen opgeslagen verzamelen en vervolgens analyseren volgens het drietrapsmechanisme (zie onder, par. 8.3.2). Dat is een enorme privacyinbreuk die op geen enkele manier te rechtvaardigen valt. Weliswaar geven mensen die gegevens extern opslaan de controle hierover tot op zekere hoogte uit handen – waarmee de redelijke privacyverwachting iets lager is

dan wanneer de gegevens in het huis blijven – maar de technische ontwikkelingen bieden dusdanige voordelen om gegevens (ook) in de cloud op te slaan en niet (alleen) in het huis[108] dat men geen normatieve consequenties kan verbinden aan de keuze die mensen maken om gegevens in de cloud te zetten. Integendeel, juist het feit dat mensen gegevens die uiterst privacygevoelig zijn (foto's, boeken, documenten, administratie) door technische veranderingen meer buitenshuis opslaan dan binnenshuis, moet aanleiding zijn voor de wetgever om een hoog beschermingsniveau te bieden voor deze externe opslag. Het in bulk kunnen verzamelen van deze gegevens is daar duidelijk mee in strijd.

Los van de toepassing van bulkinterceptie op opslagdiensten, zou de interpretatie van de diensten in elk geval beperkt moeten blijven tot opslagdiensten die aangeboden worden in het kader van communicatiefunctionaliteiten en die daarmee onlosmakelijk zijn verbonden. Dat is ook wat de formulering van de definitie grammaticaal aangeeft. Dit betekent dat webhosting en cloudopslag alleen onder de definitie vallen voor zover onlosmakelijk samenhangen met een communicatiefunctionaliteit. Daaronder vallen dus niet de clouddiensten die mensen in staat stellen om hun eigen bestanden extern op te slaan, ook niet als deze dienst wordt aangeboden in een pakket gezamenlijk met een emaildienst (het gaat dan immers om twee verschillende diensten die niet onlosmakelijk zijn verbonden).

**Besloten netwerken**

De uitbreiding tot besloten netwerken is eveneens ingrijpend, omdat het de categorie aanbieders aanzienlijk uitbreidt. Ook bedrijfsnetwerken en sectorale netwerken (zoals SURFnet voor het hoger onderwijs) gaan nu onder de interceptiebevoegdheden vallen. Eenzelfde uitbreiding heeft in 2006 plaatsgevonden in de strafvordering (via art. 126la Sv), en het wekt in die zin geen bevreemding dat ook de diensten in staat willen zijn om communicatie te onderzoeken met medewerking van aanbieders van besloten netwerken.

Er is echter een fundamenteel verschil tussen de hier voorgestelde regeling en de regeling in de strafvordering. Op basis van het Wetboek van Strafvordering kan justitie wel besloten netwerken aftappen, maar niet aanbieders van besloten netwerken verplichten om mee te werken aan een tap; de aanbieder wordt in de gelegenheid gesteld om vrijwillig mee te werken (art. 126m lid 4 Sv), maar als deze dat niet wil, moet justitie zelf de tap technisch uitvoeren. Daarentegen worden in het wetsontwerp aanbieders van besloten netwerken wel verplicht om mee te werken aan gerichte interceptie (art. 32 lid 7 Wiv 20xx). Het gaat om een uitgebreidere bevoegdheid dan in de strafvordering is geregeld. Dat geldt ook voor de kostenverdeling, waarbij aanbieders, ook van besloten diensten, verplicht worden zelf de kosten van investering en onderhoud in technische voorzieningen te dragen (zie onder, par. 8.1.3).

Dat maakt de uitbreiding tot besloten netwerken ingrijpend: de medewerkingsplichten zijn veel verstrekkender dan de wetgeving tot nu toe. De noodzaak van de uitbreiding tot besloten netwerken is in dat licht duidelijk niet voldoende gemotiveerd om de grotere privacyinbreuk te rechtvaardigen.

[108] Bijvoorbeeld uit veiligheidsoogpunt: de beschikbaarheid is beter gewaarborgd als (kopieën van) gegevens in de cloud staan dan op een computer in het huis, waar het blootstaat aan risico's van kapotte computers of brand.

*8.1.2 Medewerking bij bulkinterceptie (artikelen 36-37)*

Artikelen 36 en 37 van het wetsontwerp regelen medewerkingsverplichtingen voor de aanbieders om bulkinterceptie (art. 33) te faciliteren. Artikel 36 betreft een verplichting om relevante 'voorinformatie' te leveren, artikel 37 betreft het meewerken aan de bulkinterceptie zelf.

---

Artikel 36

1. De diensten zijn bevoegd zich te wenden tot een aanbieder van een communicatiedienst met het verzoek gegevens te verstrekken, welke noodzakelijk zijn om toepassing te kunnen geven aan de bevoegdheid als bedoeld in artikel 33, eerste lid. Bij algemene maatregel van bestuur worden de categorieën van gegevens bepaald, waarop het in de eerste volzin bedoelde verzoek betrekking kan hebben.
2. Voor de uitoefening van de bevoegdheid, bedoeld in het eerste lid, is geen toestemming vereist als bedoeld in artikel 24.
   (…)
4. De aanbieder van een communicatiedienst is verplicht aan een verzoek als bedoeld in het eerste lid, eerste volzin, te voldoen. (…)

---

Om bulkinterceptie te kunnen uitvoeren, moeten de diensten eerst zicht hebben op het 'communicatielandschap', wat 'noodzakelijk is om op enig moment uitvoering te kunnen geven aan de interceptiebevoegdheid van artikel 33' (MvT, p. 79). Dat wordt als volgt toegelicht:

> 'Om doelgericht te kunnen intercepteren dient inzichtelijk te zijn waar, welke soort communicatie wordt verwerkt c.q. getransporteerd. Het betreft hier bijvoorbeeld informatie aangaande zakelijke klanten/(ver)huurders en regulier binnen de bedrijfsvoering van aanbieders van communicatiediensten bekende gegevens over de aangeboden diensten, karakteristieke [sic] van verkeersstromen en de belegging van communicatiekanalen.' (MvT, p. 79).

Door dergelijke informatie kunnen de diensten de bulkinterceptie 'doelgericht' inzetten, oftewel niet willekeurig maar met het oog op het verkrijgen van zo relevant mogelijke communicatie. Het maakt het ook mogelijk om het verzoek tot toestemming aan de minister zo nauwkeurig mogelijk te kunnen formuleren, inclusief het type medewerking dat (conform art. 37) van de aanbieder kan worden gevraagd (MvT, p. 80). Deze informatie kan door dienstmedewerkers zonder toestemming van bovenaf worden opgevraagd (art. 36 lid 2), omdat het niet gaat om informatie waarbij de privacy van concrete personen in het geding is, maar om technische en bedrijfsinformatie, aldus de MvT (p. 80). Het gaat, naar wij aannemen, in het algemeen inderdaad om informatie die weinig privacygevoelig zal zijn voor individuen. Bovendien kan de bevoegdheid bijdragen aan een gerichtere, en daarmee minder privacybedreigende, inzet van de bevoegdheid van artikel 33. Wel kan de kanttekening worden geplaatst dat de MvT (p. 80) twee maal verwijst naar de AMvB waarin de categorieën gegevens die op basis van art. 36 kunnen worden gevorderd limitatief worden opgesomd, en daarbij de suggestie wekt dat de reikwijdte hierdoor wordt beperkt, zonder echter enig inzicht te geven in de categorieën die in de AMvB zullen worden opgenomen. Dat laat de mogelijkheid open dat de AMvB zeer ruime categorieën definieert. Het is wenselijk dat de MvT

op dit punt meer richting geeft aan wat wel en niet in de AMvB mag worden opgenomen.

Relevant is wel ook nog te wijzen op het feit dat de aanbieders verplicht zijn om aan dergelijk verzoek te voldoen (lid 4). Zoals al eerder aangegeven is de term ‘verzoek’ hier een vorm van verhullend taalgebruik, omdat er een wettelijke plicht aan het opvolgen van het verzoek ten grondslag ligt, die strafrechtelijk wordt gesanctioneerd (art. 132).

Als de diensten voldoende informatie hebben en de minister heeft ingestemd met een verzoek tot bulkinterceptie op basis van art. 33, zijn de aanbieders verplicht mee te werken aan de uitvoering hiervan:

---

Artikel 37

1. De diensten zijn bevoegd zich te wenden tot een aanbieder van een communicatiedienst met verzoek om medewerking te verlenen aan de uitvoering van een verleende toestemming als bedoeld in artikel 33, tweede lid.
2. De in het eerste lid bedoelde bevoegdheid mag slechts worden uitgeoefend, indien door Onze betrokken Minister daarvoor op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst.

(…)

4. Een toestemming als bedoeld in het tweede lid wordt niet eerder ter uitvoering gebracht dan nadat ter zake met de desbetreffende aanbieder overleg is gevoerd. Het bepaalde in de eerste volzin is niet van toepassing ingeval de toestemming ongewijzigd wordt verlengd.
5. De aanbieder van een communicatiedienst op wie niet reeds ingevolge artikel 13.2 van de Telecommunicatiewet een verplichting tot medewerking rust, is verplicht aan een verzoek als bedoeld in het eerste lid te voldoen.

---

Vanuit privacyoogpunt valt bij dit artikel slechts een enkele kanttekening te plaatsen. De (enorme, zie onder) privacyrisico’s van bulkinterceptie worden niet direct veel groter of kleiner wanneer aanbieders verplicht zijn om mee te werken aan de uitvoering ervan. Mogelijk kan de medewerking, zeker in combinatie met het overleg dat eraan vooraf behoort te gaan (lid 4), een zekere beperkende werking hebben op de reikwijdte van de interceptie, als de aanbieder in de gelegenheid is om mee te denken hoe de interceptie zo doelgericht mogelijk kan zijn met het oog op het beoogde doel; de aanbieders van communicatiediensten hebben er immers belang bij, en ook een wettelijke plicht, om de privacy van hun gebruikers zo goed mogelijk te beschermen. Onduidelijk is echter op welke manier het overleg van lid 4 in de praktijk zal worden gevoerd, en of de aanbieder een gelijkwaardige gesprekspartner is of eerder benaderd wordt met de stok van strafdreiging in de hand, en enkel als een uitvoerend orgaan van wat de diensten willen. Hier zou de MvT meer richting kunnen geven aan het type overleg dat beoogd is, waarbij ook richtlijnen kunnen worden meegegeven die bijdragen aan het serieus nemen van de opmerkingen en argumenten van de aanbieder in het overleg.

Het ontbreken van een bepaling over gegevensbescherming *by design* en *by default* (zie 10) is hier een gemiste kans, omdat een dergelijke bepaling een extra prikkel zou zijn (waarop ook het toezicht kan letten) om de inrichting van de bulkinterceptie zo toegespitst mogelijk te maken alsook adequaat te beveiligen tegen lekken of hacken. Ook de hieronder (par. 8.1.3) behandelde verplichtingen

om de technische voorzieningen na afloop nog een jaar lang beschikbaar te houden (lid 6), en om de kosten voor de technische voorzieningen zelf te dragen (lid 7), vormen een beveiligingsrisico, aangezien het maar de vraag is of (ook kleine) aanbieders van (ook private) diensten voldoende vermogen en expertise hebben om adequate technische voorzieningen te treffen die bestand zijn tegen misbruik of hacken. Op deze punten zou het wetsvoorstel moeten worden versterkt, om zeker te stellen dat bij het aanbrengen van technische voorzieningen om bulkinterceptie te faciliteren, geen achterdeuren of lekken ontstaan.

Wetstechnisch valt nog wel te wijzen op de wat merkwaardige formulering van lid 1, waar de aanbieder 'verzocht' wordt om mee te werken aan de uitvoering van de door de minister verleende toestemming tot bulkinterceptie (art. 33 lid 2), in plaats van mee te werken aan de uitvoering van de bulkinterceptie (art. 33 lid 1). Het gaat immers niet (noch door de diensten, noch door de aanbieder) om uitvoering van een verleende toestemming, maar uitoefening van een bevoegdheid waarvoor toestemming is verleend.

### *8.1.3 Kostenregeling*

Aanbieders van communicatiediensten kunnen niet alleen kunnen worden verplicht mee te werken aan een gerichte of bulkinterceptie, ook moeten zij de investeringskosten om aan het bevel te voldoen zelf dragen. Voor gerichte interceptie geldt art. 32 lid 8, dat art. 13.6 Tw van overeenkomstige toepassing verklaart. Voor bulkinterceptie bepaalt art. 37 lid 7 dat aanbieders de investeringskosten voor de medewerking zelf te dragen. Bovendien moeten de voor bulkinterceptie getroffen technische voorzieningen nog een jaar na afloop van de medewerking in stand blijven. De personeelskosten voor medewerking bij de uitvoering van interceptie worden vergoed (art. 13.6 lid 2 Tw), maar de 'investerings-, exploitatie- en onderhoudskosten voor de technische voorzieningen' moeten aanbieders dus zelf dragen (art. 13.6 lid 1 Tw). Waar dit voor aanbieders van openbare telecomnetwerken of -diensten al in de Tw is bepaald, voor zover het gaat om het technisch mogelijk maken van het gericht aftappen van communicatie, is de kostenverplichting nieuw voor aanbieders die niet onder de Tw vallen (zoals hostingaanbieders en aanbieders van besloten netwerken of diensten); ook is de verplichting nieuw voor openbare aanbieders waar het gaat om het technisch aanpassen van de systemen om bulkinterceptie mogelijk te maken. Het gaat dus om een wezenlijke uitbreiding van de investerings- en onderhoudsverplichtingen van een groot scala aan bedrijven en organisaties.

De investeringskosten om het netwerk aan te passen en te onderhouden zodat aan een tapbevel kan worden voldaan, kunnen aanzienlijk zijn, en vergen zeker voor kleinere bedrijven of instellingen een substantieel deel van de begroting.[109] Nu zijn administratieve lasten als zodanig geen aandachtspunt in een Privacy Impact Assessment, maar de lastenverzwaring van deze regeling brengt wel privacyrisico's met zich mee; als beheerders van private netwerken op eigen kosten technische voorzieningen moeten aanbrengen, en dit aanzienlijke kosten met zich meebrengt, bestaat het risico dat zij houtje-touwtje-constructies gaan aanbrengen waarmee de communicatie van specifieke medewerkers of gebruikers te filteren valt; dat verhoogt de kans aanzienlijk op veiligheidsrisico's in het netwerk, waardoor de communicatie van deze of andere medewerkers of gebruikers op straat kan komen te liggen.

[109] Vgl. Koops e.a. 2005.

De MvT (p. 61 en 84) stelt dan ook geheel ten onrechte dat er geen aanleiding is om voor gerichte of bulkinterceptie een andere kostentoedeling te kiezen dan in de huidige Tw. Hiermee wordt miskend a) dat het bij art. 33 gaat om een nieuw type bevoegdheid (kabelgebonden bulkinterceptie), waarmee aanbieders tot nu niet zijn geconfronteerd, b) de reikwijdte enorm wordt uitgebreid ten opzichte van de Tw-aanbieders (ook webhosting-achtige diensten en besloten netwerken vallen eronder), c) dat de kostenverdeling in de Tw dateert uit een tijd waarin de markt bestond uit enkele grote telecomaanbieders, terwijl het landschap nu veel diverser is, waarbij vooral ook veel kleine spelers actief zijn op wie technische aftapinvesteringen procentueel veel zwaarder drukken dan op grote telecombedrijven, en d) dat waar openbare telecommunicatieaanbieders er bewust voor kiezen om de telecommarkt op te gaan (en er dus voor kiezen aan de Tw gebonden te zijn, inclusief hfd. 13 Tw), aanbieders van besloten netwerken simpelweg communicatiefaciliteiten aan hun medewerkers of gebruikers aanbieden als bijzaak bij hun hoofdactiviteit. Het opleggen van financiële verplichtingen aan besloten aanbieders kan dan ook als nevengevolg hebben dat deze hun medewerkers of gebruikers gaan aanraden, of zelfs verplichten, om in plaats van de tot nu toe gebruikte bedrijfsfaciliteiten over te stappen op gratis emaildiensten als Gmail of Hotmail. Dat levert ook een wezenlijk privacyrisico op omdat dan de communicatie van personen binnen Nederland, die tot nu toe vaak nog beperkt blijft binnen een bedrijf of binnen Nederland, binnen de reikwijdte van de Amerikaanse overheid met haar bulkafluisterprogramma's komt.

Ook is relevant dat deze kostenverdeling geen prikkel oplevert voor de diensten om zo efficiënt mogelijk om te gaan met de bevoegdheid tot bulkinterceptie. Waar de kosten voor uitoefening van de bevoegdheid grotendeels worden geëxternaliseerd – de vergoeding voor personeelskosten bij uitvoering zal vaak maar een fractie zijn van de kosten om het systeem technisch aan te passen en te onderhouden – valt een natuurlijke drempel weg voor de diensten om terughoudendheid te betrachten. Het is een voorbeeld van het faciliteren van geautomatiseerde dataverzameling waarbij natuurlijke drempels wegvallen (zie par. 5.1.3). Wanneer de diensten (tenminste een deel van) de systeemkosten zouden moeten dragen, zou dit bijdragen aan een meer doelgerichte, en dus meer proportionele en subsidiaire, inzet van de bevoegdheden.

Los van de administratieve lastenverzwaring moet dit onderdeel van het wetsontwerp daarom ook vanuit privacyperspectief zeer kritisch worden beoordeeld. Voor het technisch faciliteren van kabelgebonden bulkinterceptie door openbare telecomaanbieders is eerst een aanvullende impactanalyse nodig om te kunnen inschatten of de kostenverdeling niet alleen qua lastenverzwaring maar ook qua privacyrisico's aanvaardbaar is. Voor het technisch faciliteren van gerichte en bulkinterceptie door private aanbieders lijkt ons een principiële afwijzing van deze kostenverdeling aangewezen, omdat op voorhand moeilijk valt in te zien waarom spelregels die gelden voor spelers die zich welbewust op een bepaalde markt begeven, van toepassing kunnen worden verklaard op spelers die niet op die markt actief zijn. Het is immers ook onzinnig om het enkele feit dat voetbal een buitenspelregel kent, te hanteren als argument dat in het basketbal een buitenspelregel moet worden ingevoerd.

### *8.1.4 Vorderen van inhoudsgegevens (art. 38)*

De diensten krijgen hier de bevoegdheid om aanbieders van telecommunicatiediensten te 'verzoeken' om 'gegevens die betrekking hebben op

de telecommunicatie van een gebruiker', waarmee inhoud van communicatie wordt bedoeld, te verstrekken. Ook hier zijn de aanbieders van deze diensten verplicht om hun medewerking te verlenen.

---

Artikel 38

1. De diensten zijn bevoegd zich te wenden tot een aanbieder van een communicatiedienst met het verzoek gegevens te verstrekken die betrekking hebben op de telecommunicatie van een gebruiker die door de aanbieder als onderdeel van de door hem verleende communicatiedienst ten behoeve van een gebruiker is opgeslagen. Bij algemene maatregel van bestuur worden met betrekking tot daarin aangeduide categorieën van communicatiediensten de categorieën van gegevens aangewezen waarop het verzoek betrekking kan hebben.
2. De in het eerste lid bedoelde bevoegdheid mag slechts worden uitgeoefend, indien door Onze betrokken Minister daarvoor op een daartoe strekkend verzoek toestemming is verleend aan het hoofd van de dienst.

(…)

4. De aanbieder van een communicatiedienst is verplicht aan een verzoek als bedoeld in het eerste lid, eerste volzin, te voldoen.

(…)

7. Gegevens verkregen door uitoefening van een bevoegdheid als bedoeld in het eerste lid worden zo spoedig mogelijk op hun relevantie voor het onderzoek waarvoor ze zijn verworven onderzocht. Gegevens, waarvan is vastgesteld dat deze niet relevant zijn voor het onderzoek dan wel niet op hun relevantie voor het onderzoek zijn onderzocht, worden na een periode van ten hoogste twaalf maanden vernietigd.

---

Deze bevoegdheid is nieuw: tot nu toe kunnen diensten alleen verkeers- en gebruikersgegevens opvragen. De inhoud van communicatie valt alleen via interceptie te verkrijgen, maar bij opgeslagen communicatie (denk aan webmail) werkt interceptie niet; de inhoud valt dan alleen op basis van een verzoek tot vrijwillige verstrekking te verkrijgen (art. 17 Wiv 2002). Volgens de MvT is artikel 38 in het leven geroepen omdat relevante gegevens zich steeds minder in de fysieke nabijheid van betreffende onderzoekssubjecten bevinden, maar veelal 'ergens' in de cloud (MvT, p. 85). Deze technologische ontwikkeling, in combinatie met het feit dat communicatiediensten onder de huidige wet niet verplicht zijn om mee te werken aan een verzoek om deze gegevens te verstrekken, zouden zorgen voor een verslechtering van de informatiepositie en onderzoeksmogelijkheden van de diensten. Daarom moet de hier voorgestelde medewerkingsplicht worden ingevoerd, aldus de MvT (p. 85).

Het moge echter duidelijk zijn dat hier sprake is van een zware inbreuk op het recht op bescherming van de persoonlijke levenssfeer van gebruikers. Het gaat om de inhoud van communicatie, die van oudsher kan rekenen op de zwaarste vorm van privacybescherming. Het ligt dan ook voor de hand om deze bevoegdheid aan dezelfde waarborgen te verbinden als gerichte interceptie (art. 32) – wat ook het geval is door ministeriële toestemming te eisen.

Vanuit het oogpunt van voorzienbaarheid bij wet, is artikel 38 niet duidelijk geformuleerd. Het gaat om inhoud van opgeslagen telecommunicatie, maar de gemiddelde burger (en zelfs de gemiddelde jurist) zal dat niet voor ogen staan bij

het lezen van de formulering ‘gegevens (…) die betrekking hebben op de telecommunicatie van een gebruiker die door de aanbieder als onderdeel van de door hem verleende communicatiedienst ten behoeve van een gebruiker is opgeslagen’. Los van de omslachtigheid, lijkt de formulering eerder te suggereren dat het om metadata gaat dan om de inhoud zelf: het betreft immers *gegevens met betrekking tot* de telecommunicatie die is opgeslagen, niet de telecommunicatie zelf. Het is moeilijk in te zien dat de inhoud van een emailbericht gegevens zijn met betrekking tot dat emailbericht; eerder betreft het gegevens waaruit het emailbericht bestaat. Ook de toelichting maakt in de opmerking dat het gaat ‘om gegevens betreffende de inhoud van de telecommunicatie’ (p. 85) dezelfde categoriefout: men wil immers niet gegevens over de inhoud verkrijgen, maar de inhoud zelf. Voor de voorzienbaarheid bij wet en rechtszekerheid is een simpeler en betere formulering nodig. Als er redenen zijn (die wij niet direct zien) om niet gewoon ‘inhoud van telecommunicatie’ te hanteren, zou men eventueel kunnen aansluiten bij de formulering die in de strafvordering voor opgeslagen communicatie wordt gebruikt: ‘gegevens die zijn opgeslagen in het geautomatiseerde werk van de aanbieder en niet voor deze bestemd of van deze afkomstig zijn’ (art. 126ng lid 1 Sv).

Hoewel het hier om een functioneel equivalent lijkt te gaan van het (gericht) onderscheppen van communicatie (in beide gevallen is het doel het verkrijgen van de inhoud, alleen het middel is anders), is dat niet helemaal het geval. Dit heeft te maken met het door elkaar lopen van verschillende clouddiensten, die niet alleen op communicatie maar ook op opslag betrekking kunnen hebben. Volgens de toelichting vallen alle typen clouddiensten hieronder:

> ‘Daarbij moet onder meer worden gedacht aan de inhoud van een mailbox van een gebruiker die in het kader van de door de aanbieder verleende webmaildienst bij hem is opgeslagen, de bij een aanbieder opgeslagen voicemail van de gebruiker, en de door een aanbieder van data-opslagdiensten bij hem opgeslagen gegevens van een gebruiker.’ (MvT, p. 86)

Zoals hierboven (par. 8.1.1 onder ‘Opslagdiensten’) uitgelegd, bestaat er een principieel verschil tussen opslag van communicatie en opslag van documenten. De opslag van *communicatie* is een verlengstuk van het communicatieproces, waarin tegenwoordig communicatie niet alleen maar wordt afgeleverd bij de ontvanger, maar ook beschikbaar blijft bij de aanbieder. Het ligt voor de hand om hierop de interceptiebevoegdheden analoog op toe te passen, in de zin dat in plaats van het onderscheppen tijdens transmissie de inhoud ook via een vordering bij de aanbieder kan worden verkregen. Of de technische veranderingen in dit opzicht daadwerkelijk tot een verslechtering van de informatiepositie van de diensten leiden als deze inhoud niet kan worden gevorderd, mag overigens met een korrel zout worden genomen. De inhoud van communicatie was voorheen vooral vluchtiger, en voor zover deze werd opgeslagen, zoals bij email, konden de diensten deze verkrijgen door het binnendringen in de computer van de gebruiker, maar het lijkt onwaarschijnlijk dat de diensten in substantiële mate in het verleden toegang hadden tot inhoud van opgeslagen communicatie ‘in de fysieke nabijheid van hun onderzoekssubjecten’. Op dit punt is een nadere motivering hoe de informatiepositie precies verslechtert, en ten opzichte van wat, aangewezen.

