· Bw. Studie 49 23-01-2007 14:39 Pagina 1

Van privacyparadijs tot controlestaat?

Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw

· Bw. Studie 49 23-01-2007 14:39 Pagina 2

© Rathenau Instituut/TILT 2007

Uitgever: Rathenau Instituut

Anna van Saksenlaan 51
Correspondentieadres:
Postbus 95366
2509 CJ Den Haag

Telefoon 070 - 342 15 42
Fax 070 - 363 34 88
E-mail info@rathenau.nl
Website www.rathenau.nl

Basisvormgeving: Hennie van der Zande, Amsterdam
Opmaak: Henny Scholten, Amsterdam
Beeld: Hollandse Hoogte, Amsterdam
Grafische productie: Herbschleb & Slebos, Monnickendam
Pre-press en druk: Meboprint, Amsterdam
Bindwerk: Meeuwis, Amsterdam
Vertaling Summary: english text company, Den Haag

Dit boek is gedrukt op kringlooppapier
Eerste druk: februari 2007
ISBN: 978-90-77364-14-7
EAN: 9789077364147

Deze publicatie kan als volgt worden aangehaald:
Vedder, Anton, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut, 2007; Studie 49

Preferred citation:
Vedder, Anton, Leo van der Wees, Bert-Jaap Koops en Paul de Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut, 2007; Study 49

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het Rathenau Instituut/TILT.

No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without prior written permission of the holder of the copyright.

· Bw. Studie 49 23-01-2007 14:39 Pagina 3

Van privacyparadijs tot controlestaat?

Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw

Auteurs
Anton Vedder
Leo van der Wees
Bert-Jaap Koops
Paul de Hert

Eindredactie
Dirk van Harten
Geert Munnichs

Projectcoördinatie Rathenau Instituut
Geert Munnichs
André Krom
Anne Kets

Studie 49
Februari 2007

· Bw. Studie 49 23-01-2007 14:39 Pagina 4

Bestuur Rathenau Instituut
drs. W.G. van Velzen (voorzitter)
mw. prof.dr. C.D. Dijkstra
mw. dr. A. Esmeijer
mr.dr. P.W. Kwant
mw. prof.dr. P. Meurs
mw. dr. B.E.C. Plesch
prof.dr. H.A.A. Verbon
dr. A. Zuurmond

· Bw. Studie 49 23-01-2007 14:39 Pagina 5

Voorwoord

Sinds het begin van het nieuwe millennium is de westerse wereld opgeschrikt door terreuraanslagen. Deze aanslagen hebben het denken over veiligheid in een stroomversnelling gebracht. Binnen zowel Nederland als Europa heeft dat geleid tot tal van overheidsmaatregelen waarmee de strijd tegen misdaad en terreur wordt aangebonden. Zie de verlengde bewaartermijn van telecommunicatiegegevens, de invoering van de identificatieplicht en het biometrisch paspoort of de aanscherping van veiligheidsmaatregelen op luchthavens.

Veel van deze maatregelen waren tien of vijftien jaar geleden ondenkbaar vanwege de gevolgen voor de privacy. De snelle veranderingen op het gebied van veiligheid waren voor het Rathenau Instituut aanleiding om begin 2006 een onderzoek te starten naar de gevolgen van die maatregelen voor de samenleving. De privacy van 'gewone' burgers vormt hierbij een belangrijk aandachtspunt. Immers, steeds vaker richten opsporings- en veiligheidsdiensten hun vizier op het doen en laten van onverdachte personen.

Een tweede reden voor dit onderzoek vormt de constatering dat het geheel aan veiligheidsmaatregelen nauwelijks maatschappelijke discussie oproept. De discussie die wordt gevoerd, gaat vooral over afzonderlijke maatregelen. Hoe deze op elkaar ingrijpen en elkaar versterken, blijft daardoor buiten beschouwing. De optelsom van de maatregelen kan echter een heel ander beeld geven dan wanneer ze alleen afzonderlijk worden bezien. Juist dat 'totaalplaatje' is van belang voor een doordachte oordeelsvorming over de maatregelen.

Het Rathenau Instituut heeft TILT (Tilburg Institute for Law, Technology and Society) opdracht gegeven een overzicht te geven van de opsporings- en veiligheidsmaatregelen die de afgelopen jaren zijn ingevoerd en die voor de komende jaren nog te verwachten zijn, inclusief het cumulatieve effect van die maatregelen op de privacy van de burger. Deze studie is daarvan het resultaat.