Tegenover de opslag van communicatie (email, een ingesproken bericht) staat de opslag van niet-communicatieve documenten in de cloud. De diensten van

cloudaanbieders die een grote hoeveelheid opslagruimte beschikbaar stellen, worden vooral gebruikt voor de opslag van muziek, foto's, boeken, dagboeken en andere bestanden en documenten die mensen voorheen (alleen) op hun eigen computer of externe gegevensdrager hadden opgeslagen (en daarvoor alleen in analoge vorm in kasten). Zoals hierboven aangegeven betreft dit niet een verlengstuk van het communicatieproces, maar een verlengstuk van de opslag van gegevens die voorheen hoofdzakelijk binnen de veilige omgeving van de woning werden bewaard. Het vorderen van dit type gegevens is geen functioneel equivalent van het onderscheppen van communicatie, maar van een huiszoeking. Dit type gegevens kon voorheen vrijwel alleen worden verkregen door in de fysieke nabijheid van personen fysiek en handmatig onderzoek te doen. Nu is het onbekend hoeveel huiszoekingen de diensten uitvoeren, maar vanwege de substantiële natuurlijke drempels bij huiszoekingen (het kost menskracht en er is het risico dat de bewoner ontdekt dat de woning wordt of is doorzocht) kunnen het er niet bijzonder veel zijn. Dat betekent dat het argument van een verslechterde informatiepositie voor dit type opslagdiensten sowieso niet opgaat. Integendeel, het argument zou moeten zijn dat de informatiepositie er met grote sprongen op vooruit gaat omdat informatie die voorheen alleen met veel moeite (en met persoonlijk risico voor de medewerkers) te verkrijgen was, nu met een enkel 'verzoek' bij een aanbieder te verkrijgen is, waarbij de informatie hapklaar en automatisch doorzoekbaar wordt aangeleverd (tenzij deze versleuteld is, wat de meeste gebruikers nog niet doen).

Daarmee is ook duidelijk dat het hier om een wezenlijke uitbreiding van de bevoegdheden van de diensten gaat, die ook een zeer ingrijpende privacyinbreuk oplevert. Foto's, muziek, boeken en dagboeken bieden immers een zeer indringende inkijk in iemands privéleven. Wat hierboven is opgemerkt ten aanzien van smartphones (waarbij, zoals het Amerikaanse Hooggerechtshof aangeeft, onderzoek van een smartphone veel meer oplevert dan de meest gedetailleerde huiszoeking) (zie par. 7.2.2), geldt evenzeer voor cloud-diensten die bestaan uit het opslaan van documenten van gebruikers. Evenals voor het binnendringen in computers zou daarom het beschermingsniveau zelfs *hoger* moeten liggen dan de bescherming van huis of communicatie, gezien het feit dat onderzoek van in de cloud opgeslagen privédocumenten veel meer van het privéleven kan blootleggen dan een huiszoeking of telefoontap.

In aanvulling op de hierboven getrokken conclusie (par. 8.1.1) dat de definitie van communicatieaanbieder beperkt moet blijven tot opslagdiensten die aangeboden worden in het kader van communicatiefunctionaliteiten en die daarmee onlosmakelijk zijn verbonden, en dus niet op losstaande cloud-opslagdiensten, zou in het licht van deze analyse dan ook de reikwijdte van art. 38 beperkt moeten zijn tot aanbieders van *communicatie*diensten (zoals email, voicemail en chat). Voor het vorderen van documenten die in de cloud liggen opgeslagen zou de noodzaak zelfstandig moeten worden gemotiveerd (waarbij in aanmerking moet worden genomen dat dit de informatiepositie sterk vergroot ten opzichte van huidige mogelijkheden, met een navenant veel grotere privacyinbreuk dan tot nu toe mogelijk is), en mocht deze noodzaak kunnen worden aangetoond, dan moet hiervoor een zelfstandige grondslag worden gegeven die losstaat van art. 38, en die (nog) zwaardere waarborgen bevat dan art. 38 of art. 32.

Wat de waarborgen in art. 38 zelf betreft moet daarbij nog worden gewezen op de bewaartermijn van lid 7. Gegevens die onder artikel 38 zijn verkregen moeten 'zo

spoedig mogelijk' worden onderzocht op relevantie voor het onderzoek, en gegevens die niet relevant zijn voor het onderzoek (of die nog niet onderzocht zijn) moeten binnen een termijn van 12 maanden worden vernietigd. Een termijn van 12 maanden is echter erg ruim voor een onderzoek dat 'zo spoedig mogelijk' moet plaatsvinden (zie hierover ook par. 4.6.3 en 4.6.4). Het louter vaststellen van een bewaartermijn, zoals in *Weber en Saravia* aangegeven, betekent niet automatisch dat er aan de waarborgen is voldaan. De bewaartermijn op zich moet tot het minimaal noodzakelijke beperkt zijn, en het is niet voorstelbaar dat voor artikel 38 een termijn van een jaar minimaal noodzakelijk is. Het gaat immers om het gericht opvragen van opgeslagen communicatie van specifieke personen, en niet om bulk-interceptie. Het vorderen van de inhoud van communicatie is een dermate ingrijpende bevoegdheid dat hiervoor, vanwege de subsidiariteit, een dringende en gewichtige reden nodig is, en het valt niet in te zien waarom de verkregen inhoud dan niet meteen wordt onderzocht. Als de communicatie binnen een maand nog niet is onderzocht, was er kennelijk ook geen dringende reden om deze überhaupt op te vragen. Evenals bij de nodige andere bewaartermijnen in het wetsontwerp past hier een aanzienlijk kortere bewaartermijn, evenals een verplichting om niet-relevant bevonden gegevens terstond (in plaats van na afloop van de bewaartermijn) te vernietigen.

### *8.1.5 Vorderen van verkeersgegevens (artikel 39)*

In artikel 39 van het wetsvoorstel is de bevoegdheid voor het opvragen van verkeersgegevens vastgelegd. Dit is vergelijkbaar met het huidige art. 28 Wiv 2002, maar vanwege de uitbreiding van de definitie van aanbieders wordt de reikwijdte, en daarmee de mogelijkheid van privacyinbreuk, wel aanzienlijk groter. Zoals hierboven opgemerkt moet de noodzaak van uitbreiding tot andere aanbieders dan onder de Tw vallen nog nader worden gemotiveerd.

Voor de privacybescherming zijn drie aspecten relevant, waarvan twee betrekking hebben op andere wijzigingen in art. 39 Wiv 20xx ten opzichte van art. 28 Wiv 2002. Nieuw is dat de bevoegdheid niet alleen verkeersgegevens die gerelateerd zijn aan een nummer of gebruiker betreft, maar ook zogenoemde 'mastgegevens', dat wil zeggen de gegevens over alle mobiele telefoons die op een bepaald moment met een bepaalde mast in verbinding staan. Dit stelt de diensten in staat om (in het kader van contra-terrorisme) targets aan relevante locaties te linken, doordat communicatieapparatuur (mobiele telefoon) waarvan men weet dat die bij targets in gebruik zijn, dan herkend worden in de verzameling mastgegevens (MvT, p.87). Zoals de MvT terecht opmerkt is daaruit overigens geen volledige zekerheid af te leiden dat een target in de buurt was; de apparatuur kan op het desbetreffende tijdstip ook door een derde in gebruik zijn geweest (MvT, p. 87). De diensten zullen dus alert moeten zijn op de interpretatie van de gegevens, en maatregelen moeten nemen om tunnelvisie te voorkomen.

Het opvragen van mastgegevens vormt een aanzienlijke inbreuk op de privacy. Omdat het om een momentopname gaat (aannemend dat de diensten de bevoegdheid niet zullen gebruiken om hoog-frequent of doorlopend bepaalde masten te bevragen, iets waarop de toezichthouder scherp zal moeten toezien) en om verkeers- en locatiegegevens, en niet inhoud, is de privacyinbreuk voor elk individu beperkt. Het gaat echter wel om heel veel individuen waarvan (althans van hun telefoon) wordt vastgelegd dat ze op een bepaald moment op een bepaalde plaats waren. Wanneer deze gegevens worden gelekt of gehackt en op Internet worden geplaatst (wat niet zelden gebeurt bij hackers die een bepaalde praktijk aan

de kaak willen stellen), kunnen privacygevoelige situaties ontstaan. Het is daarom van belang dat een verzameling mastgegevens zo spoedig mogelijk wordt doorzocht om te kijken of er relevante targets bij zitten, en de overige gegevens niet voor lange tijd te bewaren. Het wetsontwerp bevat echter geen bepaling over onderzoek op relevantie en vernietiging na een bewaartermijn; de algemene bepalingen zijn daarop van toepassing, maar daarin ontbreekt een algemene bewaartermijn (zie par. 4.6). Dat miskent dat het hier gaat om een vorm van massa-surveillance, weliswaar beperkt in tijd maar wel een grote groep mensen betreffend die niet onderwerp zijn van onderzoek door de diensten. Daarom zou voor het opvragen van mastgegevens een bepaling opgenomen moeten worden met een eis de gegevens zo spoedig mogelijk te onderzoeken en met een beperkte bewaartermijn. Gezien de verwantschap met de bulkinterceptie (het in bulk onderscheppen van communicatie) zou de bewaartermijn niet langer moeten zijn dan de termijn die in art. 33 wordt genoemd.

Eveneens nieuw is dat toestemming nodig is op het niveau van de minister of namens deze van het hoofd van de dienst. Verdere mandatering is niet toegestaan. In de huidige bepaling (art. 28 Wiv 2002) is geen toestemming vereist. Het toestemmingsvereiste is een belangrijke waarborg voor de privacvybescherming, en in die zin is het toestemmingsvereiste zeker te onderschrijven. Het past ook om niet-gemandateerde toestemming te eisen, nu de reikwijdte van de bevoegdheid door de uitbreiding van aanbieders zoveel groter wordt. Niettemin is het twijfelachtig of het aldus voorgestelde toestemmingsvereiste wel adequaat is.

Dat heeft te maken met het derde aspect. Hoewel het evenals bij de Wiv 2002 nog steeds gaat om verkeersgegevens, tegenwoordig ook veelal metadata genoemd, en niet om de inhoud van communicatie, is het karakter van onderzoek van metadata inmiddels ingrijpend gewijzigd. Het aantal beschikbare verkeersgegevens is met de enorme toename van communicatie (niet alleen mobiel, maar ook Internet) sinds de eeuwwisseling vele malen groter geworden. Dat zal in de toekomst nog meer het geval zijn, naarmate het Internet der Dingen vorm krijgt. Ook zijn de mogelijkheden om patronen te herkennen in grote dataverzamelingen aanzienlijk verbeterd. Tezamen betekent dit dat op basis van metadata veel informatie afgeleid kan worden, waarmee niet alleen relaties maar ook gedragspatronen op individueel niveau in kaart kunnen worden gebracht. Afhankelijk van de hoeveelheid gegevens en de intensiteit en duur van de periode waarover verkeersgegevens worden verzameld, kan een uiterst gedetailleerd beeld ontstaan over het doen en laten van een individu. Dit is recentelijk ook bevestigd door het Europees Hof van Justitie in de zaak-Digital Rights Ireland. Het Hof zegt over de data die op basis van de Dataretentierichtlijn (2006/24/EG) bewaard moesten worden – dat zijn bepaalde aangewezen categorieën verkeersgegevens – dat deze:

> ‘taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them’[110].

[110] EHJ 8 april 2014, Digital Rights Ireland and Seitlinger and others (C-293/12 en C-594/12), ECLI:EU:C:2014:238, §27.

Inmiddels valt daarom niet meer vol te houden dat de inhoud van communicatie per definitie privacygevoeliger is dan verkeersgegevens; bovendien is het onderscheid aan het vervagen omdat de scheidslijn tussen inhoud en metadata in een Internetcontext nauwelijks te trekken valt.[111] Op basis van het inzicht dat verkeersgegevens een zeer nauwkeurig beeld van iemands persoonlijk leven kunnen opleveren, heeft het EHJ in *Digital Rights Ireland* de Dataretentierichtlijn ongeldig verklaard, mede omdat de Richtlijn onvoldoende eisen stelde aan de autoriteit die toestemming kan geven voor het vorderen van verkeersgegevens.[112] In reactie hierop heeft het kabinet besloten om het toestemmingsvereiste voor het vorderen van verkeersgegevens in de strafvordering op te trekken van het huidige niveau van officier van justitie naar toestemming door de rechter-commissaris.[113] Dit is hetzelfde niveau als voor het onderscheppen van inhoud van communicatie vereist is. Dat is passend, gezien de uitspraak van het EHJ en het inmiddels in de literatuur breed erkende inzicht dat verkeersgegevens tegenwoordig veelal even privacygevoelig kunnen zijn als inhoud van communicatie.[114]

Deze analyse geeft aan dat het toestemmingsvereiste voor het vorderen van verkeersgegevens op hetzelfde niveau zou moeten liggen als voor interceptie van communicatie. Voor de Wiv 20xx betekent dat toestemming door de minister, die niet kan worden gedelegeerd aan het diensthoofd.

### *8.1.6 Vorderen van gebruikersgegevens (artikel 40)*

Artikel 40 (vergelijkbaar met art. 29 Wiv 2002) biedt diensten de mogelijkheid om gebruikersgegevens van communicatiediensten op te vragen. Daaronder vallen nu ook het voor de dienst gebruikte bankrekeningnummer of betalingsmiddel. (Bij dit laatste geeft de MvT, anders dan op veel andere plaatsen, de burger wel inzicht in hoe dit van toepassing is op 21e-eeuwse technologieën, door het voorbeeld te geven van *bitcoin*, p. 89.) Ook hier wordt de medewerkingsplicht uitgebreid naar alle aanbieders van communicatiediensten, inclusief aanbieders van private netwerken of diensten. Dat levert voor deze bevoegdheid geen bijzondere privacyrisico's op, aangezien het hoofdzakelijk om administratieve, NAW-achtige gegevens gaat en niet om concrete communicatie-gerelateerde gegevens.

### *8.1.7 Ontsleutelplicht (artikel 41)*

Op grond van artikel 41 van het wetsvoorstel kunnen de diensten zich wenden tot degene van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van gesprekken, telecommunicatie of gegevensoverdracht die op basis van art. 32 (gerichte interceptie) of art. 33 (bulkinterceptie) is onderschept, met het verzoek alle noodzakelijke medewerking te verlenen tot het ontsleutelen van de gegevens door de kennis beschikbaar te stellen of door zelf de versleuteling ongedaan te maken. De geadresseerde is verplicht hieraan mee te werken, op straffe van gevangenisstraf (maximaal twee jaar bij opzettelijke weigering, maximaal zes maanden bij niet-opzettelijke weigering, art. 132). Het strafrechtelijk gesanctioneerde ontsleutelbevel bestaat al in de Wiv 2002, maar is momenteel beperkt tot het gericht aftappen (art. 25 lid 7). De reikwijdte in het wetsontwerp is aanzienlijk groter, niet alleen omdat de ontsleutelplicht nu ook geldt bij voor

[111] Zie daarover ook Koops & Smits 2014.
[112] EHJ 8 april 2014, Digital Rights Ireland and Seitlinger and others (C-293/12 en C-594/12), ECLI:EU:C:2014:238, §61.
[113] *Kamerstukken II* 2014/15, 33 542, nr. 16, p. 11.
[114] EHJ 8 april 2014, Digital Rights Ireland and Seitlinger and others (C-293/12 en C-594/12), ECLI:EU:C:2014:238, §27.

bulkinterceptie maar ook omdat door de uitbreiding met besloten netwerken er meer soorten telecommunicatie getapt kan worden. Daar staat tegenover dat toestemming van de minister vereist is (lid 2), waar dat momenteel toestemming van het diensthoofd is.

Er is geen aanduiding gegeven van de personen aan wie een dergelijk verzoek kan worden gericht: het gaat om eenieder die (vermoedelijk) zou kunnen ontsleutelen. Dat betreft (medewerkers van) aanbieders van communicatiediensten, voor zover de versleuteling door de aanbieder is aangebracht, dan wel de verzender en ontvanger wanneer de communicatiepartners zelf versleuteling gebruiken. In het laatste geval kan het ook systeembeheerders betreffen als het om bedrijfsmatige communicatie gaat en de organisatie versleuteling gebruikt.

De ontsleutelplicht voor eindgebruikers is vanuit privacyoogpunt problematisch, nu deze onder dreiging van substantiële gevangenisstraf staat, waarbij ook niet-opzettelijke weigering (waaronder ook situaties kunnen vallen waarin iemand het wachtwoord tot de decryptiesleutel is vergeten) strafbaar is – wat een aanzienlijke risicoaansprakelijkheid oplevert. Dat heeft een potentieel verkillend effect op encryptiegebruik door eindgebruikers, wat niet alleen een veiligheidsrisico maar ook een privacyrisico oplevert (zie par. 7.2.8).

De ontsleutelplicht voor aanbieders is iets minder draconisch, omdat het daarbij om beroepsmatige gebruikers van versleuteling gaat, en zeker van communicatieaanbieders die zelf versleuteling aanbrengen mag men verwachten dat zij over het algemeen zorgvuldig met hun encryptie en wachtwoorden omgaan. Niettemin blijft de strafdreiging en daarmee de risicoaansprakelijkheid aanzienlijk, ook voor aanbieders.

De privacyrisico's zouden aanzienlijk groter worden wanneer personen (primair aanbieders van communicatiediensten) gedwongen zouden worden gegevens te *kunnen* ontsleutelen, oftewel om verplicht een achterdeur te installeren. Dat is gelukkig niet het geval: aanbieders hebben de mogelijkheid om hun diensten te (doen) versleutelen op een manier dat zij zelf niet, maar alleen de eindgebruikers, kunnen ontsleutelen. Dat is een belangrijke waarborg voor de veiligheid, en daarmee ook de privacy, van eindgebruikers, omdat zij erop kunnen vertrouwen dat de aanbieder zelf niet in staat is de communicatie te lezen, en in het verlengde daarvan dus ook niet overheden (niet alleen de Nederlandse, maar vooral ook de Amerikaanse, Russische, enzovoorts) de aanbieders kunnen dwingen om de klare tekst van onderschepte communicatie aan te leveren.

## 8.2 Gerichte interceptie

### *8.2.1 Algemene beschouwing over gerichte interceptie*

Artikel 32 van het wetsvoorstel gaat over onderzoek van communicatie met betrekking tot specifieke personen, organisaties en nummers en houdt daarmee 'gerichte' interceptie in. Het gaat zowel om direct afluisteren (van het 'live-gesprek') als om aftappen van telecommunicatie. Dit vormt een zware inbreuk op de privacy: art. 13 Gw stelt de zwaarste eisen aan onderscheppen van middellijke communicatie (en hoewel art. 13 Gw niet het 'live-gesprek' omvat, stelt de wetgever dezelfde eisen aan direct afluisteren als aan aftappen, vgl. art. 126l en 126m Sv) en ook het EHRM heeft in veel zaken benadrukt dat interceptie aan zware waarborgen moet voldoen vanwege de ingrijpende privacyinbreuk (zie Bijlage I). Aangezien

artikel 32 grotendeels (met een belangrijke uitzondering, zie par. 8.2.2) hetzelfde is als het huidige artikel 25 Wiv 2002, gaan we echter niet uitgebreid in op de privacyrisico's van gerichte interceptie als zodanig. We behandelen kort de belangrijkste wijzigingen.

Indien het nummer dat afgetapt moet worden nog niet bekend is, kan dit worden verkregen met een technisch hulpmiddel, zoals een IMSI-catcher. Dat is al zo onder de Wiv 2002, maar nieuw is dat bij de inzet van het technische hulpmiddel de diensten nu ook bevoegd zijn 'om in dat kader van de daarbij ontvangen gegevens kennis te nemen voor zover en zolang dat noodzakelijk is ter vaststelling van het juiste nummer. Ontvangen gegevens die geen betrekking hebben op het hier bedoelde nummer worden terstond vernietigd' (art. 32 lid 4 Wiv 20xx). Volgens de MvT (p. 59) is dit vooral van belang bij 'gebruik van mobiele (data)diensten, zoals WiFi, waarbij tevens sprake is van een grotere groep gebruikers' omdat het scannen van de ether dan niet volstaat. Waarom dat niet volstaat in deze gevallen, wordt daarbij niet uitgelegd, zodat het argument niet direct overtuigt. Aannemend dat er wel goede redenen zijn om in deze gevallen van de inhoud van communicatie kennis te nemen, blijft het privacyrisico beperkt omdat de kennisneming alleen tot doel mag hebben het juiste nummer vast te stellen, en alle gegevens die niet op het nummer betrekking hebben terstond verwijderd moeten worden. Op papier is dat een goede waarborg. In de praktijk kan de verleiding echter soms aanzienlijk zijn om even te blijven luisteren naar een interessant gesprek of nog even door te gaan om een volgend gesprek te horen, ook als aan het begin van een eerste gesprek het nummer al achterhaald is. Daarnaast zal ook de kennis die medewerkers hebben verkregen door van inhoud kennis te nemen bij het achterhalen van het nummer, niet verwijderd kunnen worden – die kennis zit immers in hun hoofd, niet in het technische hulpmiddel. Aan dit laatste valt weinig te doen en is qua privacyrisico overzienbaar; voor het eerste risico – misbruik van bevoegdheid – zullen vooral intern-organisatorische maatregelen als training en een interne cultuur van tegenspraak nodig zijn.

Nieuw is ook lid 6, waarin de zogenoemde 'bijschrijfmogelijkheid' (MvT, p. 60) wordt geregeld: het doortappen op nieuwe nummers van de desbetreffende getapte persoon of organisatie die na de toestemmingverlening bekend zijn geworden. 'Veiligheidsbewuste' onderzoekssubjecten wisselen immers zeer regelmatig van telefoon of nummer (MvT, p. 60). Zoals de MvT terecht opmerkt, ligt dit voor de hand omdat er toestemming is gegeven om deze specifieke persoon of organisatie te tappen, het precieze nummer doet er daarbij niet direct toe. Daarbij licht de MvT toe dat het alleen gaat om nieuwe nummers van de persoon of organisatie zelf – als deze nummers van anderen gebruikt, is hiervoor wel een nieuwe toestemming nodig om te tappen. Daarmee levert lid 6 geen bijzonder privacyrisico op. Wel is van belang dat de diensten uiterst zorgvuldig omgaan met de bijschrijfmogelijkheid: als er fouten worden gemaakt bij het vaststellen van het juiste nummer (bijvoorbeeld schrijffouten of het gebruik van een oud mobiel nummer dat inmiddels bij iemand anders in gebruik is), zal de verkeerde persoon worden getapt. De kans op fouten zal zo klein mogelijk moeten worden gemaakt door intern-organisatorische maatregelen, bijvoorbeeld een dubbelcheck door een collega of afdelingshoofd.

Ook nieuw zijn de medewerkingsplicht tot aftappen voor aanbieders die niet onder de Telecommunicatiewet vallen (lid 7, zie daarover par. 8.1.1) en de

kostenverdeling voor aanpassing van systemen en uitvoering van een tap voor deze aanbieders (lid 8, zie daarover par. 8.1.3).

Verder wordt nu ook een bewaartermijn voorgesteld voor niet-relevante gegevens: lid 10 bepaalt dat gegevens die niet relevant zijn voor het onderzoek of niet op hun relevantie zijn onderzocht, na ten hoogste 12 maanden worden vernietigd. Voor gegevens die niet relevant zijn is dit een lange termijn. Deze gegevens zouden terstond vernietigd dienen te worden zodra bekend is dat deze niet relevant zijn, vergelijkbaar met de onverwijlde vernietigingsplicht die in lid 4 wordt gehanteerd. Er is dan immers geen rechtvaardiging meer voor de verdere verwerking, waaronder ook louter opslag valt.[115] Verder lijkt 12 maanden een lange termijn om gegevens op relevantie te onderzoeken, zoals eerder al is opgemerkt (zie par. 4.6.3). In het geval van interceptie, ook al is deze direct, valt wel te begrijpen dat het enige tijd kan duren voordat gegevens onderzocht zijn; het kan gaan om een grote hoeveelheid communicatie, waarbij gesprekken in de nodige gevallen vertaald door iemand die de specifieke taal beheerst, en vervolgens een voor een oormatig uitgeluisterd moeten worden. Overigens kan met geavanceerde spraakherkenningssoftware (en voor sommige talen vertaalsoftware) in combinatie met automatische filterprogramma's ook in spraak tegenwoordig geautomatiseerd worden gezocht op relevantie. In dat licht zou de onderzoekstermijn van 12 maanden nader kunnen worden onderbouwd.

*8.2.2 Onterechte gelijkstelling van kabelgebonden met niet-kabelgebonden interceptie*

Waar bovenstaande wijzigingen geen grote privacyrisico's met zich meebrengen, is er één onderdeel dat wel fundamentele vragen oproept vanuit privacyperspectief.

> 9. Voor zover het gericht ontvangen en opnemen van telecommunicatie die zijn oorsprong of bestemming in andere landen heeft betrekking heeft op militair verkeer is geen toestemming vereist als bedoeld in artikel 24 en 32, tweede lid. Niet-militair verkeer dat in dit kader wordt ontvangen of opgenomen wordt terstond vernietigd.

Onder art. 25 lid 8 Wiv 2002 kan de MIVD gericht *niet-kabelgebonden* telecommunicatie onderscheppen van of naar het buitenland; hiervoor is geen toestemming nodig als het militair berichtenverkeer betreft. In de Wiv 20xx wordt in art. 32 lid 9 voorgesteld dit ook, via een 'technologieonafhankelijke' formulering, van toepassing te verklaren op gerichte *kabelgebonden* interceptie (vergelijkbaar met de voorgestelde uitbreiding van bulkinterceptie, zie par. 8.3.2). Dit wordt als volgt toegelicht:

'Allereerst is de beperking tot niet-kabelgebonden telecommunicatie komen te vervallen; er is voor gekozen om de bepaling technologieonafhankelijk te formuleren. Ook voor het militaire domein heeft het onderscheid tussen niet-kabelgebonden en kabelgebonden communicatie door de ontwikkelingen in het digitale domein immers aan betekenis verloren. Dit brengt met zich mee dat ook voor het gericht ontvangen en opnemen van kabelgebonden telecommunicatie als hier bedoeld geen toestemming vereist is.' (MvT, p. 61).

Het wetsontwerp stelt hier kabelgebonden interceptie voor als functioneel equivalent van niet-kabelgebonden interceptie. Het wetsontwerp staat hierin niet

[115] Zie EHRM 4 december 2015, Roman Zakharov t. Rusland, §252.

alleen; ook het rapport van de commissie-Dessens en andere rapporten gaan daarin mee. Kennelijk leidt het frame dat de diensten hanteren in hun betoog dat de effectiviteit van niet-kabelgebonden interceptie door technische ontwikkelingen afneemt, zonder nadere analyse tot het zoeken van de oplossing in een automatische uitbreiding van de huidige regeling voor niet-kabelgebonden interceptie met kabelgebonden interceptie. Maar de argumentatie die in dit streven naar 'technologieonafhankelijkheid' wordt gehanteerd, is misleidend en miskent dat niet-kabelgebonden en kabelgebonden interceptie van oudsher principiële verschillen kennen.

Het probleem in de argumentatie is dat de gelijkstelling twee niveaus door elkaar haalt: het feitelijke en het normatieve. Op feitelijk niveau kan vastgesteld worden dat door veranderingen in het technische landschap veel van wat voorheen uit de lucht kon worden opgevangen, tegenwoordig door de kabel gaat. Om dezelfde informatie te verkrijgen als voorheen uit niet-kabelgebonden interceptie, moet daarom meer kabelgebonden interceptie plaatsvinden. Maar dit feitelijke niveau mag niet worden verward met het normatieve niveau: het betekent niet dat kabelgebonden interceptie dezelfde privacyinbreuk oplevert als voorheen niet-kabelgebonden interceptie, en dus ook niet dat dezelfde waarborgen kunnen worden gehanteerd voor kabelgebonden interceptie als voorheen voor niet-kabelgebonden interceptie. Op normatief niveau zou voor een feitelijke uitbreiding van mogelijkheden tot kabelgebonden interceptie juist aangesloten moeten worden bij de waarborgen die voorheen bestaan bij kabelgebonden interceptie.

Wat tot nu toe in de discussie over het streven naar een technologie-neutrale regeling van interceptie miskend wordt, is dat het onderscheppen van etherverkeer van oudsher normatief een aparte categorie vormt. In de telecommunicatieregulering geldt een *sui generis*-regime voor draadloze communicatie (de *Radio Regulations* van de ITU), waarbij het beginsel van vrije ontvangst geldt. Etherverkeer is eenvoudig op te vangen: iedereen kan een antenne in de lucht steken en golven opvangen. (Aanvankelijk was het juist ook de bedoeling van draadloze communicatie dat eenieder die kon ontvangen, zoals noodsignalen of radio-uitzendingen.) Kabelverkeer is daarentegen niet eenvoudig op te vangen: niet iedereen kan zomaar gaan graven en een plug op een kabel zetten. Daarom wordt het aftappen van etherverkeer van oudsher normatief anders benaderd dan het aftappen van kabelverkeer. Dat is duidelijk te zien aan art. 139c Sr: het aftappen van telecommunicatie in het algemeen is strafbaar (lid 1), maar een uitzondering bestaat voor etherverkeer (lid 2 onder 1°): 'Het eerste lid is niet van toepassing op het aftappen of opnemen (…) van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt'. Deze uitzondering heeft te maken met de redelijke privacyverwachting: omdat iedereen een antenne in de lucht kan steken en golven kan opvangen, kan iemand die radiosignalen uitzendt niet redelijkerwijs verwachten dat de signalen niet opgevangen worden tijdens de transmissie.[116] Iemand mag wel verwachten dat in het algemeen geen bijzondere moeite wordt gedaan om zijn communicatie op te vangen: het klassieke voorbeeld is een autotelefoon, waarbij iemand er rekening mee moet houden dat een gesprek door de lucht wordt opgevangen door een lokale ontvanger, maar er geen rekening mee hoeft te houden dat de auto

[116] *Kamerstukken II* 1966/67, 8911, nr. 3, p. 6.

stelselmatig wordt gevolgd om met mobiele scanners de gesprekken vanuit volgauto's op te vangen.[117]

Op normatief niveau is daarom het opvangen van niet-kabelgebonden communicatie een uitzondering, omdat draadloze communicatie gepaard gaat met een lagere privacyverwachting dan kabelgebonden communicatie. Dat is dan ook de reden dat in de Wiv 2002 aparte regelingen bestaan voor niet-kabelgebonden interceptie.

Het feit dat tegenwoordig communicatie vaker door kabels dan door de ether gaat, leidt niet tot een verandering in privacyverwachting: nog steeds is het zo dat iedereen een antenne in de lucht kan steken, maar niet iedereen kan kabels opgraven om afluisterapparatuur te plaatsen. Daarom is de argumentatie in het wetsontwerp dat de feitelijke veranderingen gepaard zouden moeten gaan met een normatieve verandering (dat mensen tegenwoordig een lagere privacyverwachting zouden hebben bij kabel-communicatie) niet steekhoudend, en de keuze om kabelgebonden interceptie op normatief niveau gelijk te stellen met niet-kabelgebonden interceptie is dan ook niet aanvaardbaar.

Toegepast op art. 32 betekent dit dat de keuze om voor het onderscheppen van kabelgebonden militair (berichten)verkeer geen toestemming te eisen, moet worden heroverwogen of beter moet worden gemotiveerd. Daarbij moet wel in aanmerking worden genomen dat het gaat om militaire communicatie. Volgens de MvT levert het onderscheppen daarvan geen privacyinbreuk op:

> 'Belangrijker is dat militair verkeer naar zijn aard niet vergelijkbaar is met het telecommunicatieverkeer tussen gewone burgers, waarbij de persoonlijke levenssfeer van betrokkenen in het geding is.' (MvT, p. 61).

Dat lijkt een belangrijk argument. Het wordt echter niet nader uitgelegd of gemotiveerd, en het valt niet zonder meer in te zien waarom bij militair verkeer de privacy niet in het geding zou zijn. Ten eerste is volgens EHRM-rechtspraak is art. 8 EVRM ook van toepassing op de werkvloer: werknemers moeten ook kunnen rekenen op een zekere mate van privacybescherming.[118] In de zaak-Halford ging het daarbij ook niet om een 'gewone burger', maar om een medewerkster van de politie, waarbij het Hof bepaalde dat het aftappen van haar bedrijfstelefoon in strijd was met art. 8 EVRM.[119] Het valt niet in te zien waarom militair personeel in dit opzicht verschilt van civiel personeel of politieagenten: ook militairen zijn natuurlijke personen die, ook tijdens het werk, aanspraak kunnen maken op bescherming onder het EHRM. Ten tweede gaat het bij het bepalen of er sprake is van een inbreuk op de privacy bij interceptie van communicatie niet om de inhoud van de communicatie, maar om het feit dat er inbreuk wordt gemaakt op de vertrouwelijkheid van het communicatiekanaal. Interceptie van communicatie raakt *als zodanig* de privacy, ongeacht of wat er wordt gecommuniceerd te maken heeft met de persoonlijke levenssfeer, het weer, aandelenkoersen, oorlogsvoering, de politiek of onbegrijpelijk gebrabbel. Dat bij militair telecommunicatieverkeer de inhoud (meestal) niet betrekking heeft op privézaken, is daarom niet relevant voor het bepalen van de privacyinbreuk.

---

*117* HR 13 oktober 1009, *NJB* 6 november 1998, nr. 129.
*118* EHRM 25 juni 1997, Halford t. Verenigd Koninkrijk, §51.
*119* Ibid.

Ten derde is het de vraag of bij kabelgebonden interceptie het militaire verkeer voldoende onderscheidbaar is van het niet-militaire verkeer. Het is onduidelijk op welk verkeer precies wordt gedoeld: gaat het om verkeer over militaire communicatiekanalen of om berichten met een militaire inhoud? In het laatste geval kan het ook het onderscheppen van militair verkeer over civiele communicatiekanalen betreffen. Dat levert aanvullende privacyrisico's op, omdat het de vraag is of het militaire verkeer over dergelijke kanalen voldoende scherp kan worden herkend zodat er geen 'civiele bijvangst' is. Weliswaar bevat lid 9 de waarborg dat opgevangen niet-militair verkeer terstond wordt vernietigd – een belangrijke waarborg die de privacy ten goede komt – maar daarbij is dan wel kennis genomen van de inhoud van de niet-militaire communicatie. Ook kunnen (technische of interpretatie-)fouten worden gemaakt bij gerichte interceptie, waardoor het verkeer van de verkeerde personen wordt onderschept, en het kan enige tijd duren voordat deze fout wordt ontdekt. Dat betekent dat het gericht opvangen van militair verkeer wel degelijk privacyrisico's met zich meebrengt voor niet-militairen wier communicatie en passant kan worden mee-onderschept, zeker als lid 9 ook van toepassing is op militair verkeer dat via civiele kanalen plaatsvindt. Dat deze niet-militaire communicatie terstond wordt vernietigd maakt de privacyinbreuk minder groot, maar niet verwaarloosbaar.

De combinatie van deze drie punten leidt ons tot de conclusie dat er geen enorm grote maar wel enige privacyrisico's gemoeid zijn met gerichte interceptie van militair communicatieverkeer, zowel voor militairen (die ook in hun werk een zekere privacybescherming moeten hebben) als voor derden. De Memorie van Toelichting motiveert onvoldoende waarom voor deze vorm van interceptie geen toestemming nodig zou zijn. Met name als er sprake is van interceptie van militair verkeer over civiele kanalen, lijkt ons eerder toestemming op ten minste het niveau van het diensthoofd aangewezen, gezien de wezenlijke privacyrisico's die gemoeid zijn met kabelgebonden interceptie, ook als deze gericht is op militair verkeer, Waar het niet-kabelgebonden communicatie betreft, waarbij, zoals hierboven aangegeven, een lagere privacyverwachting bestaat, of waar de interceptie beperkt is tot communicatiekanalen die alleen voor militaire doeleinden worden gebruikt, zou interceptie wel zonder toestemming moeten kunnen plaatsvinden.

## 8.3 Bulkinterceptie

Artikelen 33-35 Wiv 20xx regelen de interceptie 'in andere gevallen' dan artikel 32, dat wil zeggen niet gericht op concrete personen of organisaties, waarvoor artikel 32 geldt. Deze regeling vervangt de huidige artikelen 26-27 Wiv 2002, die alleen van toepassing zijn op niet-kabelgebonden telecommunicatie: het verkennen van draadloze telecommunicatie (art. 26) en de ongerichte interceptie en selectie van draadloze telecommunicatie (art. 27). Het gaat hierbij om bulkinterceptie, die in het wetsontwerp ook mogelijk wordt gemaakt voor kabelgebonden telecommunicatie.

### *8.3.1 Terminologie*

Voordat we op de regeling zelf ingaan, is het belangrijk eerst de gehanteerde terminologie te bespreken. De diensten vinden 'ongerichte' interceptie een ongelukkige term, omdat de interceptie niet (volledig) ongericht is – ze vindt immers plaats met een bepaald doel (dat moet ook, vanwege art. 17 Wiv 20xx). Mede om die reden wordt de term 'ongerichte interceptie' zorgvuldig vermeden in het

wetsontwerp en de toelichting bij de nieuwe regeling. De MvT hanteert de term alleen om de bevoegdheden van artikelen 26-27 Wiv 2002 aan te duiden. Voor de interceptie geregeld in artikelen 33 en volgende Wiv 20xx wordt geen bepaalde term gehanteerd – artikel 33 spreekt van interceptie 'in andere gevallen dan bedoeld in artikel 32, indien wordt voldaan aan hetgeen bij of krachtens dit artikel is gesteld'. Dat is niet bepaald een formulering die houvast geeft om te begrijpen welk type interceptie hier bedoeld wordt. Het is dan ook een voorbeeld van verhullend taalgebruik (par. 2.3.2). Interceptie 'in andere gevallen dan bedoeld in artikel 32, indien wordt voldaan aan hetgeen bij of krachtens dit artikel is gesteld' levert volstrekt geen voorzienbaarheid bij wet op, omdat 'in andere gevallen' een open categorie is die alles kan betekenen, en 'indien wordt voldaan aan hetgeen bij of krachtens dit artikel is gesteld' alleen kan worden begrepen na een diepgravende analyse van de zeer complexe regeling, wat alleen voor gespecialiseerde juristen is weggelegd.

Het is daarom belangrijk om een term te hanteren die duidelijker aangeeft wat de bevoegdheid inhoudt. Dat het misschien moeilijk is om een geschikte term te vinden, mag geen excuus zijn om een omschrijving achterwege te laten die een indicatie geeft van het karakter van de bevoegdheid. Wij hebben overwogen om in dit rapport de term 'sleepnetinterceptie' te hanteren, omdat de metafoor van het sleepnet inhoudelijk gezien een vrij precieze aanduiding geeft van het type interceptie. De interceptie is niet ongericht: een sleepnet wordt immers niet ongericht maar weloverwogen in een bepaald gebied ingezet. Het is wel grootschalig: veel in dat gebied komt in het sleepnet terecht. Vervolgens wordt de vangst van het sleepnet gesorteerd, de bijvangst wordt terug- of weggegooid en de vissen waar men geïnteresseerd in is, worden verder verwerkt. Dat is precies wat er bij de interceptie van artikelen 33-35 gebeurt. Wat artikelen 33-35 nog niet doen, maar wel zouden moeten doen (par. 8.3.2 en 4.6), is bepalen dat de selectie terstond na de vangst van de dag plaatsvindt en dat onbedoelde bijvangst direct in zee wordt teruggeworpen; vis gaat immers na een paar dagen stinken, en bij invriezen van de hele vangst gaat alle bijvangst dood. 'Select while you collect' is dan ook een belangrijke stelregel bij gebruik van sleepnetten.

De term sleepnetinterceptie roept daarnaast ook negatieve associaties op, in verband met de ecologische schade die sleepnetten kunnen aanrichten aan de leefomgeving van de vissen. Ook dat is op zich een terechte associatie: massale interceptie van kabelcommunicatie is een vorm van *mass surveillance* die schade toebrengt aan de leefomgeving van burgers, vanwege de grootschalige privacyinbreuk waarbij iedereen in het net terecht kan komen. Zulke ecologische schade is niet per definitie onaanvaardbaar – ook sleepnetten zullen in sommige omstandigheden het enige hulpmiddel zijn om zeer belangrijke vis te vangen – maar de schade aan de leefomgeving moet wel tot het minimum worden beperkt en worden verantwoord als zijnde noodzakelijk in een democratische samenleving. Hoewel de connotaties van de term sleepnet (gericht op een bepaald gebied en bepaald type vissen, grootschalig, bijvangst, risico van ecologische schade) bij elkaar genomen wel een goede aanduiding geven van het type bevoegdheid, overheersen naar onze ervaring bij het gebruik van deze term echter te veel de negatieve connotaties, en blijven de inhoudelijke connotaties (het belang om met een bepaalde methode in een bepaald gebied een bepaald type vissen te vangen) onterecht buiten beeld. Met een te negatieve bijklank is 'sleepnetinterceptie' geen geschikte term om een goed, inhoudelijk, debat te voeren over de voorgestelde bevoegdheid.

Daarom hebben wij uiteindelijk gekozen voor de term ‘bulkinterceptie’, een term die tussendoor ook wel in de MvT wordt gesuggereerd: ‘interceptie als hier bedoeld (interceptie in “bulk”)’ (p. 55; vgl. ook p. 63, 74, 162). Deze term heeft een iets neutraler karakter en brengt eveneens de connotatie van grootschaligheid goed tot uitdrukking.[120] Ook heeft het een zekere connotatie van ongesorteerdheid (de vangst is nog niet uitgesplitst, opgedeeld en verpakt),[121] die wel past bij het karakter van de onderhavige bevoegdheid. ‘Bulkinterceptie’ of ‘interceptie in bulk’ is daarom voor de voorzienbaarheid bij wet een veel duidelijker term dan interceptie ‘in andere gevallen dan bedoeld in artikel 32’.

### *8.3.2 Beschouwing over de voorgestelde regeling*

De regeling van bulkinterceptie wordt anders vormgegeven dan de huidige ‘ongerichte’ interceptie. Het betreft een drietrapsraket:

- **Stap 1 (art 33)**: bulkinterceptie van telecommunicatie; hierop kan alleen een technische analyse worden uitgevoerd om het proces van interceptie te optimaliseren (bijvoorbeeld doelgerichter in te zetten). De gegevens worden drie jaar bewaard;
- **Stap 2 (art 34)**: voorbewerking van onderschepte gegevens. Hierbij kan kennis worden genomen van de inhoud, maar het gaat niet om kennisneming van de inhoud *om de inhoud*, maar om informatie te verzamelen waarmee in het bijzonder het interceptieproces in bredere zin kan worden geoptimaliseerd;
- **Stap 3 (art 35)**. Verdere verwerking. Hierbij vindt (onder meer) selectie van gegevens plaats, waarbij het juist wel gaat om de inhoud van de gegevens en het vaststellen van de relevantie daarvan voor het onderzoek door de diensten. Ook is geautomatiseerde metadata-analyse mogelijk.

De bevoegdheden mogen voor een (telkens verlengbare) periode worden uitgevoerd van twaalf maanden, met uitzondering van de selectie in stap 3 (waarbij het vooral om kennisneming van de inhoud om de inhoud gaat), waarvoor een (telkens verlengbare) periode van 3 maanden geldt. Voor elke stap is toestemming van de Minister nodig.

Over dit onderdeel van het wetsontwerp is al heel veel gezegd, niet alleen door de CTIVD en andere instanties en personen in hun reacties op het consultatiedocument, maar ook in de literatuur. De in die reacties geuite kritiek geeft reeds voldoende aanleiding voor de wetgever om het voorstel te heroverwegen. Daarom geven wij geen integrale analyse van de privacyrisico’s van dit onderdeel, maar beperken wij ons tot enkele opmerkingen die in het verlengde liggen van kanttekeningen die we in dit rapport al bij andere onderdelen hebben gemaakt en die de kritiekpunten van anderen onderstrepen.

Ten eerste moet worden gewezen op het doortrekken van de huidige regeling van niet-kabelgebonden naar kabelgebonden interceptie, waarbij miskend wordt dat de

[120] Merk op dat, hoewel ‘bulk’ duidt op een grote hoeveelheid, het in absolute aantallen niet altijd om enorme hoeveelheden hoeft te gaan; het gaat meer om relatieve aantallen die in de context als ‘relatief veel’ gelden. De Oxford English Dictionary geeft bijvoorbeeld als voorbeeldzin: ‘bulk orders of over 100 copies’: ook kleinere aantallen kunnen aldus in een bepaalde context als ‘bulk’ gelden. Zie http://www.oxforddictionaries.com/definition/english/bulk (geraadpleegd 1 december 2015).
[121] Zie de vijfde betekenis van het woord ‘bulk’ in het Engels: ‘Cargo in an unpackaged mass such as grain or oil’, http://www.oxforddictionaries.com/definition/english/bulk (geraadpleegd 1 december 2015).

privacyinbreuk van kabelgebonden interceptie wezenlijk anders is dan die van niet-kabelgebonden interceptie (zie par. 8.2.2). Dit punt is in de discussie onderbelicht, maar verklaart onzes inziens mede waarom juist dit onderdeel van het wetsontwerp zoveel kritiek krijgt: de bulkinterceptie van kabel-communicatie is van een andere orde dan de huidige bevoegdheden tot niet-kabelgebonden interceptie.

Ten tweede kan, in het verlengde daarvan, erop gewezen worden dat de privacyrisico's zeer groot zijn. Het gaat om bulkinterceptie, en hoewel deze niet volledig ongericht is (dat zou ondoelmatig zijn, en bovendien in strijd met artikel 17 lid 2), gaat het wel om massale interceptie van heel veel mensen, waarvan de overgrote meerderheid niet het doelwit is van de diensten. Hierover heeft het Europees Hof van Justitie vastgesteld dat wetgeving die het mogelijk maakt voor autoriteiten om op een algemene basis toegang te krijgen tot de inhoud van telecommunicatie, 'must be regarded as compromising the essence of the fundamental right to respect for private life'.[122] Daarnaast betekent het huidige en toekomstige communicatielandschap ook dat niet alleen berichten tussen personen worden opgevangen, maar ook alle communicatie in de context van het Internet der Dingen, waarmee dus ook gedragspatronen van burgers in beeld komen. Terwijl in de toelichting veelal uitgegaan lijkt te worden van kabelgebonden verkeer, zoals internetverkeer en emailverkeer, tussen personen, zullen ook met het Internet verbonden auto's, thermostaten, sensornetwerken en veel andere technologieën die in de (nabije) toekomst worden uitgerold binnen de context van het Internet der Dingen binnen de reikwijdte vallen. Daarnaast betekent een dergelijk grote reikwijdte dat de bevoegdheden een veel grotere impact zullen hebben dan door de meesten voorzien zal worden, aangezien 'connected' technologieën en persoonlijke apparaten die iemand heeft een uitzonderlijke rijkheid aan gegevens en informatie kunnen bevatten en blootleggen. Juist de koppelingen van dergelijke apparaten en het genereren van gegevens door die apparaten en sensoren in een gestructureerde vorm, maakt dat de impact op privacy van bulkinterceptie veel groter kan zijn dan op het eerste gezicht zal lijken. In dat licht wordt het criterium van voorzienbaarheid niet vervuld, omdat de toelichting hier niets over zegt.