Van privacyparadijs tot controlestaat? laat zien dat technologische mogelijkheden een grote, zoniet doorslaggevende rol spelen binnen het veiligheidsbeleid. In toenemende mate staan politie en justitie middelen ter beschikking als telefoontaps, toezichtcamera's, DNA-profielen of de mogelijkheid om met behulp van computerprogramma's bestanden met persoonsgegevens te analyseren (*datamining*).

· Bw. Studie 49 23-01-2007 14:39 Pagina 6

In combinatie met hun – fors verruimde – bevoegdheden krijgen opsporings- en veiligheidsdiensten daarmee bijna onbeperkte toegang tot alle persoonsgegevens van burgers. Tegelijkertijd lijkt de privacy van de burger steeds minder gewicht in de schaal te leggen, zodra veiligheidsbelangen in het geding zijn.

De studie roept de vraag op of de balans tussen veiligheid en privacy niet is doorgeslagen. Ze maakt duidelijk dat de gevolgen van de optelsom van de veiligheidsmaatregelen veel verder gaan dan velen tot voor kort voor mogelijk of wenselijk hielden. Deze uitkomst vraagt om een hernieuwde maatschappelijke en politieke bezinning op de vraag hoeveel privacy 'wij' als samenleving overhebben voor onze veiligheid. Met deze uitgave wil het Rathenau Instituut een stimulans geven aan het debat daarover.

Mr.drs. Jan Staman
Directeur Rathenau Instituut

· Bw. Studie 49 23-01-2007 14:39 Pagina 7

Inhoud

Voorwoord 5

Samenvatting 9

1 Inleiding 15

Deel I

De ontwikkelingen in kaart gebracht

2 Toenemende controle 21
2.1 Nederland privacyparadijs: 1960-1985 21
2.1.1 Politie en justitie 22
2.1.2 Inlichtingendiensten 23
2.2 Verlies van onschuld: 1985-2006 23
2.2.1 Privacywetgeving 23
2.2.2 DNA-onderzoek 24
2.2.3 Cameratoezicht 25
2.2.4 Computeronderzoek 26
2.2.5 Bijzondere opsporingsbevoegdheden 27
2.2.6 Identificatieplicht 28
2.2.7 Koppeling bestanden 28
2.2.8 Inschakelen van derden 29
2.2.9 Aftappen telecommunicatie 29
2.2.10 Vorderen gegevens 31
2.2.11 Buitenlandse druk 32
2.3 Achtergronden 32
2.3.1 Georganiseerde misdaad 34
2.3.2 Einde Koude Oorlog 34
2.3.3 Europa 35
2.3.4 Technologische ontwikkelingen 35
2.4 Trends 36

3 Toekomstige ontwikkelingen 39
3.1 Binnenkort te verwachten 39
3.1.1 Burgerservicenummer 39
3.1.2 Bevoegdheden AIVD 40
3.1.3 Bewaartermijn verkeersgegevens 40
3.1.4 Buitenlandse toegang politieregisters 41
3.1.5 Biometrisch paspoort 41

· Bw. Studie 49 23-01-2007 14:39 Pagina 8

3.2 Op langere termijn 42
3.2.1 Slimme camera's 42
3.2.2 RFID 43
3.2.3 Ambient Intelligence 44
3.3 Veranderende beleidsopvattingen 44

Deel II

De ontwikkelingen nader bezien

4 Maatschappelijke bezwaren 49
4.1 Kritiek op de maatregelen 49
4.1.1 DNA-onderzoek 49
4.1.2 Cameratoezicht 49
4.1.3 Bijzondere opsporingsbevoegdheden 50
4.1.4 Identificatieplicht 52
4.1.5 Koppeling bestanden 52
4.1.6 Vorderen financiële gegevens 53
4.1.7 Vorderen telecommunicatiegegevens 53
4.1.8 Wet bevoegdheden vorderen gegevens 54
4.1.9 Bewaartermijn verkeersgegevens 56
4.1.10 Biometrisch paspoort 57
4.2 Kenmerken van het debat 57

5 Een agenda voor debat 61
5.1 Privacy onder de loep 61
5.1.1 Wat is privacy? 61
5.1.2 Privacy en 'gewone' mensen 63
5.1.3 Afwegingen bij privacyconflicten 63
5.1.4 Gaten in de muur 65
5.2 De optelsom van maatregelen 66
5.2.1 Privacy en technologie 66
5.2.2 Privacyrisico's 67
5.3 Thema's voor het debat 69

Summary 71

Noten 75

Literatuur 81

Adviescommissie 87

Over de auteurs 89

· Bw. Studie 49 23-01-2007 14:39 Pagina 9

Samenvatting

De bestrijding van georganiseerde misdaad en terrorisme staat nationaal en internationaal hoog op de politieke agenda. De afgelopen jaren heeft de Nederlandse overheid talrijke wetten aangenomen die de opsporingsbevoegdheden van politie, justitie en de veiligheidsdiensten drastisch hebben verruimd.