Daarbij moet worden benadrukt dat ook het enkele vastleggen van al deze gegevens, zonder kennisneming van de inhoud, een meer dan geringe privacyinbreuk vormt, in tegenstelling tot wat de MvT (p. 68) beweert, omdat het massaal vastleggen van informatie een verkillend effect kan hebben op het gedrag van burgers.[123] Verder moet het privacyrisico van analyse van metadata niet worden onderschat; geautomatiseerde analyse van metadata is qua privacyinbreuk niet minder ingrijpend dan kennisneming van inhoud (zie par. 8.1.5) – het is in dat licht twijfelachtig dat voor het eerste in art. 35 minder waarborgen (want een langere periode) gelden dan voor het laatste.

In het licht van de zeer grote privacyrisico's, zijn, ten derde, waarborgen cruciaal om te voorkomen dat de bevoegdheden ongebreideld worden toegepast. Een cruciale waarborg is het vereiste van doelbinding (art. 17 lid 2, zie par. 4.1). Dit

[122] EHJ 6 oktober 2015, Schrems (C-362/14), ECLI:EU:C:2015:650, §94.

[123] Vgl. EHRM 29 juni 2006, Weber en Saravia t. Duitsland, §78: '*the mere existence of legislation* which allows a *system for the secret monitoring* of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, *irrespective of any measures actually taken against them*' (cursivering toegevoegd).

vereiste betekent dat ook bij bulkinterceptie deze zoveel mogelijk toegespitst moet zijn op communicatiestromen die het meest relevant voor de diensten zijn, en vooral dat er zo snel mogelijk selectie moet plaatsvinden om de nadere verwerking te beperken tot de kring van personen die tot het aandachtsveld van de diensten behoren. Een snelle beoordeling op relevantie van gegevens is daarom nodig, gevolgd door het terstond vernietigen van gegevens die niet relevant blijken te zijn. Jacobs heeft deze werkwijze uiteengezet en pleit daarom voor een aanpak in twee fasen (in plaats van de voorgestelde drie stappen, die nogal kunstmatig zijn en in de praktijk moeilijk scherp te scheiden). In de eerste fase, van 'vluchtigheid', wordt vluchtig gekeken naar relevantie, en dus niet systematisch-inhoudelijk, van gegevens; de vluchtige blik wordt direct en doorlopend uitgevoerd bij elke binnenkomst van gegevens, en irrelevante gegevens worden terstond verwijderd zodra is vastgesteld dat ze niet relevant zijn, volgens het principe 'select while you collect'.[124] De tweede fase, van stelselmatigheid, is gericht op het daadwerkelijke, inhoudelijke onderzoek van de aldus gefilterde (en meer relevant en daarom hoogwaardiger geworden) gegevensverzameling.[125] Met een goede naleving van het doelbindingsvereiste wordt de inbreuk op de persoonlijke levenssfeer van met name personen die niet de aandacht van de diensten (zouden moeten) hebben, zo beperkt mogelijk gehouden.

Daarnaast is de belangrijkste waarborg in het wetsontwerp toestemming op ministerieel niveau. Het toestemmingsvereiste is versterkt in stap 1, waar voorheen geen toestemming nodig was en nu wel toestemming van de minister nodig is. Dat is een belangrijke waarborg, in elk geval op papier; het zal van de uitvoeringspraktijk afhangen of de minister niet dusdanig be- of overvraagd wordt dat ministeriële toestemming verwordt tot een stempelmachine.[126] Daarbij is het ook de vraag of de afzonderlijke ministeriële toestemming voor elke stap veel meerwaarde heeft. De minister zou alleen een last moeten afgeven voor stap 1 indien hij ook voornemens is ook een last voor stap 2 en 3 af te geven in de context van het onderzoek waarvoor de bulkinterceptie nodig wordt gevonden. Die stappen moeten immers tot op zekere hoogte vooraf duidelijk zijn om stap 1 te kunnen legitimeren. Het zou meer normerende werking hebben om de toestemming in stap 1 al explicieter aan een zo specifiek mogelijk omschreven doel te verbinden, waarmee zekergesteld wordt dat een opgebouwde gegevensset niet voor andere doelen kan worden gebruikt; de algemene eis van doelbinding van art. 17 lid 2 heeft minder slagkracht dan een specifiek doelspecificatie- en doelbindingseis in art. 33 zou hebben.

Ook de mogelijke duur waarvoor toestemming kan worden gegeven – een jaar voor stap 1, 2 en 3 (metadata-analyse) – biedt geen duidelijke privacywaarborg. Juist de grote kwantitatieve omvang van de gegevensverzameling zou een reden moeten

[124] Een snelle, vluchtige selectie zal in sommige contexten eenvoudiger uit te voeren zijn dan in andere; zo kan het bij militaire operaties in het buitenland bijvoorbeeld moeilijk zijn om op voorhand al veel gegevens uit te filteren als niet relevant, omdat de dreigingsbeelden diffuus kunnen zijn. Dat doet echter niets af aan het principe: verzamelde gegevens kunnen zo spoedig mogelijk met een vluchtige blik bekeken worden op relevantie, en waar duidelijk is dat gegevens niet relevant zijn voor het doel van de gegevensverzameling, kunnen deze terstond worden verwijderd.

[125] Zie Jacobs 2015 en Jacobs 2016.

[126] Vgl. CTIVD (2015), p. 13: 'Hierbij onderkent de CTIVD overigens dat op dit punt alleen sprake kan zijn van een waarborg indien het vereiste van ministeriële toestemming niet in zoveel gevallen wordt gesteld, dat een aanvraag vooral een administratieve invuloefening voor de diensten wordt en de inhoudelijke toets van de minister aan waarde verliest.'

zijn om de termijn waarvoor de toestemming verleend kan worden te beperken. Een beperktere termijn biedt een prikkel tot spoedige selectie van relevante gegevens en het sneller verwijderen van niet-relevante gegevens. Een verzoek tot verlenging van de toestemming kan dan in de verlengingsperiode ook specifieker en gerichter worden onderbouwd en uitgevoerd, waarmee de privacy van burgers die geen target zijn beter gewaarborgd kan worden.

De algemene waarborgen van subsidiariteit en proportionaliteit lijken bij toestemming vooraf ook geen sterk normerende werking op art. 33-35 te kunnen hebben vanwege het dynamische karakter van het proces, omdat de stappen interacteren en in beweging zijn. In de praktijk is de drietrap niet zo duidelijk aanwezig als op papier wordt voorgesteld. Meestal is er sprake van iteraties in het doorzoeken van een gegevensset of het voortdurend aanvullen van een gegevensset waarop een last is afgegeven door de minister om technische kenmerken te analyseren.[127] Het dynamische karakter maakt het moeilijk om in de wettekst, en in het verzoek om toestemming vooraf en in de toestemming zelf, strakke grenzen te trekken; de toets op rechtmatigheid zal vooral tijdens het uitvoeringsproces doorlopend moeten worden uitgevoerd. Dat onderstreept het belang van onmiddellijk toezicht door de CTIVD met de mogelijkheid om in te grijpen zodra deze vaststelt dat de uitvoering disproportioneel of doelafwijkend wordt.

Naast direct en onafhankelijk toezicht ligt de belangrijkste waarborg in de omgang met niet-relevante gegevens. Hier moet gewezen worden op het punt dat we op diverse plaatsen al hebben gemaakt over de gebrekkige motivering van bewaartermijnen, die in het algemeen langer lijken te zijn dan nodig. In het geval van bulkinterceptie moet de voorgestelde bewaartermijn zeker worden heroverwogen.

Een bewaartermijn van drie jaar voor gegevens uit stap 1 is erg lang. Onduidelijk is of dit een absolute bewaartermijn is, of dat deze langer wordt als het onderzoek van art. 34 of 35 op de gegevensverzameling van art. 33 nog loopt en dus de relevantie van de dataverzameling nog vastgesteld aan het worden is. De MvT geeft daarover, voor zover wij het lezen, geen uitsluitsel. Ook wanneer we uitgaan van een bewaartermijn van alle gegevens voor een bepaald onderzoek van drie jaar, gaat het om een zeer lange periode (substantieel langer bijvoorbeeld dan de Dataretentierichtlijn toestond, die wegens een te grote privacyinbreuk ongeldig is verklaard). De MvT geeft aan dat de huidige termijn van één jaar (bij niet-kabelgebonden telecommunicatie) ‘in de praktijk van de diensten al jaren als een groot knelpunt ervaren’ wordt (p. 68), maar waarom dat zo’n groot knelpunt is wordt niet duidelijk, noch waarom de termijn verdrievoudigd zou moeten worden. Zoals in onze algemene beschouwing opgemerkt (par. 2.3.1), gaat het wetsontwerp wel erg makkelijk uit van de behoeften uit de praktijk in plaats van de normerende werking die de wet behoort te hebben op de praktijk.

[127] In het geval van de MIVD zijn bijvoorbeeld concrete situaties waar de noodzaak tot het combineren van stap één en twee ontstaat. Vanwege vereiste snelheid gedurende een opdracht binnen een missie kan het noodzakelijk zijn om de stappen parallel uit te voeren. Tevens is het mogelijk dat bij een missie op een vaartuig de ruimte dusdanig beperkt dat stap één en twee noodzakelijkerwijs door eenzelfde persoon worden uitgevoerd. Ook de CTIVD heeft in haar reactie op het wetsvoorstel aangegeven dat de stappen in de praktijk door elkaar lopen.

Los van de precieze lengte van de bewaartermijn is een principieel bezwaar tegen de regeling dat gegevens waarvan vastgesteld is dat deze niet relevant zijn, pas na afloop van de maximale bewaartermijn worden vernietigd, en niet terstond na het moment van vaststelling van niet-relevantie. Het bewaren van niet-relevante gegevens levert een privacyrisico op (van hacken, lekken of misbruik) terwijl het bewaren niet nodig is – de gegevens zijn immers niet-relevant. Bij bulkinterceptie (maar even goed bij andere bevoegdheden waarbij grote hoeveelheden data worden verzameld waar veel niet-relevante gegevens tussen zullen zitten, zoals vorderen van gegevensbestanden, geautomatiseerde toegang tot gegevensbestanden, of OSINT) moet het uitgangspunt zijn een continue selectie op relevantie: 'select while you collect'[128] en in de vervolgstappen 'select while you analyse'. Hierbij omvat selectie inherent ook de directe verwijdering van gegevens zodra blijkt dat die niet relevant zijn: selecteren is immers niet alleen het kaf van het koren onderscheiden, maar ook het kaf gelijk weggooien.

[128] Zie daarover Jacobs 2016, een uitgebreidere versie van Jacobs 2015.

# 9 Toezicht

Over het toezicht op de diensten is al heel veel gezegd, zowel in het algemeen als in de discussie naar aanleiding van de commissie-Dessens en het wetsontwerp. Daarom hebben wij ervoor gekozen om andere, meer onderbelichte delen van het wetsontwerp meer aandacht te geven en niet de discussie over toezicht te herhalen. Wij beperken ons hier tot twee aandachtspunten in relatie tot de CTIVD – de belangrijkste steunpijler van het stelsel van toezicht – die samenhangen met de lijnen die we in voorgaande hoofdstukken hebben uitgezet.

In veel opzichten is de vormgeving van het toezicht door de CTIVD waardevol. De CTIVD is onafhankelijk (de leden worden door het parlement voorgedragen, er is geen sprake van ondergeschiktheid aan de verantwoordelijke ministers); heeft toegang tot alle gegevens en stukken waar de diensten mee werken, ook geclassificeerde;[129] kan een proactieve houding aannemen om de praktische uitvoering van de taken van de diensten te controleren, met toezicht op de activiteiten van de diensten in brede zin[130]. Met name onafhankelijk toezicht op eigen initiatief en over het brede scala aan activiteiten is van groot belang, vanwege de complexiteit van de wet (vgl. par. 2.3.3) en van de uitvoeringspraktijk (vgl. par. 8.3.2), en vanwege te technologie-onafhankelijke formulering die ertoe leidt dat bevoegdheden in potentie een zeer ruim toepassingsbereik hebben. Om dezelfde redenen is het essentieel dat toezicht doorlopend kan plaatsvinden, dus niet alleen achteraf maar ook tijdens de uitoefening van bevoegdheden.[131]

Het is echter niet voldoende dat onafhankelijk toezicht doorlopend plaatsvindt, het moet ook effectief zijn. Het eerste aandachtspunt dat wij willen benadrukken is dan ook dat de CTIVD de mogelijkheid moet krijgen om bindende besluiten te nemen. In *Kennedy* heeft het EHRM de bindendheid van een oordeel nogmaals benadrukt als een essentieel onderdeel van effectief toezicht. De toezichthouder moet daadwerkelijk een onrechtmatigheid kunnen voorkomen of beëindigen: ‘In the event that the IPT finds in the applicant's favour, it can, *inter alia*, quash any interception order, require destruction of intercept material and order compensation to be paid’.[132] Het gaat bij toezicht immers om het effectief kunnen voorkomen of beëindigen van een onrechtmatige uitoefening van een bevoegdheid. Op grond van de vereisten uit het EVRM dient een oordeel van de CTIVD dan ook juridisch bindend te zijn om van effectief toezicht te kunnen spreken.[133] Die conclusie is ook getrokken door het Hof Den Haag: toezicht voldoet alleen aan de eisen van artikel 8 EVRM als het zowel onafhankelijk als effectief is, met de mogelijkheid om daadwerkelijk de uitoefening van een bevoegdheid te beëindigen.[134]

---

*129* Vgl. EHMR 4 december 2015, Roman Zakharov t. Rusland, §284.
*130* Vgl. Council of Europe Commissioner for Human Rights 2015, p. 49: ‘Examples of expert oversight bodies whose mandate covers this broad scope of security services’ personal data-related activities include (…) the Netherlands’ CTIVD’.
*131* Vgl. Council of Europe Commissioner for Human Rights 2015, p. 49: ‘Recognising the value of *ongoing*, expert, non-partisan oversight’ (cursivering toegevoegd).
*132* EHRM 18 mei 2010, Kennedy t. Verenigd Koninkrijk, §167.
*133* Zie ook de hoofdconclusie op dit punt van Loof e.a. 2015, p. 39: ‘Een niet volledig expliciet geformuleerde, maar desalniettemin duidelijk te herkennen, eis van *bindend* ex post rechtmatigheidstoezicht door een onafhankelijke toezichthouder’ (cursivering toegevoegd).
*134* Gerechtshof Den Haag, 27 oktober 2015, zaaknr. 200.174.280-01, ECLI:NL:GHDHA:2015:2881, §2.9: ‘Dit neemt niet weg dat de voorzieningenrechter terecht uit de rechtspraak van het EHRM heeft afgeleid dat onafhankelijk toezicht in de door het EHRM

Momenteel kan de CTIVD nog geen bindende besluiten nemen. Indien de CTIVD iets onrechtmatig acht wordt dit voorgelegd aan de verantwoordelijke minister die vervolgens op grond van het concept-wetsvoorstel een heroverwegingsplicht heeft (die overigens ook nog minimaal wordt ingevuld omdat het beperkt is tot de uitoefening van bevoegdheden die ministeriële toestemming vereisen). Hoewel daarbij het parlement (CIVD) ingelicht moet worden en de minister dus politiek ter verantwoording kan worden geroepen als hij een oordeel van de CTIVD negeert, blijft de uiteindelijke beslissing bij de minister liggen, die niet onafhankelijk is. Een onafhankelijk bindend oordeel over rechtmatigheid is daarom momenteel niet aanwezig.

Het wetsontwerp komt hier ten dele aan tegemoet door de CTIVD de bevoegdheid tot bindende oordelen te laten geven binnen de procedure voor klachtbehandeling. Op basis van een klacht zal de CTIVD kunnen bepalen dat een lopend onderzoek wordt gestaakt, de uitoefening van een bijzondere bevoegdheid wordt beëindigd (maar kennelijk niet de uitoefening van de algemene bevoegdheid, die op basis van art. 22 lid 3 zich ook over langere tijd kan uitstrekken; onduidelijk is waarom de CTIVD zich hierover niet op klacht zou kunnen uitspreken), of dat gegevens worden verwijderd en vernietigd (art. 113 lid 4 Wiv 20xx). De Minister is verplicht dit oordeel van de CTIVD uit te voeren (art. 113 lid 5).

Dit bindend adviesrecht binnen de klachtprocedure is een uiterst waardevolle versterking van het toezicht, omdat daarmee de effectiviteit van het toezicht aanzienlijk wordt versterkt. Voor de privacybescherming biedt dit onderdeel dan ook een aanzienlijke versterking. Het is ook in lijn met de *Kennedy*-uitspraak die het toezicht door de Britse toezichthouder IPT betreft in relatie tot de procedure van klachtbehandeling.

Het blijft evenwel de vraag of dit voorstel voldoende is voor een adequate afdekking van alle in de voorgaande hoofdstukken aangegeven privacyrisico's. Het bindend oordeel wordt immers afhankelijk van het feit of iemand een klacht indient. Het hoeft niet zo te zijn dat de grootste privacyrisico's ook het snelst tot een klacht leiden. Sommige privacyrisico's zijn relatief onzichtbaar voor de betrokkenen; het kan jaren duren voordat een handeling van de diensten tot feitelijke gevolgen leidt bij betrokkenen; en het zal niet altijd voor betrokkenen duidelijk zijn dat bepaalde situaties (bijvoorbeeld het weigeren van een vergunning of het geweigerd worden van een vlucht op een buitenlands vliegveld) het gevolg zijn van bepaalde handelingen van de diensten uit het verleden. Onterechte handelingen van de diensten zullen daarom niet in alle gevallen, of niet altijd tijdig, tot klachten leiden. Het valt niet goed in te zien waarom de CTIVD wel een bindend oordeel kan geven over een bepaalde onrechtmatigheid of onaanvaardbaar privacyrisico als dit ontdekt wordt nadat een klacht is ingediend, maar niet wanneer dezelfde onrechtmatigheid of hetzelfde onaanvaardbare privacyrisico ontdekt wordt door de CTIVD tijdens de

---

bedoelde zin niet denkbaar is indien het toezichthoudende orgaan niet op zijn minst de bevoegdheid heeft om het (direct of indirect) tappen van advocaten te voorkomen of te beëindigen. (…) [D]e voorzieningenrechter heeft met zoveel woorden overwogen dat de onafhankelijke toets niet in alle gevallen voorafgaand aan de inzet van bijzondere bevoegdheden hoeft plaats te vinden (rechtsoverweging 4.14), mits het toezichthoudende orgaan de bevoegdheid heeft het tappen van advocaten te voorkomen *of* te beëindigen.' Hierbij wordt verwezen naar EHRM 22 november 2012, Telegraaf Media t. Nederland, §100: 'the use of special powers would appear to have been authorised by the Minister of the Interior and Kingdom Relations, if not by the head of the AIVD or even a subordinate AIVD official, but in any case without prior review by an independent body with the power to prevent *or terminate* it' (cursivering toegevoegd).

zelfstandige uitoefening van het toezicht, bijvoorbeeld bij een steekproefcontrole. De kern van effectief toezicht ligt immers in de aard van wat er door de toezichthouder wordt geconstateerd, niet in de aanleiding van een onderzoek. In dat licht zou de wetgever nadrukkelijk moeten overwegen om de CTIVD in het algemeen bindend adviesrecht te geven ook buiten de klachtprocedure om.

Het tweede aandachtspunt volgt uit de nog steeds in belang toenemende rol van technologie in de taakuitoefening van de diensten. In voorgaande hoofdstukken hebben we aangegeven dat de uitoefening van bevoegdheden vaak niet los kan worden gezien van de technologie die daarbij wordt ingezet. Juist ook omdat de keuze voor zo technologie-onafhankelijk mogelijke bepalingen ertoe leidt dat de wet zelf abstraheert van technologieën, is het essentieel dat er zicht komt en blijft bestaan op de manier waarop technologieën worden ingezet in de uitvoeringspraktijk. Die bepaalt immers mede de reikwijdte van de inzet van bevoegdheden en daarmee ook de mate en wijze van privacyinbreuk. Bovendien, en hier ligt ook een verband met het voorgaande punt van doorlopend toezicht, kunnen technische ontwikkelingen er vaak toe leiden dat grijze gebieden ontstaan, omdat de toepassing van de wet op nieuwe technologische mogelijkheden interpretatie vergt. Het risico bestaat dan ook dat de diensten, als zij niet in de hand worden gehouden door onafhankelijk en effectief toezicht, te ruim gaan experimenteren met nieuwe technologieën in dit grijze gebied (wat ook weer een risico inhoudt dat ontstane praktijken in donkergrijze gebieden te gemakkelijk wit geverfd gaan worden door codificatie in een opvolgende wet, zie par. 2.3.1).

Nu bestaat de CTIVD hoofdzakelijk uit juristen. Technische expertise is slechts beperkt aanwezig en wordt vaak op basis van detachering betrokken. Adequate technische inbreng in de CTIVD is noodzakelijk, gezien de vele, diverse en complexe technologieën die worden toegepast door de diensten. De CTIVD heeft weliswaar onbeperkt toegang tot de diensten en kan dus binnenlopen en inzage vragen wanneer gewenst. Maar het vergt specialistische technische expertise om daarbij ook inzicht te krijgen in de technische methodieken voor bijvoorbeeld het analyseren van metadata, of om de billijkheid en robuustheid van filteringsystemen, profileringsalgoritmes en programmatuur gebaseerd op machinaal leren te kunnen beoordelen. Daarom moet worden geïnvesteerd in technische expertise binnen de CTIVD.[135] Die investering zal veel verder moeten gaan dan het inhuren van experts: integratie tussen technische en juridische perspectieven is nodig om een adequate rechtmatigheidstoets te kunnen uitoefenen. Dergelijke integratie kan alleen worden bereikt als technische en juridische deskundigen op langdurige basis samenwerken en op de werkvloer steeds in elkaars nabijheid zijn. Naast investeren in technische expertise bij de toezichthouder, kunnen de met de continue technologische ontwikkelingen samenhangende risico's ook binnen de perken worden gehouden door in de wet een bepaling op te nemen over privacy en gegevensbescherming in het ontwerp en als standaard in systemen (zie hfd.10). Ook dat hangt weer samen met de rol van de toezichthouder, omdat een dergelijke bepaling de CTIVD in staat stelt rechtmatigheidstoezicht uit te oefenen op de manier waarop systemen bij de diensten technisch worden ingericht, wat belangrijk is omdat technisch ingebouwde waarborgen en beperkingen privacyrisico's sterk kunnen inperken. Ook daarvoor

[135] Vgl. European Union Agency for Fundamental Rights 2015, p. 58: 'While understanding the legal aspects of surveillance is indispensable, expert bodies must also be technically competent. Some Member States ensure this by including experts from a range of fields, including information and communications technology (ICT).'

heeft de CTIVD dan wel technische expertise nodig, om de systeeminstellingen goed te kunnen beoordelen.

In het verlengde van het tweede aandachtspunt over technische expertise, willen we ook nog een vergelijkbare overweging meegeven met betrekking tot het voorstel toezicht en klachtenafhandeling bij de CTIVD strikt te scheiden. In het wetsvoorstel wordt de CTIVD in twee afdelingen gesplitst, een afdeling toezicht en een afdeling klachtbehandeling. Om onafhankelijkheid te waarborgen wordt een strikte scheiding tussen de afdelingen nagestreefd. Een klacht over een werkwijze of een specifiek geval kan immers situatie betreffen waar de CTIVD tevens toezicht over heeft uitgeoefend. Medewerkers kunnen daarom niet voor beide afdelingen tegelijk werkzaam zijn. Hoewel een dergelijke scheiding de onafhankelijkheid ondersteunt, mag dit echter niet ten koste te gaan van de kwaliteit van het toezicht of de klachtbehandeling. Bij een strikte institutionele scheiding kunnen de deskundigheid en ervaring die door medewerkers van de afdeling toezicht worden opgebouwd, niet worden ingezet in het kader van klachten, en omgekeerd kunnen de gedetailleerde inzichten die klachtprocedures bieden in concrete uitvoeringspraktijken, alsook in de feitelijke effecten daarvan voor de privacy van burgers in concrete gevallen, niet geïntegreerd worden in de manier waarop het toezicht plaatsvindt. De voorgestelde scherpe institutionele scheiding zou daarom ten koste kunnen gaan van de kwaliteit, zowel van het toezicht als van de klachtbehandeling. Een institutionele scheiding die ten koste gaat van een adequaat kennisniveau bij beide afdelingen valt daarom af te raden. Volledige institutionele scheiding is volgens Loof en anderen ook niet noodzakelijk.[136] Mogelijk kunnen tussenvormen worden overwogen die zowel onafhankelijkheid waarborgen (door te bepalen dat medewerkers die in het kader van toezicht betrokken zijn geweest bij een concrete activiteit van de diensten niet tevens betrokken kunnen zijn bij een klachtenprocedure over deze zelfde activiteit) als synergie tussen de afdelingen te bevorderen waarbij de inzichten die opgedaan worden vanuit toezicht en klachtbehandeling elkaar wederzijds kunnen bevruchten.

[136] Zie Loof e.a. 2015, p. 41.

# 10 Privacy en gegevensbescherming *by design* en *by default*

## 10.1 Het belang van technische verankering van privacy en gegevensbescherming

In aanvulling op en ter ondersteuning van wettelijke normering, is voor privacybescherming ook van belang dat privacy en gegevensbescherming in het ontwerp van systemen worden ingebouwd – een notie die aanvankelijk vooral Privacy by Design werd genoemd, maar inmiddels, omdat het vooral gaat om de beginselen van bescherming van persoonsgegevens, Data Protection by Design wordt genoemd. Daar is ook het belang aan gekoppeld om de standaardinstellingen in systemen op de meest privacyvriendelijke manier te zetten, zodat gebruikers niet extra moeite moeten doen om gegevens beter te beschermen: Data Protection by Default. Gegevensbescherming *by design* is nauw verwant aan Privacy *by design*, wat echter lastiger is af te bakenen en te concretiseren, omdat het recht op privacy een vrijheidsrecht is dat zich niet eenvoudig laat definiëren en waarvan de normen over het algemeen minder gedetailleerd zijn uitgewerkt in concrete regels.

In de voorgestelde Algemene verordening gegevensbescherming wordt aan de verantwoordelijke die persoonsgegevens verwerkt de verplichting opgelegd tot gegevensbescherming *by design* (DPbDesign) en *by default* (DPbDefault) (art. 23 Avg). Het laatste ziet vooral op de eis om de verwerking te allen tijde te beperken tot wat noodzakelijk is voor het expliciet gespecificeerde doel. Dit wordt vaak kort samengevat als dataminimalisatie en vereist een proportionaliteitstoets. Gegevensbescherming *by default* betekent dat de technische systemen die de verwerking mogelijk maken, zo moeten zijn ontworpen en ingericht dat zo min mogelijk persoonsgegevens worden verwerkt. DPbDesign is – binnen het kader van de Verordening – een breder begrip, dat ziet op het zoveel mogelijk verankeren van alle regels uit de Verordening in de betrokken technische systemen; denk aan inzageverzoeken, informatieverplichtingen, uitoefening van het verzetsrecht of het verbod om, behoudens toegestane uitzonderingen, gegevens buiten de jurisdictie van de EU te brengen.

Hoewel de Verordening niet van toepassing is op de inlichtingen- en veiligheidsdiensten, is de notie van DPbDesign en DPbDefault (die we in het navolgende samennemen onder de noemer van DPbD) ook voor de diensten van groot belang. Het gaat om een notie die hard op weg is om zich te nestelen binnen de standaard-catalogus van beginselen van persoonsgegevensbescherming, en die dan ook via de band van rechtsontwikkeling onder artikel 8 EVRM, in samenhang met artikelen 7 en 8 van het Handvest, vroeg of laat zijn weerslag zal hebben op de activiteiten van de diensten. Door nu reeds aandacht te besteden aan DPbD, wordt de kans dan ook groter dat de Wiv 20xx toekomstbestendig zal zijn. Maar los van de juridische inbedding gaat het vooral om een notie die de mogelijkheid biedt om de balans te versterken die de Wiv 20xx zoekt tussen effectieve bescherming van de nationale veiligheid en het respecteren van grondrechten, waaronder privacy en gegevensbescherming.

We hebben hierboven al gezien dat de Wiv 20xx op velerlei plaatsen aandacht besteedt aan de bescherming van persoonsgegevens. Daarbij is het evident dat technische systemen vrijwel altijd meer kunnen dan mag, al was het maar omdat

wat mag vaak per situatie verschilt. Daarenboven moeten systemen zo worden gebouwd dat zij – gezien de grote investeringen – redelijk toekomstbestendig zijn en verder ontwikkeld kunnen worden wanneer nieuwe technologie of andere omstandigheden dat nuttig, wenselijk of noodzakelijk maken. Precies omdat systemen meer mogelijk maken dan waartoe hun gebruikers bevoegd zijn, zijn de keuze van het ontwerp en de inrichting cruciaal voor de effectieve bescherming van de betrokken grondrechten.

Biedt het wetsontwerp in dit opzicht voldoende houvast? Verwijzingen naar technieken of technische aspecten komen 25 maal voor in het ontwerp, maar die zien in bijna alle gevallen op technische maatregelingen die het uitoefenen van bevoegdheden mogelijk maken en zelden op technische maatregelingen die het uitoefenen van bevoegdheden aan waarborgen binden. De veelheid van bepalingen die spreken van technische maatregelen waarmee inbreuken kunnen worden gemaakt staat in schril contrast tot het aantal bepalingen dat eisen stelt aan het ontwerp en de inrichting van de desbetreffende technische systemen. Op indirecte wijze stelt artikel 28 lid 7 eisen aan het ontwerp van een databank: ‘Bij algemene maatregel van bestuur worden in ieder geval regels gesteld voor het verwerken van DNA-profielen, waaronder begrepen de inrichting, het beheer en de toegang tot deze gegevens, en celmateriaal.’ Een vergelijkbare bepaling vinden we in artikel 82 lid 2, dat rechtstreekse automatische doorgifte van gegevens van politie en justitie naar de diensten regelt: ‘Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld met betrekking tot de te treffen technische en organisatorische maatregelen.’ In dat laatste geval is niet duidelijk of het hier gaat om beschermende maatregelen; in het eerste geval geeft de wet te weinig richting aan de in de AMvB neer te leggen normering. In artikel 21 wordt vereist dat wordt zorggedragen voor ‘de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking.’ Dit is echter qua reikwijdte beperkt tot de beveiliging van gegevens; het gaat niet om andere beginselen van gegevensverwerking, en bovendien is de bepaling in zeer algemene termen geformuleerd zonder enige concrete houvast. Feitelijk is de benadering – zowel in de huidige praktijk als in het wetsontwerp – er een van organisatorische maatregelen. Uit onze gesprekken met de diensten blijkt dat veel afbakeningen en *checks and balances* intern geregeld zijn in het proces.

Wij menen dat de consequenties van het ontwerp, de inrichting en het afstellen van de te gebruiken technische systemen te groot zijn om op interne organisatorische maatregelen te vertrouwen en verder in de wet met enkele – zeer algemeen geformuleerde en maar beperkt van toepassing zijnde – bepalingen af te doen. De bij de diensten in gebruik zijnde, en in de toekomst nog op te zetten, technische systemen vragen vanwege de geautomatiseerde verwerking van zeer grote hoeveelheden data om specifieke, ingebouwde waarborgen, die niet alleen organisatorisch maar ook technisch zijn geborgd. Wij herhalen in dat licht dat ook bij gerichte interceptie, het hacken van computersystemen, geautomatiseerde doorgifte door derden en geautomatiseerde OSINT enorme hoeveelheden data verzameld mogen worden, waarbij het merendeel van die data niet alleen irrelevant zal zijn maar ook ernstige en frequente inbreuken op privacy en gegevensbescherming mogelijk maakt van non-targets.

Daarbij moet worden bedacht dat het opzetten van dit soort systemen door inlichtingen- en veiligheidsdiensten een wezenlijk risico met zich meebrengt van

misbruik door toekomstige regeringen of bezettende machten die het met de mensenrechten minder nauw nemen en die permanente heimelijke grootschalige surveillance gaan doorvoeren, gericht op de bevolking als geheel of op bepaalde minderheden in het bijzonder. Weliswaar is de kans op dergelijk toekomstig machtsmisbruik klein, maar de schade ervan kan enorm zijn, wat betekent dat het risico (= kans vermenigvuldigd met schade) niet te verwaarlozen is. Daarom moet bij het toekennen en inperken van bevoegdheden, en juist ook bij het stellen van eisen aan de technische systemen die de uitoefening van zulke bevoegdheden mogelijk maken, er rekening mee worden gehouden dat de waarborgfunctie van de rechtsstaat ook moet functioneren met het oog op toekomstig machtsmisbruik. De technische systemen moeten dus zodanig worden gebouwd dat ze in dergelijke gevallen zo min mogelijk schade kunnen berokkenen aan de individuele vrijheid.

## 10.2 Een bepaling over gegevensbescherming *by design* en *by default*

Gezien de rechtsstatelijke eis dat het toekennen van bevoegdheden zo moet gebeuren dat zij daarmee tegelijk zijn ingeperkt schiet het huidige ontwerp op dit punt tekort. Het verschil tussen het uitoefenen van macht enerzijds en het uitoefenen van bevoegdheden anderzijds steekt precies in het feit dat een wettelijke bevoegdheid feitelijke macht zowel legitimeert als inperkt. PbD en DPbD zijn gebaseerd op een vergelijkbare dubbelslag: bij het toekennen van de bevoegdheid om door de inzet van specifieke technologie inbreuken te maken op grondrechten moet worden vereist dat deze specifieke technologie zo is ontworpen dat de inbreuken uitsluitend plaatsvinden als zij noodzakelijk zijn in een democratische samenleving en – indien dat het geval is – dat de inbreuken niet groter zijn dan noodzakelijk.

Het verdient daarom sterk aanbeveling om een bepaling in het wetsontwerp op te nemen dat gegevensbescherming *by design* en *by default* verplicht stelt. Een enigszins aangepaste, op de context van de Wiv 20xx toegesneden, versie van de desbetreffende bepaling in de Algemene verordening gegevensbescherming (art. 23) kan daartoe volstaan.[137] Een dergelijke bepaling heeft grote meerwaarde boven artikel 21, omdat artikel 21 alleen het beveiligingsbeginsel codificeert, maar niet de andere beginselen van gegevensbescherming. Deze bepaling zou daarmee in brede zin eisen stellen (1) bij de aanbesteding, ten aanzien van het ontwerp van het systeem, en (2) bij de uitvoering van de desbetreffende overeenkomst, ten aanzien van de inrichting van het systeem. Die eisen zullen bijvoorbeeld gericht zijn op het

[137] De tekst van artikel 23 Avg, in de compromisversie van 15 december 2015 (15039/15), luidt:
'*Data protection by design and by default*
1. Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing**,** the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of individuals.
(…)'

beperken van grootschalige inbreuken op de privacy van een veelheid van burgers waarvan de meesten geen target zijn. Daarnaast zullen de eisen de transparantie van de systemen betreffen, zodat snel en zoveel mogelijk langs automatische weg kan worden gedetecteerd of, hoe vaak, wanneer, hoe en door wie gebruik wordt gemaakt van het systeem. Dit is van groot belang voor de toezichthouder.

Ook heeft het opnemen van een dergelijke bepaling meerwaarde vanuit wetssystematisch oogpunt, omdat het de CTIVD in de gelegenheid stelt om de inrichting van systemen en de standaardinstellingen te beoordelen op rechtmatigheid. Zonder wettelijke bepaling heeft de CTIVD immers geen grondslag om oordelen te geven over systemen als zodanig, alleen over het gebruik daarvan. Vanwege het grote belang van de inrichting van systemen en de standaardinstellingen, is een rechtmatigheidstoets hierop een belangrijke aanvulling op het stelsel van waarborgen rond het toezicht.

## 10.3 Uitwerking

Om enige handen en voeten te geven aan hoe een vereiste van gegevensbescherming *by design* en *by default* verder vorm kan krijgen, bijvoorbeeld in specifieke onderdelen van het desbetreffende wetsartikel of in onderliggende regelgeving, geven wij hier een handreiking van hoe dit vereiste nader uitgewerkt zou kunnen worden, in de volgende drie vormen van DPbD.

*Less is more*
In alle gevallen zou de wet moeten voorschrijven dat (1) bij iedere verwerking de beginselen worden doorgevoerd van ‘select before you collect’ (dus geen ongerichte inzet van een bevoegdheid), ‘select while you collect’ (dus een onderzoeksplicht om irrelevante gegevens direct uit te filteren) en ‘select after you collect’ (beperking van gebruik tot doel-relevante gegevens en vernietiging zodra het doel is bereikt). Dat betekent dat in overeenstemming met de noodzakelijkheidsvereisten permanent verantwoording wordt afgelegd voor opslag en vernietiging van gegevens, ook *binnen* de maximaal mogelijke bewaartermijnen.

*Requirements engineering*
Bij de aanschaf en de inrichting van de technische systemen die onderzoek aan gegevensstromen en gegevenssets mogelijk maken, moeten de juridische voorwaarden waaraan de uitoefening van bevoegdheden moet voldoen, worden omgezet in technische specificaties. Binnen de computerwetenschappen bestaat ‘requirements engineering’ als zelfstandige sub-discipline, die hier buitengewoon relevant is. Het gaat daarbij om het formuleren van de eisen waaraan een systeem moet voldoen in termen van de eindgebruiker van het systeem. Bij het ontwerp van het systeem worden die vereisten dan weer omgezet in technische specificaties.

Wij menen dat in de Wiv 20xx moet worden opgenomen (1) een wettelijke verplichting om bij de aanbesteding specifiek te letten op de mate waarin het ontwerp van systemen grotere inbreuken toestaan dan noodzakelijk, en (2) een wettelijke verplichting om bij de inrichting van systemen de standaardinstellingen zo vast te stellen dat de inbreuk zo klein mogelijk is en nooit groter dan noodzakelijk. Bij dergelijke standaardinstellingen kunnen we denken aan het vergrendelen van onderdelen van een systeem, het pseudonymiseren van datastromen, het automatisch verwijderen, vernietigen of versleuteld archiveren van datasets, het

loggen van bewerkingen of het instellen van signaleringen wanneer een bepaalde frequentie, termijn of verhouding wordt overschreven.

*Softwareverificatie en controleerbaarheid*
Ten slotte is het zaak dat de toezichthouder haar wettelijke taak naar behoren kan uitoefenen door bij de rechtmatigheidstoets expliciet te onderzoeken of bij de inrichting van de systemen is voldaan aan de beginselen van gegevensbescherming, waaronder dataminimalisatie, doelbinding en noodzakelijkheid, en of de standaardinstellingen voldoen aan de eis van gegevensbescherming *by default*. Dit kan alleen wanneer de systemen zo zijn ontworpen dat zij zoveel mogelijk op geautomatiseerde wijze transparantie bieden over de verwerking (verzameling, analyse en toepassing) die heeft plaatsgevonden. Dit veronderstelt bovendien dat met enige regelmaat gebruik wordt gemaakt van softwareverificatie, dat wil zeggen dat ter zake kundige experts onderzoeken of de programmatuur doet wat de diensten menen dat deze doet, en of de instellingen kunnen worden aangepast om met minder dataverwerking hetzelfde doel te bereiken.

# 11 Conclusies en aanbevelingen

## 11.1 Conclusies

Het wetsontwerp voor de Wiv 20xx is in diverse opzichten een geslaagde poging om de Wiv 2002 te actualiseren. Er ligt een uitgebreid wetsvoorstel voor dat over het algemeen goed in elkaar zit, waarbij op veel plaatsen duidelijk aandacht is besteed aan het stellen van grenzen aan wat de inlichtingen- en veiligheidsdiensten, die uit de aard van hun werk ruime bevoegdheden nodig hebben, mogen doen. In de Memorie van Toelichting wordt vaak veel werk gemaakt van het uitleggen van keuzes en beargumenteren waarom deze verenigbaar (zouden) zijn met het recht op privacybescherming.

Het wetsontwerp is echter niet in alle opzichten geslaagd. Vanuit de kritische functie die een Privacy Impact Assessment heeft om de risico's van een wetsvoorstel in kaart te brengen, hebben wij ons in dit rapport niet gericht op wat goed is, maar op wat beter kan en beter moet, vanuit het oogpunt van een adequate privacybescherming. Een adequate privacybescherming betekent niet dat de diensten belemmerd moeten worden in hun taakuitoefening; het betekent dat de taakuitoefening moet worden gekanaliseerd en gelegitimeerd. Inbreuken op de privacy zijn toegestaan, als dat nodig is in een democratische samenleving.

De diensten hebben inherent ruime bevoegdheden nodig, omdat sommige bedreigingen van de nationale veiligheid dermate ingrijpend zijn dat vergaande maatregelen getroffen moeten kunnen worden. Ruime bevoegdheden moeten echter niet in alle gevallen kunnen worden ingezet; daarvoor is maatwerk nodig, dat in elke concrete situatie het belang van ingrijpen afweegt tegen de nadelen van ingrijpen, waaronder de met het ingrijpen gemoeide privacyinbreuken. Voor dat maatwerk is een normeringskader nodig, dat de inzet van in potentie zeer ruime bevoegdheden kanaliseert in de concrete gevallen waarin ingrijpen door de diensten nodig wordt gevonden.

Hoewel het wetsontwerp een goede aanzet biedt voor het normeringskader, schiet het op veel plaatsen tekort. Privacyrisico's worden bij behoorlijk veel onderdelen onvoldoende onderkend, en de voorgestelde waarborgen zijn vaak niet voldoende om de privacyrisico's af te dekken. De privacyrisico's die ontstaan bij veel van de voorgestelde bevoegdheden zijn groot. De inzet van een concrete bevoegdheid kan grote gevolgen hebben voor iemands leven. Privacyrisico's ontstaan onder andere doordat er fouten kunnen worden gemaakt in de uitoefening van bevoegdheden of in de verwerking of interpretatie van gegevens; persoonsgegevens kunnen worden gehackt of gelekt, of verstrekt aan derden met verlies aan controle over wat er vervolgens met de gegevens gebeurt; gegevens kunnen voor andere doelen worden hergebruikt, en door geautomatiseerde analyses of hergebruik buiten hun oorspronkelijke context terechtkomen, waardoor het risico op interpretatiefouten toeneemt. Ook kunnen bevoegdheden voor andere doelen of in andere contexten of op andere manieren worden toegepast dan voorzien is bij de formulering ervan; diensten kunnen de grenzen van bevoegdheden opzoeken en experimenteren in grijze gebieden waar de wet onvoldoende houvast geeft; en de neiging tot codificatie van bestaande praktijken in (donker)grijze gebieden leidt tot een neerwaartse spiraal van langzame maar gestage uitkleding van

privacybescherming. Daarnaast ontstaan ook privacyrisico's waar natuurlijke drempels wegvallen (zoals benodigde menskracht, financiën, fysieke nabijheid) door het automatiseren van processen, wat gefaciliteerd wordt door de nog steeds toenemende digitalisering, vernetwerking en mogelijkheden van geautomatiseerde data-analyse.

Het feit dat diverse van deze privacyrisico's onvoldoende worden onderkend, heeft mede te maken met een aantal onjuiste aannames die, meer of minder expliciet, aan het wetsontwerp ten grondslag liggen. Ten eerste is er de aanname dat het zonder meer goed is om bevoegdheden technologie-onafhankelijk op te schrijven. De keuze om zo technologieneutraal mogelijk te zijn is begrijpelijk (je wilt niet dat een wet bij elke technische vernieuwing moet worden aangepast), maar heeft belangrijke nadelen. Het leidt tot ruime en algemeen omschreven bevoegdheden, die daarmee dreigen overinclusief te worden, omdat ze vele mogelijke technologische toepassingen in de toekomst kunnen omvatten. Toekomstige toepassingen kunnen materieel een aanzienlijk grotere, dan wel kwalitatief andere, inbreuk op de privacy maken dan momenteel het geval is. Het uitgangspunt moet daarom niet zijn dat bevoegdheden zo technologie-neutraal mogelijk moeten worden geformuleerd, maar dat een balans moet worden getroffen tussen technologie-onafhankelijkheid en rechtszekerheid: technologie-onafhankelijk waar dat kan, maar niet als dat leidt tot bepalingen waarvan de reikwijdte niet is te overzien.

Ten tweede hanteert het wetsontwerp de traditionele aanname dat verwerking van verkeersgegevens (metadata) minder ingrijpend is dan kennisneming van de inhoud van communicatie. Die aanname is achterhaald: metadata kunnen een bijzonder scherp beeld geven van iemands persoonlijke levenssfeer, en zijn inmiddels regelmatig belangrijker en veelzeggender als informatiebron dan communicatie-inhoud.

Ten derde gaat het wetsontwerp ervan uit dat kabelgebonden interceptie een functioneel equivalent is van draadloze interceptie. Dat is niet het geval: kabelgebonden communicatie kent van oudsher een hogere privacyverwachting dan draadloze communicatie, en dat is nog steeds zo; het gaat daarom om principieel verschillende typen interceptie (par. 8.2.2).
Ten vierde hanteert het wetsontwerp de aanname dat welbekende, veelal 20$^{e}$-eeuwse technologieën als verrekijkers en fotocamera's nog steeds de belangrijkste technische hulpmiddelen zijn voor de diensten. Het wetsontwerp lijkt in veel opzichten te zijn gebaseerd op bekende en vaak oudere technologie en daarmee gepaard gaande privacyinbreuken. Dat komt vooral naar voren in de toelichting, waar regelmatig oude technologie wordt genoemd (zoals verrekijkers) maar nieuwe technologie (zoals drones) maar sporadisch in beeld komt. Hoewel dat deels een gebrek in de toelichting betreft, heeft het onmiskenbaar ook zijn weerslag op de voorgestelde wettelijke bepalingen: wanneer men met de bril van oude en huidige technologie een bevoegdheid bekijkt, schat men de privacyrisico's anders in dan wanneer de – technologie-onafhankelijk geformuleerde en dus toekomstbestendig bedoelde – bevoegdheid bekeken wordt door de bril van toekomstige technologie. Een wetsvoorstel dat, naar men mag aannemen, zo'n 10-20 jaar mee moet, kan er niet omheen om vooruit te kijken en rekening te houden met de technologische toepassingen die men nu veelal kan zien aankomen. Zo moeten bijvoorbeeld het Internet der Dingen, Big Data Analytics, machinaal leren, drones en gezichtsherkenning nadrukkelijk worden betrokken bij de beoordeling van de

uitwerking die bevoegdheden op de privacy in het decennium na inwerkingtreding van de wet zullen hebben, en de waarborgen moeten daar navenant op worden afgestemd.

Naast deze onjuiste aannames, kent het wetsontwerp enkele andere valkuilen die privacyrisico's opleveren. De wet is complex, met vaak ingewikkelde constructies, zowel op zinsniveau als op artikelniveau. Sommige constructies, zoals de driestappenbenadering bij bulkinterceptie (par. 8.3) werken misschien op papier maar zijn in de praktijk veel diffuser. Het normeringskader is verspreid over verschillende afdelingen en onderdelen daarvan zijn soms wel en soms niet van toepassing op activiteiten van de diensten (hfd. 4). De vele kruisverwijzingen maken daarnaast de reikwijdte van bepalingen moeilijk te overzien, zeker waar spaghetticonstructies ontstaan waarbij slierten uit een ingewikkelde kluwen ontward moeten worden (par. 2.3.3). Al met al is het een wetsvoorstel dat alleen door gespecialiseerde juristen te bevatten valt. Dat gaat niet alleen ten koste van de kenbaarheid van de wet voor de burger, maar bergt ook een belangrijk risico in zich dat in het wetgevingstraject de reikwijdte van de voorstellen niet goed ingeschat wordt. Dit legt een zware hypotheek op de Memorie van Toelichting, die hier aanzienlijk meer houvast zal moeten bieden dan ze nu doet.