Deze bevoegdheidsuitbreidingen kunnen vergaande gevolgen hebben voor de grondrechten en privacy van burgers. Toch leiden ze maar in zeer beperkte mate tot maatschappelijke discussie. Als er al discussie ontstaat, gaat die bovendien vaak uitsluitend over één afzonderlijke maatregel; hoe de maatregelen op elkaar ingrijpen en elkaar mogelijk versterken, blijft buiten beschouwing. Een doordachte oordeelsvorming over de veiligheidsmaatregelen en hun gevolgen voor de privacy van burgers, vergt echter inzicht in deze cumulatieve effecten. Deze studie wil in deze behoefte voorzien.

Het onderzoek is op twee manieren afgebakend. Vanuit de veronderstelling dat de beschikbaarheid van opsporings- en onderzoekstechnieken een belangrijke factor vormt bij de uitbreiding van bevoegdheden, richt het onderzoek zich hoofdzakelijk op technologiegerelateerde maatregelen. Daarnaast worden de gevolgen van veiligheidsmaatregelen voor de 'gewone' burger centraal gesteld.

Overzicht van maatregelen

De studie geeft een opsomming van de overheidsmaatregelen in het kader van het opsporings- en veiligheidsbeleid. Daartoe worden drie periodes onderscheiden.

De periode vanaf de jaren zestig tot halverwege de jaren tachtig laat een relatief rustig en stabiel beeld zien. Politie en justitie beschikken over bekende en aloude bevoegdheden als huiszoeking, observatie en bevel tot uitlevering van voorwerpen. Verdergaande opsporingsmethoden (afluisteren, telefoontaps) worden als zeer ingrijpend beschouwd en – mede met het oog op de gevolgen voor de privacy van burgers – onderworpen aan beperkende voorwaarden. Dit beeld gaat in grote lijnen ook op voor de bevoegdheden van de veiligheidsdiensten.

Vanaf het einde van de jaren tachtig en het begin van de jaren negentig verandert de situatie drastisch. Wetten en wetswijzigingen die bestaande bevoegdheden verruimen of nieuwe introduceren, volgen elkaar in hoog tempo op. Ze vergemakkelijken het gebruik door politie, justitie en veiligheidsdiensten van DNA-onderzoek, cameratoezicht, taps, inkijkoperaties en computeronderzoek en maken het mogelijk om

· Bw. Studie 49 23-01-2007 14:39 Pagina 10

bestanden aan elkaar te koppelen en gegevens bij derden te vorderen. De terroristische aanslagen in de Verenigde Staten, Spanje en Groot-Brittannië en de moord op Theo van Gogh hebben een extra impuls gegeven aan deze beweging. Een groot deel van de veiligheidsmaatregelen is echter ruim voor 2001 voorbereid of zelfs van kracht geworden.

De studie schetst ten slotte kort de te verwachten ontwikkelingen voor de komende jaren, waaronder de invoering van het burgerservicenummer en het biometrisch paspoort, en een verdere uitbreiding van de bevoegdheden van de inlichtingendiensten.

Trends

Uit het overzicht van de opsporings- en veiligheidsmaatregelen komt een aantal trends naar voren die zich de komt jaren lijken voort te zetten:

- Het opsporingsonderzoek breidt zich steeds vaker uit tot personen op wie zelf geen verdenking rust, in de omgeving van verdachten.
- Het onderzoek is steeds vaker verkennend van karakter, waarbij op basis van risicoprofielen potentieel verdachte groepen worden gevolgd.
- Wettelijke beperkingen voor het gebruik van bepaalde opsporingsmethoden worden verlicht of weggenomen.
- Opsporingsdiensten krijgen, zowel juridisch als technologisch, steeds meer mogelijkheden om (zelfstandig) onderzoek te verrichten.
- Opsporingsdiensten hebben in toenemende mate toegang tot informatie van overige (semi)overheidsdiensten die voor andere dan opsporingsdoeleinden is verzameld.
- Opsporingsdiensten dwingen steeds vaker andere partijen om mee te werken aan onderzoek.