Mede als gevolg van de gehanteerde aannames en de aanwezige valkuilen zijn de waarborgen, zoals wij in dit rapport hebben laten zien, niet altijd voldoende om de privacyrisico's op te vangen. Op diverse punten moeten de waarborgen – soms ingrijpend – worden verzwaard. Op enkele punten zijn de privacyrisico's, ook als de waarborgen zouden worden verzwaard, onaanvaardbaar en moeten onderdelen van het wetsvoorstel achterwege worden gelaten. In de volgende paragraaf werken we dat verder uit.

Naast aanpassingen in het wetsvoorstel, betekenen de aannames en valkuilen ook dat de Memorie van Toelichting scherper, uitgebreider en met meer visie moet uitleggen wat het wetsvoorstel inhoudt. Er is bij de consultatieversie gekozen voor een relatief sobere toelichting. 218 pagina's lijkt omvangrijk, maar is in verhouding tot de wet niet overdreven lang – eerder relatief kort. Het gaat met 150 artikelen om een omvangrijke wet, die een compleet domein – nationale veiligheid – reguleert en die, als aangegeven, complex en moeilijk te overzien is. Op veel punten, zoals we in voorgaande hoofdstukken hebben aangegeven, moet de toelichting helderder, specifieker of uitgebreider. Te vaak worden voor de hand liggende, zelfs simplistische, voorbeelden gegeven, niet alleen met betrekking tot technologische toepassingen maar ook bijvoorbeeld bij de aanduiding van wat 'nationale veiligheid' inhoudt. Evidente voorbeelden (nationale veiligheid is wel terrorismebestrijding maar geen opsporing van strafbare feiten) geven geen houvast om de wet toe te passen op moeilijke gevallen; daarvoor is juist een bespreking nodig van het grijze gebied tussen wat evident wel en evident niet onder de wet valt, met bij voorkeur een materieel criterium of richtlijn hoe moeilijke gevallen kunnen worden geïnterpreteerd. De keuze voor zoveel mogelijk technologieonafhankelijkheid legt een grote verantwoordelijkheid bij de toelichting, die de burger de noodzakelijke uitleg moet geven wat de diensten kunnen en mogen doen, ook – en vooral – met gebruikmaking van 21$^{e}$-eeuwse technologieën. Dit vraagt ook om visie: hoe ver vindt de wetgever dat de diensten mogen gaan in het gebruiken van nieuwe technologieën die steeds meer en steeds makkelijker inzicht geven in het persoonlijke leven van individuen? Als het niet de bedoeling is om ongebreidelde massale *surveillance* van burgers toe te staan, moeten nu piketpalen worden

geslagen in de witte vlekken die ontstaan bij zeer ruim en technologieonafhankelijk geformuleerde bevoegdheden.

Een scherpere en uitgebreidere toelichting hoeft overigens niet per se tot een veel langere tekst te leiden. Evidente voorbeelden kunnen vervangen worden door sprekender voorbeelden, criteria kunnen compact worden geformuleerd en visies kunnen kort maar krachtig worden neergezet. Bovendien bevat de huidige toelichting op vrij veel plaatsen overbodige tekst, waar in licht andere, of soms letterlijk dezelfde, bewoordingen wordt aangegeven wat in het wetsartikel staat. Dat is niet toelichten maar herhalen, en kan beter achterwege blijven, ten faveure van teksten die daadwerkelijk iets toevoegen aan het begrip van de wettekst. En als betere uitleg leidt tot een langere tekst, dan hoeft dat – mits de tekst helder en informatief is – niet ten koste te gaan van begrijpelijkheid of overzichtelijkheid. Ook burgers, juristen en parlementariërs staan immers hulpmiddelen tot data-analyse ter beschikking, zoals zoekfuncties om snel een relevante passage te vinden. Niet soberheid maar duidelijkheid en houvast moeten het uitgangspunt zijn van de Memorie van Toelichting.

Onze analyse geeft aanleiding tot reflectie en heroverweging op veel punten. Sommige punten zijn makkelijk te adresseren; andere vergen substantiële aandacht en tijd. Wil de Wiv 20xx daadwerkelijk een goede balans vinden tussen een effectieve bescherming van de nationale veiligheid en de bescherming van de persoonlijke levenssfeer van burgers (MvT, p. 188), dan is nog het nodige werk te verzetten. Het is van wezenlijk belang voor de burger dat dat werk ook daadwerkelijk verzet wordt: een onbalans tussen effectiviteit en rechtsbescherming leidt tot minder kwaliteit van leven van burgers, die niet alleen behoefte hebben aan (nationale) veiligheid, maar ook behoefte hebben aan mogelijkheden om onbevangen zichzelf te kunnen zijn en zonder inmenging van de overheid hun privéleven vorm te kunnen geven.

Essentieel is dan ook dat de wetgever niet overhaast te werk gaat. Aanslagen als die in Parijs in november 2015 mogen geen aanleiding zijn om een wetsvoorstel versneld in te dienen of gehaast te behandelen. Dat gaat ten koste van de aandacht en het debat die nodig zijn om zorgvuldige wetgeving tot stand te brengen. Snelle wetgeving lijkt misschien daadkrachtig, maar is voor een wet die een zo essentieel domein als de nationale veiligheid reguleert en die jaren mee moet, uiterst riskant – ook voor de nationale veiligheid. Lacunes, onzorgvuldigheden en onvoorziene neveneffecten, waarvan we in dit rapport de nodige voorbeelden hebben gegeven, komen vroeg of laat als een boemerang terug, bijvoorbeeld als de Eerste Kamer of de Nederlandse of Europese rechter oordeelt dat de wet onvoldoende rechtsbescherming, waaronder privacybescherming, kent. Naast de concrete aanbevelingen die wij hieronder doen, is daarom onze eerste en misschien wel voornaamste aanbeveling om de impact van het wetsvoorstel op de privacy, zoals wij die in dit rapport hebben geanalyseerd, serieus te nemen.

## 11.2 Aanbevelingen

In deze paragraaf zetten wij de aanbevelingen op een rij die doorheen het rapport staan vermeld, volgend uit de analyses en conclusies op de diverse onderdelen. Wij doen dit compact, onder verwijzing naar de argumentatie in de desbetreffende paragrafen. De aanbevelingen moeten dan ook in samenhang met de analyse en argumentatie aldaar worden gelezen. Gegeven het belang van privacybescherming

van burgers en goed functionerende diensten in een democratische samenleving, hebben we de aanbevelingen scherp geformuleerd. Het doel van deze PIA is immers om de privacyrisico's zo duidelijk mogelijk voor het voetlicht te brengen, en op die manier bij te dragen aan de zorgvuldige totstandkoming van een Wiv 20xx waarin alle privacyrisico's zo goed mogelijk, met inachtneming van het belang dat de diensten de komende jaren effectief én legitiem kunnen functioneren, zijn geadresseerd.

**Algemene aanbeveling**

1. De structuur van de wet kan helderder en simpeler. De diverse bepalingen die de activiteiten van de diensten in algemene zin normeren (art. 17-21, 23-24, 43-45, 57) kunnen beter bij elkaar worden geplaatst in één normeringskader (hfd. 4). Het onderscheid tussen de 'algemene' bevoegdheid en de 'bijzondere' bevoegdheden kan komen te vervallen; alle bevoegdheden gaan gepaard met substantiële privacyrisico's en moeten in elk geval onder hetzelfde normeringskader vallen (par.5.1).

**Ontbrekende bepalingen**

Sommige privacyrisico's worden ten onrechte niet onderkend in het wetsvoorstel. Deze kunnen worden geadresseerd door bepalingen op te nemen die de taakuitoefening op deze punten normeren.

2. Het vergaren en vastleggen van informatie uit open bronnen (OSINT) maakt inbreuk op de privacy, een inbreuk die ingrijpend kan zijn bij stelselmatige toepassing. Het wetsvoorstel zou een zelfstandige grondslag moeten bevatten voor het stelselmatig vastleggen van gegevens uit open bronnen, in de vorm van een bijzondere bevoegdheid die onder het algemene normeringskader valt. Bij vergaande (langdurige of met gebruik van nepprofielen) vormen zijn zwaardere eisen nodig aan het toestemmingsniveau (par. 5.2). Het monitoren van sociale media zou niet onder observatie moeten vallen maar kan beter in een dergelijke OSINT-bevoegdheid worden geïntegreerd (par. 7.1.5).
3. Er zou een bepaling opgenomen moeten worden over gegevensbescherming *by design* en *by default*. Bij de aanbesteding en inrichting van systemen moet privacybescherming waar mogelijk worden vertaald in technische eisen aan het ontwerp, de gebruiks(on)mogelijkheden, de standaardinstellingen en de transparantie van systemen. Privacy per ontwerp verkleint privacyrisico's, versterkt de interne privacycultuur, en biedt de toezichthouder een grondslag om een rechtmatigheidstoets uit te voeren op de privacy(on)vriendelijkheid van de keuzes die de diensten in hun systeemontwerpen en operationele praktijken maken (hfd. 10).

**Onaanvaardbare privacyrisico's**

Bij de volgende onderdelen zijn de privacyrisico's onaanvaardbaar groot. De noodzaak ervan is niet aangetoond en is onzes inziens ook niet aannemelijk te maken, ook niet als er zwaardere waarborgen zouden worden voorgesteld.

4. Er moet geen DNA-databank bij de diensten worden opgezet. Er worden geen klemmende redenen aangevoerd die de privacyrisico's van een eigen DNA-databank kunnen rechtvaardigen (par. 6.6). Mocht er een 'pressing social need' zijn om toekomstige zelfmoordterroristen na een zelfmoordaanslag te kunnen identificeren en dit doel aantoonbaar niet met andere middelen kunnen worden bereikt (wat wij voorshands niet inzien), dan moet het voorstel om DNA-profielen op te slaan beperkt worden tot deze specifieke groep, met een

maximale bewaartermijn die proportioneel is voor het doel van opslag voor deze specifieke groep (par. 6.6).

5. Het binnendringen in computers van derden om bij de computer van een doelwit te kunnen komen, moet worden afgewezen. Het feit dat doelwitten van de diensten hun computers over het algemeen goed beveiligen kan nooit de privacyrisico's rechtvaardigen van het hacken van computers van onverdachte burgers in hun omgeving (par. 7.2.5).
6. De verplichting voor aanbieders van niet-openbare communicatie (zoals interne bedrijfsnetwerken) om zelf de kosten te dragen om hun systemen aftapbaar te maken, moet worden afgewezen. Het valt niet in te zien waarom spelregels die gelden voor spelers die zich welbewust op een bepaalde markt begeven (openbare telecommunicatie), van toepassing kunnen worden verklaard op spelers die niet op die markt actief zijn. Los van administratieve lastenverzwaring brengt dit onaanvaardbare privacyrisico's met zich mee (par. 8.1.3). Voor het technisch faciliteren van kabelgebonden bulkinterceptie door openbare telecomaanbieders is eerst een aanvullende impactanalyse nodig om te kunnen beoordelen of de voorgestelde kostenverdeling qua privacyrisico's aanvaardbaar is (par. 8.1.3).
7. De uitbreiding van de definitie van communicatieaanbieders moet zich niet uitstrekken tot diensten die externe opslag van gegevens aanbieden. Dergelijke diensten zijn een hedendaags functioneel equivalent van de traditionele opslag van privédocumenten (foto's, muziek, boeken, dagboeken en administratie) binnen de woning. Bevoegdheden tot (bulk)interceptie en gegevensbevraging zijn niet bedoeld om privédocumenten te vergaren die traditioneel onder de bescherming van het huisrecht vallen; in elk geval levert bulkinterceptie van dergelijke privédocumenten onaanvaardbare privacyrisico's op. De afdeling over onderzoek van communicatie moet beperkt blijven tot (cloud-) opslagdiensten die aangeboden worden *in het kader van communicatiefunctionaliteiten* en die daarmee *onlosmakelijk* zijn verbonden. Daaronder vallen wel webmaildiensten, maar niet de clouddiensten die mensen in staat stellen om hun eigen bestanden extern op te slaan voor eigen gebruik, ook niet als deze dienst wordt aangeboden in een pakket gezamenlijk met een webmaildienst (par. 8.1.1).
8. De verstrekking van ongeëvalueerde gegevens (dus gegevens die nog niet op relevantie zijn onderzocht) aan buitenlandse diensten is een aantasting van de essentie van het recht op privacy en voldoet niet aan het subsidiariteitsbeginsel. Indien een samenwerking met een buitenlandse dienst is overeengekomen, zouden gegevens niet ongeëvalueerd verstrekt mogen worden, maar zou de Nederlandse dienst, namens of gezamenlijk met de buitenlandse dienst, de gegevens zelf moeten analyseren met het oog op het doel waarvoor de buitenlandse dienst de gegevens verzoekt (par. 5.4.2).
9. Gegevens genoemd in artikel 55 lid 1 (verouderde of onbetrouwbare gegevens) zouden niet verstrekt mogen worden aan buitenlandse diensten (wat het wetsontwerp toelaat op basis van art. 77 lid 3 j$^{o}$ 55 lid 2). Het gaat immers om gegevens die hoogstwaarschijnlijk niet relevant zijn of waarvan de relevantie (vanwege de onbetrouwbaarheid) niet kan worden vastgesteld, en waarvan niet kan worden gecontroleerd op welke manier de buitenlandse dienst er gebruik van zal maken. Daarom zou artikel 55 lid 2 onder a integraal moeten komen te vervallen.

**Onaanvaardbare privacyrisico's, tenzij waarborgen ingrijpend worden versterkt**

Op de volgende onderdelen is een ingrijpende versterking van de waarborgen nodig, om de grote privacyrisico's te kunnen rechtvaardigen.

10. Toezicht moet niet alleen onafhankelijk maar ook effectief zijn. Het wetsontwerp beperkt een onafhankelijk bindend oordeel over rechtmatigheid tot situaties waarin een klacht is ingediend bij de CTIVD (en twee zeer specifieke onderdelen waar voorafgaande toestemming van de rechter nodig is). Voor een adequate afdekking van de met de bevoegdheden gepaard gaande grote privacyrisico's moet de wetgever nadrukkelijk overwegen de CTIVD in het algemeen bindend adviesrecht te geven, ook buiten de klachtbehandeling om (hfd. 9).
11. De 'algemene' bevoegdheid tot het opvragen van gegevens(bestanden) is in potentie even ingrijpend als, en soms aanzienlijk ingrijpender dan, de bijzondere bevoegdheden. Deze bevoegdheid moet op zijn minst aan hetzelfde algemene normeringskader als de bijzondere bevoegdheden zijn onderworpen (zie ook aanbeveling 1). In gevallen waarin uit de opgevraagde gegevens een indringend beeld van de persoonlijke levenssfeer kan ontstaan, moet de normering daarbovenop aanvullende eisen stellen. Voor geautomatiseerde toegang tot bestanden is ingrijpend zwaardere normering nodig qua toestemming, duur en omvang (par. 5.1.2, 5.1.3).
12. Het regime voor opslag en vernietiging van gegevens moet met aanzienlijk sterkere waarborgen worden omkleed.
    a. Bewaartermijnen moeten beter worden gemotiveerd, maar ook korter zijn dan voorgesteld (par. 4.6).
    b. Het wetsvoorstel zou een *algemene* bepaling moeten bevatten, vergelijkbaar met de onderzoeksplicht en bewaartermijn bij gerichte interceptie, die zekerstelt dat gegevens (ongeacht met welke bevoegdheid verkregen) zo spoedig mogelijk op relevantie worden onderzocht, en dat gegevens worden vernietigd zodra is vastgesteld dat deze niet relevant zijn (par. 4.6.2, 4.6.3). De term 'zo spoedig mogelijk' moet daarbij aansluiten op wat men daar in het algemene spraakgebruik onder verstaat, en dus niet 'binnen twaalf maanden' kunnen betekenen (par. 2.3.2).
    c. Het bewaren van verwijderde (maar nog niet vernietigde) gegevens levert een groot risico op function creep op. Voor specifiek wettelijk bepaalde uitzonderingsgronden waarbij verwijderde gegevens voor een ander doel nodig zijn (archiefplicht, inzageverzoek), zijn de privacyrisico's van bewaring van verwijderde gegevens aanvaardbaar. Het wetsvoorstel zou moeten bepalen dat, tenzij een van de specifieke uitzonderingsgronden van toepassing is, gegevens terstond worden *vernietigd* zodra blijkt dat ze niet relevant zijn, of wanneer de termijn voor onderzoek op relevantie is verstreken. Dat geldt zowel voor de specifieke bevoegdheden waarin aparte onderzoeksplichten met termijnen worden genoemd, als voor de algemene bepaling van artikel 57. Indien zich noodsituaties voordoen waarin verwijderde maar nog niet vernietigde gegevens essentieel blijken voor operationele doelen, zou daarvoor een aparte procedure, met onafhankelijke toestemming vooraf, moeten gelden (par. 4.6.4).
    d. Voor opslag van relevante gegevens moet een maximale bewaartermijn worden gesteld. Deze mag relatief lang zijn, maar niet onbepaald. De wet moet periodieke controle op relevantie in enige vorm vereisen, om te voorkomen dat gegevens veel langer dan nodig opgeslagen kunnen blijven. Denkbaar is een combinatie van integrale periodieke controle op relevantie

door daartoe aangewezen, gekwalificeerde medewerkers van de diensten, met steekproefsgewijze controles door de CTIVD. Wanneer bij controle wordt vastgesteld dat opslag niet meer noodzakelijk is, zouden de gegevens terstond moeten worden verwijderd en, als er geen van de specifieke uitzonderingsgronden voor bewaring van toepassing is, vernietigd (par. 4.6.5).

13. Nu de computer (pc, tablet, smartphone) een steeds centralere rol inneemt in het privéleven, als de toegangspoort tot de informatie en contacten waarmee mensen hun leven vormgeven, vormt het binnendringen in computers de zwaarst denkbare inbreuk op de privacy (par. 7.2.2). De bevoegdheid hiertoe moet dan ook met het zwaarst mogelijke toezicht worden omkleed. In gevallen waarin de overheid toegang kan krijgen tot alle informatie op computers, moet het beschermingsniveau *hoger* liggen dan de bescherming van huis of communicatie, gezien het feit dat computeronderzoek veel meer van het privéleven kan blootleggen dan een huiszoeking of telefoontap. Bij deze zwaarst denkbare inbreuk op de privacy achten wij voorafgaande toestemming van de rechtbank aangewezen om de privacyrisico's te kunnen rechtvaardigen. Ook zou de aanbeveling van de commissie-Dessens om onmiddellijke toetsing in te voeren tijdens de uitoefening van de bevoegdheid, hier moeten worden overgenomen (par. 7.2.4).
14. Het feit dat tegenwoordig communicatie vaker door kabels dan door de ether gaat, leidt niet tot een verandering in privacyverwachting: nog steeds is het zo dat iedereen een antenne in de lucht kan steken, maar niet iedereen zomaar kabels kan opgraven om afluisterapparatuur te plaatsen. De argumentatie om bij bulkinterceptie de niet-kabelgebonden communicatie gelijk te schakelen met kabelgebonden communicatie geeft zich onvoldoende rekenschap van dit normatieve verschil in privacyverwachting tussen draadloze en draadgebonden communicatie. Bulkinterceptie van kabelgebonden interceptie mag op normatief niveau dan ook niet gelijk gesteld worden met niet-kabelgebonden bulkinterceptie (par. 8.2.2). Dit betekent dat de regeling voor bulkinterceptie, nu deze ook van toepassing wordt op kabelgebonden communicatie, zwaarder genormeerd moet worden (par. 8.3.2). Het dynamische karakter van bulkinterceptie maakt het moeilijk om in de wettekst, en in het verzoek om toestemming vooraf en in de toestemming zelf, strakke grenzen te trekken. De toets op rechtmatigheid zal vooral ook *tijdens* het uitvoeringsproces doorlopend moeten worden uitgevoerd. Onmiddellijk toezicht door de CTIVD vormt hier dan ook een belangrijke, en moeilijk vervangbare, waarborg (par. 8.3.2).
15. De grote privacyrisico's van bulkinterceptie kunnen beter binnen enige perken worden gehouden door de door Jacobs voorgestelde tweefasenaanpak, dan door het voorgestelde papieren onderscheid in drie stappen, die in de praktijk diffuus zijn en snel door elkaar kunnen lopen. In de eerste fase wordt vluchtig, en dus niet systematisch-inhoudelijk, gekeken naar relevantie van gegevens; de vluchtige blik wordt direct en doorlopend uitgevoerd bij elke binnenkomst van gegevens, en irrelevante gegevens worden terstond verwijderd zodra is vastgesteld dat ze niet relevant zijn, volgens het principe 'select while you collect'. De tweede fase, van stelselmatigheid, richt zich op het inhoudelijke onderzoek van de aldus gefilterde en dus meer relevante gegevens (par. 8.3.2). Hierbij is aanscherping van het regime van onderzoek op relevantie, bewaartermijn en vernietigingsplicht van via bulkinterceptie vergaarde gegevens essentieel (par. 4.6, zie ook aanbeveling 12).

**Aanvaardbare privacyrisico's, mits de normering wordt verbeterd**

Bij de volgende onderdelen zijn verbeteringen nodig, hetzij in de waarborgen hetzij in de formulering of afbakening van bepalingen, om de privacyrisico's te rechtvaardigen.

16. Het huisrecht is van oudsher een van de belangrijkste hoekstenen van privacy, waarbij een sterke bescherming nodig is tegen elke bevoegdheid waarbij kennis wordt genomen van wat zich binnen een woning afspeelt. Het gaat er daarbij niet om of er fysiek wordt binnengetreden in de woning, maar of er kennis wordt genomen van het huiselijk leven. Bevoegdheden waarbij van buitenaf kennis wordt genomen van wat zich binnen een woning afspeelt, zoals observatie, direct afluisteren of het opvragen van gegevens die inzicht geven in wat zich binnen de woning afspeelt, zoals energieverbruiksgegevens, moeten gebonden worden aan dezelfde waarborgen als het betreden van woningen (par. 7.1.2).
17. Privacy in de publieke ruimte heeft meer dan voorheen juridische bescherming nodig. De ongewijzigde regeling van observatie (buiten de woning) doet geen recht aan de gewijzigde realiteit. De wetgever moet sterkere waarborgen overwegen, qua toestemmingsniveau of duur van uitvoering, voor observatie en registratie in de publieke ruimte, met name waar door combinatie van hulpmiddelen en/of langdurige observatie een cumulatief beeld kan ontstaan (door losse steentjes samen te voegen tot een mozaïek) van iemands privéleven (par. 7.1.3, 7.1.4).
18. De definitie van 'geautomatiseerd werk' (oftewel computersysteem) is zeer breed, en omvat meer dan de meeste burgers daaronder zullen begrijpen. De wetgever moet zich afvragen of het wel de bedoeling is dat de diensten kunnen binnendringen in alle apparaten die technisch onder de definitie vallen maar functioneel een andere rol vervullen dan het type computers (zoals pc's, laptops en smartphones) waarvoor deze bevoegdheid primair bedoeld is. De risico's van het hacken van apparaten in het Internet der Dingen, zoals slimme energiemeters, thermostaten en boordcomputers van auto's, zijn aanzienlijk, en het is sterk de vraag of het noodzakelijk is om dergelijke apparaten te kunnen hacken om gegevens te verzamelen die niet op een minder ingrijpende manier zouden kunnen worden verzameld (par. 7.2.3).
19. Aangezien verkeersgegevens (metadata) inmiddels evenveel (en soms meer) inzicht bieden in het privéleven als communicatie-inhoud, moet het toestemmingsvereiste voor het opvragen van verkeersgegevens op hetzelfde niveau liggen als voor interceptie van communicatie. Dat betekent dat toestemming van de minister nodig is, die niet kan worden gedelegeerd aan het diensthoofd (par. 8.1.5).
20. De verplichting voor communicatieaanbieders om bulkinterceptie te faciliteren levert privacyrisico's op. Het is de vraag of (ook kleine) aanbieders van (ook private) diensten voldoende vermogen en expertise hebben om adequate technische voorzieningen te treffen die bestand zijn tegen misbruik of hacken. Hier zou het wetsvoorstel moeten worden versterkt, om zeker te stellen dat bij het aanbrengen van technische voorzieningen om bulkinterceptie te faciliteren, geen achterdeuren of lekken ontstaan (par. 8.1.2).
21. De Memorie van Toelichting motiveert onvoldoende waarom voor gerichte interceptie van militair (ook kabelgebonden) communicatieverkeer geen toestemming nodig zou zijn. Met name als er sprake is van interceptie van militair verkeer over civiele kanalen, lijkt eerder toestemming op ten minste het niveau van het diensthoofd aangewezen, gezien de wezenlijke privacyrisico's die gemoeid zijn met kabelgebonden interceptie, ook als deze gericht is op

militair verkeer. Waar het niet-kabelgebonden communicatie betreft of waar de interceptie beperkt blijft tot communicatiekanalen die uitsluitend voor militaire doeleinden worden gebruikt, zou interceptie wel zonder toestemming moeten kunnen plaatsvinden (par. 8.2.2).

22. Bij de intensievere samenwerking tussen de diensten verdient het aanbeveling om, evenals een beoordeling op subsidiariteit en proportionaliteit, ook doelbinding expliciet te betrekken bij de afweging om gegevens te verstrekken aan de collega-dienst. Doelafwijkend gebruik door de collega-dienst vergt een nieuwe grondslag en daarom ook toestemming op ten minste hetzelfde niveau als de toestemming die nodig was voor het verkrijgen van de gegevens door de verstrekkende dienst (par. 3.2).
23. De bevoegdheid om aan buitenlandse diensten ondersteuning te vragen, waaronder inzet van bevoegdheden die de diensten zelf ook hebben, levert privacyrisico's op omdat het moeilijk te beoordelen is aan welke eisen buitenlandse diensten moeten voldoen bij de uitoefening van hun bevoegdheden. Het wetsontwerp en de toelichting geven zich hiervan onvoldoende rekenschap. De wetgever moet duidelijk maken hoe geborgd kan worden dat bij het verzamelen van gegevens door buitenlandse diensten op verzoek van de Nederlandse, vergelijkbare waarborgen en beperkingen in acht worden genomen als die gelden bij uitoefening van bevoegdheden in Nederland (par. 5.4.3).
24. Voor de volgende artikelen zijn specifieke verbeteringen aangewezen (zie de desbetreffende paragrafen voor het exacte verbetervoorstel).
    - Art. 17 lid 5: het verdient aanbeveling een aanzienlijk kortere bewaartermijn te hanteren voor gegevens over informanten, dan wel veel scherper de noodzaak te onderbouwen waarom de gegevens nog tot 30 jaar na dato beschikbaar zouden moeten blijven (par. 5.1.4).
    - Art. 25: het monitoren van sociale media zou apart geregeld moeten worden (par. 7.1.5, zie ook aanbeveling 0).
    - Art. 28: indien een DNA-profiel bij externe databanken (in Nederland of in het buitenland) wordt nagetrokken, moet worden gestipuleerd dat het profiel alleen mag worden gebruikt voor matching, en niet mag worden opgenomen in de externe databank (of anderszins door de derde worden gebruikt) (par. 6.4). Lid 5 zou moeten bepalen dat het celmateriaal zo spoedig mogelijk, doch uiterlijk binnen twee of vier weken, wordt vernietigd (par. 6.5).
    - Art. 42: voor het plaatsen van apparatuur in de woning is ministeriële toestemming nodig (par. 7.1.7).
    - Art. 47: gezien de grote impact die geautomatiseerde data-analyse kan hebben, die vergelijkbaar is met de impact van metadata-analyse (art. 35), zou deze bevoegdheid op hetzelfde niveau als metadata-analyse moeten worden genormeerd, wat betekent ministeriële toestemming vooraf (par. 5.3.2).
    - Art. 77: de toestemmingeis van art. 77 leden 5 en 6 moet ook van toepassing worden verklaard op de gegevensverstrekking van lid 1 (par. 5.4.2). Bij ondersteuning op verzoek van buitenlandse diensten moeten ook de waarborgen vermeld in artikelen 51, 55 en 56, van overeenkomstige toepassing zijn; art. 77 lid 3 zou dan ook niet alleen naar lid 1 maar ook naar lid 4 moeten verwijzen (par. 5.4.2).

**<u>Wenselijke aanvullingen of aanscherpingen van bepalingen</u>**

25. Uit de toelichting en wetssystematiek blijkt onvoldoende dat, ondanks de expliciete vermelding van de beginselen van subsidiariteit en proportionaliteit in

artikel 43 (met betrekking tot bijzondere bevoegdheden), deze beginselen ook besloten liggen in artikel 17 lid 2, door het begrip ‘noodzakelijk’, en dus van toepassing zijn op alle vormen van gegevensverwerking door de diensten. De toelichting moet op dit punt worden verhelderd (par. 4.1.3).

26. In de volgende artikelen zijn aanvullingen of aanscherpingen wenselijk in de formulering (zie de desbetreffende paragrafen voor het exacte verbetervoorstel).
    - Art. 17 lid 4: deze bepaling zou ook een betrouwbaarheids- of bronaanduiding van de programmatuur waarmee gegevensverzamelingen worden geanalyseerd moeten vereisen (par. 4.1.4).
    - Art. 18 lid 3: de opsomming van gevoelige persoonsgegevens zou ook lidmaatschap van een vakvereniging moeten vermelden (par. 4.2.2).
    - Art. 28 lid 3 kan beter ‘een zo nauwkeurig mogelijke aanduiding van de persoon’ eisen dan ‘gegevens betreffende de identiteit van de persoon’ (par. 6.2).
    - Art. 30 zou, als waarborg tegen al te omvangrijke semi-continue monitoring, in lid 4 moeten bepalen dat het verzoek om toestemming ook een specificatie bevat van de beoogde reikwijdte van het verkennen (als bedoeld in het eerste lid, onder a) (par. 7.2.6).
    - Art. 38 lid 1 bevat een nodeloos ingewikkelde omschrijving van het object; men kan beter ‘inhoud van telecommunicatie’ gebruiken, of anders aansluiten bij de formulering die in de strafvordering voor opgeslagen communicatie wordt gebruikt (par. 8.1.4).
    - Art. 47 lid 3 zou qua formulering moeten worden aangescherpt, zodat duidelijker is dat maatregelen niet mogen worden getroffen of bevorderd louter gebaseerd op één of meer automatische verwerkingen. Daarnaast zou in de toelichting meer uitgewerkt moeten worden waaruit de benodigde menselijke tussenkomst bij geautomatiseerde beslissingen zou moeten bestaan (par. 5.3.3).
    - Art. 78 lid 5 is fout geformuleerd. Art. 78 lid 3 zou moeten verwijzen naar alle van toepassing zijnde waarborgen, niet alleen naar de waarborgen die vervat zijn in paragrafen 3.2.2, 4.2 en 4.3 (par. 5.4.3).

**Niet-wettelijke maatregelen**

De nadruk in dit rapport ligt op de wettelijke regeling van de Wiv 20xx, het gaat immers om een PIA op het wetsvoorstel. Ter ondersteuning van de wettelijke waarborgen, achten wij een aantal niet-wettelijke maatregelen aangewezen die nodig zijn voor een goede balans tussen effectiviteit en rechtsbescherming zoals de wet die probeert te vinden. Deze maatregelen hoeven als zodanig niet per se wettelijk te worden verankerd, maar zouden wel onderdeel moeten zijn van de beleidsvorming aanpalend aan de totstandkoming van de Wiv 20xx.

27. Vanwege de uitbreidingen in de wet en de versterking van het toezicht, is versterking van de capaciteit van de CTIVD nodig. Bij die versterking, die op zich al wordt voorzien, moet vooral ook worden meegenomen dat adequate technische inbreng nodig is. Er moet worden geïnvesteerd in technische expertise binnen de CTIVD, die veel verder moet gaan dan het inhuren van experts. Integratie tussen technische en juridische perspectieven is nodig om een adequate rechtmatigheidstoets te kunnen uitoefenen. Dergelijke integratie kan alleen worden bereikt als technische en juridische deskundigen op langdurige basis samenwerken en op de werkvloer steeds in elkaars nabijheid zijn (hfd. 9).

28. Niet alleen de CTIVD heeft meer capaciteit nodig. Aangezien op diverse onderdelen de toestemming vooraf is verzwaard, en deze verzwaring op basis van onze aanbevelingen nog verder moet worden doorgevoerd, is ook voldoende ondersteuning nodig van de diensthoofden en de ministers, om zorgvuldige afwegingen op deze niveaus te kunnen waarborgen. Voorkomen moet worden dat toestemmingsverzoeken, vanwege grote hoeveelheden of onvoldoende kritische beschouwing van de inhoud, automatisch afgestempeld worden. Dat vergt niet alleen versterking van de capaciteit in de ambtelijke ondersteuning van de diensthoofden en ministers, maar ook versterking van de expertise en het kritisch vermogen van degenen die verantwoordelijk zijn voor de afhandeling van toestemmingsverzoeken. Deze personen zouden niet als verlengstuk van de diensten moeten fungeren bij de afhandeling van verzoeken, maar een opbouwend-kritische en onafhankelijke adviesfunctie moeten hebben. Hun positie zou wellicht gemodelleerd kunnen worden, qua onafhankelijkheid en rechtspositie, naar die van functionarissen voor de gegevensbescherming.
29. Tot slot is het van wezenlijk belang dat binnen de diensten zelf privacybewustzijn aanwezig is en een continue, kritische zelfreflectie plaatsvindt op de taakopvatting en taakuitoefening. Ook met stevige wettelijke normering van, en onafhankelijk en effectief toezicht op, de taakuitoefening, komt uiteindelijk veel aan op de keuzes die de diensten zelf maken in hun werk. Voor een adequate balans tussen effectiviteit en privacybescherming, die ook doorlopend gekalibreerd zal moeten worden, is een interne cultuur van tegenspraak van wezenlijk belang, waarbij men collega's, ondergeschikten en leidinggevenden steeds bevraagt, aanspreekt en kritische vragen durft te stellen. Voorts kan een intern moreel kompas worden bevorderd bij de diensten door doorlopende training, discussiebijeenkomsten en ethische reflectie op de uitvoeringspraktijk.

# A Background: the framework of the right to privacy according to article 8 ECHR

## A.1 The right to privacy[138]

Article 8 of the European Convention on Human Rights (ECHR) stipulates the following:

**Right to respect for private and family life**

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

### *A.1.1 Material scope*

Article 8 safeguards the right to respect for private and family life, home and correspondence and is commonly referred to as protecting the right to privacy. The European Court of Human Rights (ECtHR) has taken the position that "Private life is a broad term not susceptible to exhaustive definition. […] Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, **a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor**. […] **Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain**. It is for this reason that files gathered by **security services** on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method (see Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V)" (emphasis added).[139]

The second paragraph of Article 8 stipulates that an interference with the right to privacy is only allowed if it "is **in accordance with the law** and **is necessary in a democratic society** in the **interests of national security** (…)", so these are the requirements to be met by the proposed Wiv 20xx.

### *A.1.2 Relationship with the Charter of Fundamental Rights*

In our analysis for this PIA, we also examined cornerstone decisions of the Court of Justice of the European Union (CJEU) in relation to Article 7 of the Charter of Fundamental Rights of the European Union (CFR) on "Respect for private and family life". Article 52(3) CFR provides that "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall

[138] Unless otherwise stated, references to cases in this Appendix are to ECtHR cases.
[139] P.G. and J.H. v the United Kingdom (2001), §§56-57.

not prevent Union law providing more extensive protection."[140] In the context of Article 7 CFR, in the recent cases *Digital Right Ireland*[141] and *Schrems*[142], the CJEU has been referring extensively to the case law of the ECtHR in order to build a common "meaning and scope" of the right to respect for private life.

Article 52 CFR in its first paragraph establishes the conditions for any restrictions that may be imposed on the rights that are protected in the CFR. In particular, Article 52(1) CFR stipulates that "[a]ny limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the **essence** of those rights and freedoms. Subject to the **principle of proportionality**, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[143] (emphasis added).

The limitations established in Article 52(1) CFR and the limitations to the right to privacy in Article 8(2) ECHR are not identical. In particular the criterion that a limitation has to respect the "essence" of a right is difficult to construe, especially given the absence of established case law by the CJEU. In the two recent cases, *Digital Right Ireland* and *Schrems*, the concept of the "essence" of the right to respect for private life was examined by the CJEU. In *Digital Right Ireland* the Court examined Article 7 in relation to the limitations that are established in Article 52(1) CFR and found that the interference with the right to privacy posed by the retention of data, in accordance with Directive 2006/24/EC, was "not such as to adversely affect the essence"[144] of –among others- the right to privacy. However, the Court found that the "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality"[145] and thus declared Directive 2006/24/EC invalid on this basis. The CJEU, in *Schrems* examined again Article 7 in relation to the limitations that are established in Article 52(1) CFR and found that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter"[146].

The limitations set out in Article 52(1) CFR and those in Article 8(2) ECHR are not completely overlapping, although the CJEU "has identified the requirements listed in Article 8(2) of the ECHR with those of Article 52(1) of the Charter"[147]. As Gloria González Fuster notes "Reading these provisions as having the same meaning raises some complex questions. Not only is the wording of Article 8(2) of the ECHR and of Article 52(1) of the Charter not identical, but, in addition, the case law of the

---

[140] Article 52(3) CFR.
[141] ECJ 8 April 2014, Digital Rights Ireland (Joined cases C-293/12 & 594/12) ECLI:EU:C:2014:238.
[142] ECJ 6 October 2015, Schrems (C-362/14) ECLI:EU:C:2015:650.
[143] Article 52(1) CFR.
[144] ECJ 8 April 2014, Digital Rights Ireland (Joined cases C-293/12 & 594/12) ECLI:EU:C:2014:238, §39.
[145] ECJ 8 April 2014, Digital Rights Ireland (Joined cases C-293/12 & 594/12) ECLI:EU:C:2014:238, §69.
[146] ECJ 6 October 2015, Schrems (C-362/14) ECLI:EU:C:2015:650, §94.
[147] González Fuster 2015, p. 524.

European Court of Human Rights on the requirements of Article 8(2) of the ECHR and the case law of the EU Court of Justice on Article 52(1) of the Charter is also different".[148] However, González Fuster further notes that "As the EU Court of Justice nowadays often bases its judgements on joint readings of Article 7 and 8 of the Charter, the specificity of the requirements derived from the ECHR and those derived from the Charter tends to be blurred".[149] Therefore, even if the CFR is not directly applicable to national security and intelligence authorities, it is important to examine the interpretation of this right in the case law of the CJEU in cases relevant to Article 7 CFR.

*A.1.3* *1.3. Guidelines on human rights and the fight against terrorism*

The Guidelines on human rights and the fight against terrorism were adopted by the Council of Europe in 2002[150] and contain two chapters that present great relevance for the current analysis. Chapter V "Collection of personal data by any competent authority in the field of State security" sets out specific conditions under which the processing of personal data is allowed by intelligence and national security agencies and law enforcement authorities. More concretely is required that:

> "Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:
> (i) are governed by appropriate provisions of domestic law;
> (ii) are proportionate to the aim for which the collection and the processing were foreseen;
> (iii) may be subject to supervision by an external independent authority".[151]

Moreover, Chapter VI provides guidance for measures that can be taken by States and would interfere with the right to privacy:

> "1. Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court.
> 2. Measures taken to fight terrorism must be planned and controlled by the authorities so as to minimise, to the greatest extent possible, recourse to lethal force and, within this framework, the use of arms by the security forces must be strictly proportionate to the aim of protecting persons against unlawful violence or to the necessity of carrying out a lawful arrest."[152]

[148] González Fuster 2015, p. 524-525.
[149] González Fuster 2015, p. 526.
[150] Council of Europe, *Guidelines on human rights and the fight against terrorism adopted by the Committee of Ministers on 11 July 2002 at the 804th meeting of the Ministers' Deputies*, available at https://www1.umn.edu/humanrts/instree/HR%20and%20the%20fight%20against%20terrorism.pdf (accessed 1 December 2015).
[151] Ibid. p. 9.
[152] Ibid., p. 9.

## A.2 In accordance with the law (national laws have to refer to the following elements)

According to Art. 8(2) ECHR the interference has to be "in accordance with the law". This requirement is what is known as the legality requirement and it is common in the second paragraph of articles 8 to 11 ECHR. In order to satisfy the legality test, the interferences shall be based on domestic law and compatible with the rule of law.[153] The first requirement is set out in the text of article 8(2) and the second, as Mentioned in S and Marper, "is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of article 8."[154]

The legality test was initially discussed -regarding article 10(2) ECHR- by the Court in the Sunday Times case[155]. The similarity between the right limitation clauses included in article 8 to 11 ECHR opened the door to apply Sunday Times' interpretation of article 10 to the limitations on the right to privacy. The Court confirmed this possibility in Silver[156] where it explicitly extended the interpretation of article 10(2) made in Sunday Times to the limitations of the right to privacy contained in article 8(2) ECHR and established that any admissible interference with article 8 in order to satisfy the legality test needs to be based on a national law that is adequately accessible and foreseeable. Subsequently, the Court has repeatedly held this position, as it be elaborated below.[157]

### *A.2.1 Legal basis in the national law*

The ECtHR has taken a broad understating of the concept of the "law". When the Court stipulates that any interference needs to have some basis in domestic law it does not refer to formal sense of law but to the substantive sense. Therefore, the legal basis can be given by statute law, but also by provisions with lower than legal rank, case-law and rules of public international law incorporated in the domestic legal system[158]. By taking this position, the Court preserves the essence of the common law legal systems and allows the "law" to adapt to the continuous technological development through judicial decisions. Moreover, it includes in the concept of *law* other statutes that without being formal law contribute to the legality requirement by permitting the subject of surveillance to foresee in which conditions he might be subject to such measures and therefore reduce arbitrariness.

### *A.2.2 Accessibility and foreseeability of the law*

The ECtHR considers that a law is **adequately accessible** when: "the citizen must be able to have an indication that is adequate, in the circumstances, of the legal

---

*153* S and Marper v UK (2008), §95.
*154* S and Marper v UK (2008), §95.
*155* Sunday Times v UK (1979), §49.
*156* Silver v UK (1983), §§85-88.
*157* See, inter alia, Leander v Sweden (1978), Huvig v Fance 1990, Kruslin v France 1990, Kopp v Switzerland (1998), Lambert v France (1998), Amman v Switzerland (2000), Khan v UK (2000), Perry v UK (2003), Weber Saravia v Germany (2006), Libery v UK (2008) , Iordachi v Moldova (2009), Kennedy v UK (2010) Shimovolos v Russia (2011).
*158* See, among others, Sunday Times v UK (1970) § 47, Kruslin v France (1990) § 29, Huvig v France (1990) §28, Kopp v Switzerland (1998) §60, Weber and Saravia v Germany (2006) § 87, etc.

rules applicable to a given case." [159] To have an indication of the rules that can be applied to each case implies that the provisions legitimizing the interferences need to be "open to public scrutiny and knowledge". The requirement of **foreseeability** means that a citizen "must be able –if need be with appropriate advice- to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"[160]. The Court admits that in some cases, the legislation cannot avoid using vague terms, the "interpretation and application [of which] are questions of practice"[161]. The Court states, "especially where a **power of the executive is exercised in secret**, the risks of arbitrariness are evident"[162] and thus, "there must be a **measure** of legal protection in domestic law **against arbitrary interferences** by public authorities with the rights safeguarded by paragraph 1 (art. 8-1)"[163]. Such legal protection is provided when satisfying the adequate level of accessibility and foreseeability. According to the case law of the ECtHR, "the level of precision required depends to a considerable degree on the content of the instrument in issue, the field it is designed to cover, and the number and status of those to whom it is addressed".[164]

The accessibility of the laws legitimising human rights limitations usually does not represent a problem. In relation to secret surveillance, only in a few cases the Court declared an interference to be unlawful because of lack of accessibility. One such example was Liberty (2008)[165] where the UK government did not reveal the circumstances under which the examination and disclosure of external intercepted communications were conducted. The Government argued that disclosing such information would damage the efficacy of the surveillance systems. The ECtHR discarded this possibility based on the full disclosure done by the German authorities in the case of Weber-Saravia v Germany (2006) in similar circumstances and subsequent disclosures done by the UK that did not seem to pose any risk for national security. Thus, when governments avoid public access to the provisions regulating surveillance measures on the sole basis that it would pose extra risks for national security or the surveillance operations, such law will not satisfy the accessibility requirement. Legal provisions permitting secret surveillance measures must "set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material".[166]

Although the Court in a lot of cases dealt with interception of communications, it found that there is no particular reason to apply different principles with regard to the accessibility and clarity of the law in cases of general surveillance programmes. In Liberty (2008) the Court found that: "It is true that the […] requirements [on foreseeability of the law] were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses […]. However, the Weber and Saravia case was itself concerned with generalised

[159] Sunday Times v UK, Silver and others v UK (1983), §87
[160] Sunday Times v UK series A no 30 (1979), §49.
[161] Sunday Times v UK series A no 30 (1979), §49.
[162] Klass v Germany (1978), §§42 and 49.
[163] Malone v UK (1984), §67.
[164] Sottiaux 2008, p. 43.
[165] Liberty v UK (2008).
[166] Liberty v UK (2008), §69.

"strategic monitoring", rather than the monitoring of individuals […]. **The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.** The Court's approach to the foreseeability requirement in this field has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in its above-cited decision in Christie v. the United Kingdom."[167]

In the specific field of secret surveillance of communications, in Malone[168] the Court ruled on interference with article 8 caused by legislation allowing secret surveillance of communications **by the police**. It reaffirmed the necessity to comply with the foreseeability requirement, but noting that in cases of secret surveillance such requirement "cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly"[169] Requiring full foreseeability in regards to secret surveillance measures would impede their effectiveness and undermine their ability to effectively counter terrorist threats.

Nonetheless, the Court set **minimum admissible standards of foreseeability**: "the law must be **sufficiently clear in its terms** to give citizens an **adequate indication as to the circumstances in which and the conditions** on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[170] With this ruling the Court aimed to ensure the effectiveness of surveillance operations while providing the adequate level of foreseeability required to be compatible with the rule of law. As mentioned in Malone, "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, **the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity**, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."[171]

The requirement of foreseeability of the law however does not need to be fulfilled by the substantive law itself, **the accompanying provisions lacking legal rank, like administrative instructions[172] or established practices**[173], can also be taken into

[167] Liberty v UK (2008), §63.
[168] Malone v UK, §§66-67.
[169] Malone v UK, §67.
[170] Malone v UK, §67.
[171] Malone v UK (1984), §68.
[172] Malone v UK (1984), §68.
[173] Silver and Others v UK (1983), §88.

account by the Court when deciding on whether the provisions are foreseeable enough. In this respect, in Malone[174] the Court decided on whether instructions or practices accompanying substantive law allowing surveillance measures should be taken into account to assess its level of foreseeability. by citing Sunday Times[175] to finally stipulate: "**the detailed procedures and conditions to be observed do not necessarily have to be incorporated in the substantive law**"[176].

## A.3 Legal safeguards against abuse in the legality test

The Court admitted that increasing terrorist threats affecting democratic societies justify the undertaking of secret surveillance measures to effectively counter such threats.[177] To avoid the authorities abusing the power provided modern surveillance technologies, the ECtHR requires its systems to "afford adequate safeguards against various possible abuses."[178] The first judgements detailing the safeguards to be included in legislations regulating secret surveillance of communications were Huvig[179] and Kruslin[180]. The Huvig and Kruslin judgments concerned telephone tapping. It is our opinion that the standards there set apply to any other surveillance measure causing similar level of interference. Subsequently, other cases[181] included the same safeguards and eventually they were listed in Weber and Saravia[182].

---

[174] Malone v UK (1984).

[175] Sunday Times, §88-89: 88. "…In view of these considerations, the Court points out once more that "many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice" (ibid.). And in the present case the operation of the correspondence control system was not merely a question of practice that varied in each individual instance: the Orders and Instructions established a practice which had to be followed save in exceptional circumstances (see paragraphs 26 and 27 above). In these conditions, the Court considers that although those directives did not themselves have the force of law, they may - to the admittedly limited extent to which those concerned were made sufficiently aware of their contents - be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the Rules. 89. For this reason, the Court cannot accept the applicants' additional contention that the conditions and procedures governing interferences with correspondence - and in particular the directives set out in the Orders and Instructions - should be contained in the substantive law itself."

[176] Malone v UK (1984), §68.

[177] Klass v Germany (1978), §48.

[178] Huvig v France (1990), §34 and Kruslin v France (1990), §35: "…the system does not for the time being afford adequate safeguards against various possible abuses. For example, the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court…"

[179] Huvig v France, §34.

[180] Kruslin v France, §35.

[181] See, among others, Amman v Switzerland (2000), §76 and Valenzuela Contreras v Spain (1998), §46 part (iv)

[182] Weber and Saravia v Germany (2006).

In Weber and Saravia, the Court mentions that according to the case law on surveillance measures it developed the **minimum safeguards** that have to be included in statute law are:

a. the nature of the offences which may give rise to an interception order;
b. a definition of the categories of people liable to have their telephones tapped;
c. a limit on the duration of telephone tapping;
d. the procedure to be followed for examining, using and storing the data obtained;
e. the precautions to be taken when communicating the data to other parties;
f. the circumstances in which recordings may or must be erased or the tapes destroyed.[183]

The development of new surveillance technologies moved the Court to adapt it requirements to new surveillance modalities. In Uzun (2010)[184], the Court examined which legal safeguards should apply to GPS surveillance. Its judgement took into account that location surveillance is a lower interference than surveillance of communications and there also reduced the required safeguards to the more general ones already mentioned in Klass,[185] as follows:

a. all the circumstances of the case, such as the nature, scope and duration of the possible measures,
b. the grounds required for ordering them,
c. the authorities competent to permit, carry out and supervise them,
d. and the kind of remedy provided by the national law.[186]

When assessing whether the safeguards listed above are part of the national law regulating the secret surveillance measures as part of the legality test, the Court **only evaluates their presence**, not its impact on the surveillance measure carried on or the actual level of protection they provide.

In S and Marper (2008) when the Court is assessing whether the national legislation provides sufficient level of accessibility and foreseeability, the Court repeats that domestic law should not only provide “clear, detailed rules governing the scope and application of (surveillance) measures” [but also] “**minimum safeguards** concerning*, inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data, and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.”[187]

## A.4 Oversight

The ECtHR has developed a very comprehensive classification of the stages when oversight in relation to secret surveillance is relevant and has identified three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. The three stages are briefly but comprehensively analysed in

[183] Ibid., §95.
[184] Uzun v Germany (2010).
[185] Klass v Germany (1978), §50.
[186] Uzun v Germany (2010), §63.
[187] S and Marper v UK (2008), §99.

the recent case *Roman Zakharov v. Russia*: “As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual’s knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure […]. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively […] or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts’ jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications […].[188]

The ECtHR has taken the position that the oversight of surveillance authorities should in principle be entrusted to a judge. In *Telegraaf Media* the ECtHR summarized its established case-law as follows: “[t]he Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge”.[189] However the Court has been “prepared to accept as adequate the independent supervision available”[190] in a few cases.

In *Telegraaf Media* it was presented that “the use of special powers would appear to have been authorised by the Minister of the Interior and Kingdom Relations, if not by the head of the AIVD or even a subordinate AIVD official, but in any case without prior review by an independent body with the power to prevent or terminate it. […] Moreover, review post factum, whether by the Supervisory Board, the Committee on the Intelligence and Security Services of the Lower House of Parliament or the National Ombudsman, cannot restore the confidentiality of journalistic sources once it is destroyed”[191]. Therefore the ECtHR required effective prior oversight to protect

[188] Roman Zakharov v Russia (2015), §233-234.
[189] Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands, (Application no. 39315/06), 22 November 2012 (FINAL 22 February 2013), §98.
[190] Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands, (Application no. 39315/06), 22 November 2012 (FINAL 22 February 2013), §98, citing Klass and Others v Germany, §56, and Kennedy v UK, §167.
[191] Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands, (Application no. 39315/06), 22 November 2012 (FINAL 22 February 2013), §100-101.

journalistic sources. As the issue of oversight depends on the actual safeguards that governments have put in place for the supervision of their surveillance authorities, it is worth examining in detail some of the most prominent cases examined in detail by the ECtHR.

In *Klass* the Court examined the oversight of a surveillance system foreseen in the German Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnisses), the G10. The G10 excluded judiciary control, which was "replaced by an initial control effected by an official qualified for judicial office and by the control provided by the Parliamentary Board and the G10 Commission"[192]. The Court found that "the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society"[193]. In accordance with the G10 "in practice and except in urgent cases, the Minister seeks the prior consent of [the G10] Commission"[194]. What played crucial role in order for the Court to reach such a conclusion was that both the Parliamentary Board and the G 10 Commission are "independent of the authorities carrying out the surveillance, and are vested with sufficient powers and competence to exercise an effective and continuous control. Furthermore, the democratic character is reflected in the balanced membership of the Parliamentary Board. The opposition is represented on this body and is therefore able to participate in the control of the measures ordered by the competent Minister who is responsible to the Bundestag. The two supervisory bodies may, in the circumstances of the case, be regarded as enjoying sufficient independence to give an objective ruling"[195]. Moreover the individuals, even if only in exceptional circumstances, had the opportunity to complain to the G10 Commission and could have recourse to the Constitutional Court.[196] It should be noted that the G10 Commission was chaired by an official qualified to hold judicial office.[197] So, the exercise of effective and continuous control, as well as the fact that the measures ordered by the Minister could be limited by the Parliamentary Board, where the opposition was also represented. When the ECtHR examined the G10 in the context of a more recent case, it found that the supervision system, which remained unchanged in the G10, was "such as to keep the interference resulting from the contested legislation to what was "necessary in a democratic society""[198].

In *Kennedy* the ECtHR examined the oversight system in the UK and found that the oversight exercised by the Interception of Communications Commissioner for the interception of internal communications, along with the scrutiny of the Investigatory Powers Tribunal (IPT) provide sufficient safeguards against abuse. In particular the ECtHR repeated its position that "it is in principle desirable to entrust supervisory control to a judge [….]. In the present case, the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems […], any person who suspects that his

[192] Klass v Germany (1978), §56.
[193] Klass v Germany (1978), §56.
[194] Klass v Germany (1978), §21.
[195] Klass v Germany (1978), §56.
[196] Klass v Germany (1978), §56.
[197] Klass v Germany (1978), §21.
[198] Weber and Saravia v Germany (2006), §117

communications have been or are being intercepted may apply to the IPT […]. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers […]. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of a warrant of all documents it considers relevant […]. In the event that the IPT finds in the applicant's favour, it can, *inter alia*, quash any interception order, require destruction of intercept material and order compensation to be paid […]. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom […]"[199].

In addition to the IPT, the oversight in the UK is realised via the Interception of Communications Commissioner. The Commissioner was appointed by the Prime Minister and had a three-year, renewable term. According to the ECtHR, to the date of the judgment there had been two Commissioners appointed under RIPA, who were both former judges of the Court of Appeal.[200] The Commissioner has the task to oversee the general functioning of the surveillance regime and the authorisation of interception warrants in specific cases in the UK and reports any violation to the Prime Minister.With regard to the role and responsibilities of the Interception of Communications Commissioner the Court made specific statements to support its position that the oversight system was in accordance with Article 8 ECHR: "The Court notes that the Commissioner is independent of the executive and the legislature and is a person who holds or has held high judicial office […]. He reports annually to the Prime Minister and his report is a public document (subject to the non-disclosure of confidential annexes, which is laid before Parliament […]. In undertaking his review of surveillance practices, he has access to all relevant documents, including closed materials and all those involved in interception activities have a duty to disclose to him any material he requires […]. The obligation on intercepting agencies to keep records ensures that the Commissioner has effective access to details of surveillance activities undertaken. The Court further notes that, in practice, the Commissioner reviews, provides advice on and approves the section 15 arrangements […]. The Court considers that the Commissioner's role in ensuring that the provisions of RIPA and the Code are observed and applied correctly is of particular value and his biannual review of a random selection of specific cases in which interception has been authorised provides an important control of the activities of the intercepting agencies and of the Secretary of State himself."[201]

Contrary to the aforementioned cases, the ECtHR found the oversight system deployed in Bulgaria as not sufficient to safeguard infringements to Article 8 ECHR. In *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, the ECtHR examined the Special Surveillance Means Act of 1997

[199] Kennedy v United Kingdom (2010), §167.
[200] Kennedy v United Kingdom (2010), §57.
[201] Kennedy v United Kingdom (2010), §166.

(SSMA). The ECtHR found, among others, that "the overall control over the system of secret surveillance is entrusted solely to the Minister of Internal Affairs […] – who not only is a political appointee and a member of the executive, but is directly involved in the commissioning of special means of surveillance –, not to independent bodies, such as a special board elected by the Parliament and an independent commission[…], or a special commissioner holding or qualified to hold high judicial office […], or a control committee consisting of persons having qualifications equivalent to those of a Supreme Court judge".[202] The ECtHR also focused on the fact that "neither the Minister, nor any other official is required to **regularly report** to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases".[203] In *Roman Zakharov v. Russia* the ECtHR found that "The prohibition on logging or recording interceptions set out in Russian law makes it impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. Combined with the law-enforcement authorities' technical ability, pursuant to the same Order no. 70, to intercept directly all communications, this provision renders any supervision arrangements incapable of detecting unlawful interceptions and therefore ineffective"[204]. The ECtHR therefore established a requirement that sufficient information should be kept about the surveillance measures taken in order for the supervising authorities to be able to assess their legitimacy. Moreover in *Roman Zakharov v. Russia* the ECtHR reiterated its position in previous cases on "whether the supervisory body's activities are open to public scrutiny"[205], which is an essential feature to guarantee independent and effective supervision. The fact that in *Roman Zakharov v. Russia* the semi-annual report that are submitted by the prosecutors "concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. Moreover, the reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. It is also significant that the reports are confidential documents. They are not published or otherwise accessible to the public […]. It follows that in Russia supervision by prosecutors is conducted in a manner which is not open to public scrutiny and knowledge".[206]

In the recent *Roman Zakharov v. Russia* the ECtHR summarised its established case law on the issue of **independence** of the supervisory authorities: "As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the Prime Minister […]. In contrast, a Minister of Internal Affairs – who not only was a political

[202] Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria (2007), §87.
[203] Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria (2007), §88.
[204] Roman Zakharov v Russia (2015), §272.
[205] Roman Zakharov v Russia (2015), §283.
[206] Roman Zakharov v Russia (2015), §283.

appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent […]. Similarly, a Prosecutor General and competent lower-level prosecutors were also found to be insufficiently independent […]".[207]

In the recent *Roman Zakharov v. Russia* the ECtHR highlighted the fact that " the supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the **effectiveness** of its supervision (see, for example, Klass and Others […]§ 53, where the intercepting agency was required to terminate the interception immediately if the G10 Commission found it illegal or unnecessary; and Kennedy […]§ 168, where any intercept material was to be destroyed as soon as the Interception of Communications Commissioner discovered that the interception was unlawful). The Court is satisfied that prosecutors have certain powers with respect to the breaches detected by them. Thus, they may take measures to stop or remedy the detected breaches of law and to bring those responsible to […]. However, there is no specific provision requiring destruction of the unlawfully obtained intercept material […]."[208] In particular the ECtHR found that the" prosecutors' inability to obtain access to classified materials relating to interceptions [as an] example [that] raises doubts as to the effectiveness of supervision by prosecutors in practice.[209] In view of the established case law of the ECtHR the fact that the WiV 20xx does not provide the CTIVD with a competence to prevent or stop interventions that it deems unlawful, would render the oversight system as ineffective.

In the recent *Roman Zakharov v. Russia* the ECtHR examined in detail the competences and powers vested to the prosecutor, who according to the Russian legislation may exercise supervision over operational-search activities. The ECtHR repeated his position that "it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required"[210] . The ECtHR in *Roman Zakharov v. Russia* found that the scope of supervision of the Russian prosecutors was limited due to the fact that "information about the security services' undercover agents, and about the tactics, methods and means used by them, [was] outside the scope of prosecutors' supervision. […] Moreover, surveillance measures related to counter-intelligence de facto escape supervision by prosecutors".[211]

## A.5 Legitimate purpose

According to article 8(2) ECHR, lawful interferences with the right to privacy must serve one of the following legitimate purposes: national security, public safety, economic wellbeing of the country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others. The Court has accepted a very broad range of legitimate purposes.

---

[207] Roman Zakharov v Russia (2015), §278.
[208] Roman Zakharov v Russia (2015), §282.
[209] Roman Zakharov v Russia (2015), §284.
[210] Roman Zakharov v Russia (2015), §281, citing also Kennedy, §166.
[211] Roman Zakharov v Russia (2015), §281.

When assessing the interference of surveillance systems with the right to privacy, the most used legitimate aims are **national security**[212] and **prevention of disorder or crime**[213]. As in the text of the Convention the legitimate aims are expressed in very broad terms, making it to justify any interference under one of the listed purposes, the requirement has almost been converted into a mere formality and the Court examines the legitimacy of the purposes as part of the necessity test[214]. The Court accepted these broad expressions and did not require more specific terms to consider valid the legitimate aims.[215]

### *A.5.1 Concept of national security*

National security is commonly used as a "legitimate aim" to justify interferences with the right to privacy caused by surveillance measures.[216] The broad terms in which the legitimate aims contained in article 8(2) are expressed, do not help to set the boundaries of the term "national security" and define the purposes that can fall under this concept[217]. Furthermore, the Court never defined the scope of the term **national security** either. However, in Liberty[218] the Court referred to the definition of national security given by the British Commissioner designated under the British Interception of Communications Act of 1985 (RIPA's predecessor ). In his report of 1986 he defined **threats to national security** as activities: "which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means."[219] Later on, the Court again mentions this definition in Kennedy[220] when indicating how to apply the term regarding secret surveillance activities in the UK.

## A.6 Necessary in a democratic society

The ECHR is introducing in the second paragraph of articles 8 to 11 a democratic necessity test[221]. The notion of "democratic society" and that of "necessity" as intrinsic elements to the democratic necessity test. The necessity test is satisfied when the right limitation corresponds to a **pressing social need** and it is **proportionate** to the legitimate aim pursued[222]. The interference will be considered lawful when it contributes to make the social interest prevail over the interests of individuals. Moreover, the interference cannot go beyond what is necessary in democratic society[223].

---

[212] See, among others Segerstedt-Wiberg v Sweden (2006), §87 and Weber and Saravia v Germany (2006), §106.
[213] See, among others, Lambert v France (1998), §28, S and Marper v UK (2008), §100, Kvasnika v Slovakia (2009), §82
[214] Cameron 2000, p. 35.
[215] See, among others, Lambert v France (1998), §28, Weber and Saravia v Germany (2006), §106, Segerstedt-Wiberg v Sweden (2006), §87, S and Marper v UK (2008), §100, Kvasnika v Slovakia (2009), §82.
[216] See, among others Segerstedt-Wiberg v Sweden (2006), §87 and Weber and Saravia v Germany (2006), §106.
[217] Cameron 2000, p. 36.
[218] Liberty v UK (2008), §20
[219] Report of the UK Commissioner of 1986 under reference of Liberty v UK (2008), §20.
[220] Kennedy v UK (2010), §159.
[221] Sottiaux 2008, p. 44.
[222] Gillow v UK (1986), §55 under reference of Leander v Sweden (1987), §58.
[223] Jacobs, White and Ovey 2010, p. 311.

The Court discussed extensively the democratic necessity test in the context *Handyside v. UK* (1976), which dealt with the right to freedom of expression (Art. 10 ECHR). However, as the requirements for justifying interference with the right to freedom of expression are similar to the ones of the right to privacy, the Court's views are relevant for the present analysis. On the use of the adjective "necessary" in the French law in question, the Court found that"'the adjective "necessary", within the meaning of Article 10 para. 2 […], is not synonymous with "indispensable" […], the words "absolutely necessary" and "strictly necessary" and […], the phrase "to the extent strictly required by the exigencies of the situation"), neither has it the flexibility of such expressions as "admissible", "ordinary" […], "useful" […], "reasonable" […] or "desirable". Nevertheless, it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context"[224].

In the same case the Court clearly stated however that "*it is for the national authorities to make the initial assessment of the reality of the pressing social need implied by the notion of "necessity" in this context.*"[225]

The reasoning that the Court expressed in *Handyside*, "was first applied in the sphere of Article 8 s 2 in the cases *Dudgeon v United Kingdom* and *Silver v United Kingdom*"[226]. The Court has explicitly purported that "the notion of necessity implies that the interference corresponds to a **pressing social need** and, in particular, that it is **proportionate** to the legitimate aim pursued; in determining whether an interference is 'necessary in a democratic society', the Court will take into account that **a margin of appreciation** is left to the Contracting States […]."[227]. The elements of pressing social need and proportionality to the legitimate aim pursued has been part of established jurisprudence of the ECtHR.

### *A.6.1 Margin of appreciation*

The doctrine of the margin of appreciation indicates the **level of discretion** a State has in relation to the protection of the rights that are safeguarded in the ECHR. According to the Court "*This margin is given both to the domestic legislator ("prescribed by law") and to the bodies, judicial amongst others, that are called upon to interpret and apply the laws in force […]*."[228]

Contracting States enjoy a certain margin of appreciation when defining the *necessity* of right limitations in their jurisdictions. The proximity and continuous contact of the national authorities with the actors and undergoing situations in their countries provides them a privileged position in comparison to any international judge[229]. The discretion of national authorities is nonetheless not unlimited. It is the task of Strasbourg to rule on their adherence to the ECHR[230], deciding whether or not the national authorities imposed restrictions are according to the Convention.

---

[224] Handyside v UK (1976), §48.
[225] Handyside v UK (1976), §49.
[226] Sottiaux 2008, p. 271.
[227] Olsson v Sweden (1998), §67.
[228] Handyside v UK (1976), §48.
[229] Handyside v UK (1976), §48.
[230] Handyside v UK (1976), §49.

When developing its supervisory function the Court will have to put special emphasis in the principles that characterize a democratic society[231].
The application of the margin of appreciation is difficult to foresee. It changes according to the context of each case and its elements - summarized in Silver[232] - are addressed inconsistently by the jurisprudence of Court[233]. The breadth of the margin of appreciation nevertheless follows some general patterns:

1. Contracting states have a narrow margin of interest when:
    a. particularly important existence or identity aspects of an individual are involved. Some examples found in case law involve the right of physical integrity, sexual freedom or the disclosure of sensitive personal data[234].
2. Contracting sates have a wide margin of appreciation when:
    a. areas where States have no common standards in respect to certain issues. This happens in cases involving morals, since there is no uniform conception of morality amid the contracting states;
    b. it is necessary to strike a balance between public and private interests or rights contained in the ECHR;[235]
    c. national Security is the issue at stake.[236]

Limitations to rights caused by measures of secret surveillance of communications are often conducted in the interest of national security.[237] While in the sphere of national security authorities enjoy a wide margin of discretion, the Court -playing its supervisory role- ensures national authorities have adequate safeguards in place to avoid arbitrariness and abuse.[238]

[231] Handyside v UK (1976), §49.
[232] Silver v UK (1983), §97.
[233] Robin, White and Ovey 2010, p. 326.
[234] X and Y v Netherlands (1985) and case of Z v Finland (1998), under reference of Robin, White and Ovey 2010, p. 326.
[235] Taşkin and Others v Turkey, (2004), §119; Giacomelli v Italy, (2006), §83; and Hardy and Maile v the United Kingdom (2012), §221.
[236] Weber and Saravia v Germany (2006), §104.
[237] See, among others, Weber and Saravia v Germany (2006), §104 , Segerstedt-Wiberg v Sweden (2006), §87, Uzun v Germany (2010), §77,
[238] Klass v Germany (1978), §49 and Weber and Saravia v Germany (2006), §106.

# B Lijst met geïnterviewde personen

Mevr. H. Bos-Ollerman – Secretaris CTIVD
Dhr. M. Brinkman – medewerker MIVD
Dhr. Mr. H. Brouwer – Voorzitter CTIVD
Dhr. H. de Groot – hoofd juridische zaken AIVD
Drs. G. Kuiper – plv. directeur MIVD
Dhr. M. Kuipers – plv. DG AIVD
Mevr. mr. A. van Loon – plv. hoofd juridische zaken
Mevr. mr. Neijndorff – hoofd juridische zaken MIVD
N.N. – medewerker AIVD
Dhr. R. Prins – CEO Fox-IT

# C Literatuur

Bowden, Caspar (2013), *The US surveillance programmes and their impact on EU citizens' fundamental rights*, Report for the European Parliament.

Cameron, I. (2000), *National Security and the European Convention on Human Rights*, London/The Hague/Boston: Kluwer Law International.

Commissie Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002 (2013). *Naar een nieuwe balans tussen bevoegdheden en waarborgen.*

Commissie-GDT [Commissie Grondrechten in het digitale tijdperk] (2000), *Rapport*, Den Haag.

Council of Europe Commissioner for Human Rights (2015), *Democratic and effective oversight of national security services*, 5 June 2015, beschikbaar op https://www.coe.int/t/dghl/standardsetting/media/conf-foe-2015/Commissioner%20for%20Human%20Rights_Democratic%20and%20effective%20oversight%20of%20national%20security%20services.pdf.
CTIVD (2009), *Toezichtsrapport. Inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, CTIVD-rapport nr. 22A.

CTIVD (2014a), *Toezichtsrapport inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD*, CTIVD-rapport nr. 38, 5 februari 2014.
CTIVD (2014b), *Toezichtsrapport inzake onderzoek door de AIVD op sociale media*, CTIVD-rapport nr. 39, 16 juli 2014.

CTIVD (2015a), *Toezichtsrapport inzake toepassing van biologisch forensische onderzoeksmethoden door AIVD*, CTIVD-rapport nr. 42, 7 januari 2015.

CTIVD (2015b), *Toezichtsrapport over de samenwerking van de MIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*, CTIVD-rapport 22B, 10 juni 2015.

CTIVD (2015c), Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX, 26 augustus 2015.

Cuijpers, Colette & Bert-Jaap Koops (2008), *Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM*, TILT, oktober 2008.

Eskens, Sarah, Ot van Daalen & Nico van Eijk (2015), *Ten standards for oversight and transparency of national intelligence services*, Amsterdam: Institute for Information Law.

European Union Agency for Fundamental Rights (2015), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, Luxembourg: European Union Agency for Fundamental Rights.

González Fuster, Gloria (2015), 'Curtailing a Right in Flux: Restrictions of the Right to Personal Data Protection', in Artemi Rallo Lombarte and Rosario García Mahamut (eds.), *Hacia un nuevo régimen europeo de protección de datos. Towards a new European Data Protection Regime*, Tirant lo Blanch, Valencia.

Hazewinkel-Suringa-Remmelink (1994), *Inleiding tot de studie van het Nederlandse Strafrecht*, 13e druk, Arnhem: Gouda Quint.

Jacobs, Bart (2015), 'Vluchtig en Stelselmatig. Een bespreking van interceptie door inlichtingen- en veiligheidsdiensten', NJB-blog, 5 februari 2015. Te raadplegen op: http://njb.nl/blog/vluchtig-en-stelselmatig-een-bespreking-van.13474.lynkx.

Jacobs, Bart (2016), 'Select while you collect. Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten', *Nederlands Juristenblad* (4), p. 256-261.

Jacobs, F.G., R.C.A. White and C. Ovey (2010), *The European Convention on Human Rights*, 5th ed., Oxford: Oxford UP.

Koops, Bert-Jaap & Jan Smits, m.m.v. Frank van der Kroon (2014), *Verkeersgegevens en artikel 13 Grondwet. Een technische en juridische analyse van het onderscheid tussen verkeersgegevens en inhoud van communicatie*, Oisterwijk: Wolf Legal Publishers.

Koops, Bert-Jaap (2012), 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor veiligheid* 11 (2), p. 30-46.

Koops, Bert-Jaap, Hanneke van Schooten & Merel Prinsen (2004), *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, ITeR-reeks deel 70.

Koops, Bert-Jaap, Rudi Bekkers, Frank Bongers & Marieke Fijnvandraat (2005), *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, Tilburg, november 2005.

Loof, J.P. e.a. (2015), *Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Universiteit Leiden, augustus 2015.

Nissenbaum, Helen (2010), *Privacy in Context. Technology, policy, and the integrity of social life*, Stanford: Stanford University Press.

Sottiaux, Stefan (2008), *Terrorism and the Limitation of Rights*, Hart Publishing.

Tokmetzis, Dimitri (2013), 'Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst', *de Correspondent* 20 december 2013.

WRR (2011), *iOverheid*, WRR-rapport nr. 86.