Voor de 'gewone', niet-verdachte burger zijn vooral twee ontwikkelingen van belang: de inzet van nieuwe technologieën (DNA-onderzoek, camera's, *datamining*, koppeling van bestanden) en het gebruik dat politie, justitie en de veiligheidsdiensten maken van de voortschrijdende digitalisering van administraties van overheden en private organisaties. Als daarmee al niet voor het eerst informatie over tot dan toe onbereikbare dimensies van de persoonlijke levenssfeer kan worden vergaard, kan het in elk geval gemakkelijker en op veel grotere schaal dan daarvoor. Personen kunnen dan ook sneller dan voorheen object van onderzoek worden, dikwijls zonder dat zij daar enige weet van hebben.

Maatschappelijke reacties

Een aantal veiligheidsmaatregelen (maar lang niet alle) heeft maatschappelijke reacties opgeroepen. Hierin wordt vooral gewezen op de mogelijk problematische inpasbaarheid van de maatregelen binnen de uitgangspunten van het strafrecht en op de beperkte transparantie van de (Europese) politieke besluitvorming. Drie dingen vallen op:

· Bw. Studie 49 23-01-2007 14:39 Pagina 11

- De discussie richt zich vrijwel zonder uitzondering op afzonderlijke maatregelen en niet op hun onderlinge samenhang.
- De discussie wordt vooral in beperkte, juridische kring gevoerd.
- De privacy van burgers speelt nauwelijks een rol van betekenis in het debat.

Aandacht voor privacy

Om beter zicht te krijgen op de gevolgen van de veiligheidsmaatregelen voor de privacy van burgers, gaat de studie nader in op de betekenis van het privacybegrip. De auteurs kenmerken privacy als de principiële beschermwaardigheid van de persoonlijke levenssfeer. Deze beschermwaardigheid is echter niet absoluut. Inbreuken op de privacy zijn toegestaan, mits daar goede redenen voor kunnen worden gegeven.

Hoe de afweging tussen privacy en andere belangen moet worden gemaakt, hangt af van de precieze context. Daarbij dienen diverse zorgvuldigheidscriteria in acht te worden genomen. De vereiste afweging vraagt echter vóór alles om een open discussie, waarin alle voor- en tegenargumenten aan bod komen. Bedacht moet worden dat inbreuken op de privacy persoonlijke rechten of belangen schaden en derhalve bijzondere rechtvaardiging vergen.

Een agenda voor debat

In het huidige politieke en maatschappelijke debat over de opsporings- en veiligheidsmaatregelen ontbreekt het aan een dergelijke openheid. Daardoor is er ook geen sprake van een doordachte oordeelsvorming over de veiligheidsmaatregelen en over hun gevolgen voor de privacy van burgers. Zeker gezien de nog steeds voortgaande bevoegdheidsuitbreidingen van politie, justitie en inlichtingendiensten bestaat er meer dan ooit behoefte aan discussie hierover.

Het debat moet in ieder geval aandacht besteden aan de volgende onderwerpen:

- Essentieel is dat naar het cumulatieve effect van de opsporings- en veiligheidsmaatregelen wordt gekeken. Afzonderlijke maatregelen moeten mede beoordeeld worden op de mate waarin ze de privacyaantasting van andere maatregelen versterken.
- Hierbij aansluitend is aandacht nodig voor de voortschrijdende digitalisering van gegevensbestanden. De bestaande bevoegdheden om gegevens bij derden te vorderen, geven opsporingsdiensten nu al welhaast onbeperkte toegang tot alle informatie die over burgers verkrijgbaar is.
- De effectiviteit van de veiligheidsmaatregelen behoeft tevens aandacht. Vergroten de maatregelen de veiligheid daadwerkelijk? Dit is van belang vanwege de inbreuk op de privacy die ze met zich meebrengen en de zorgvuldige argumentatie die nodig is om dergelijke inbreuken te rechtvaardigen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 12

- Meer openheid is nodig over de (Europese) procedures via welke bevoegdheidsuitbreidingen tot stand komen. Deze procedures kenmerken zich door een grote mate van ondoorzichtigheid die burgers buiten de discussie sluit.
- De beperkte kring waarin het debat over veiligheidsmaatregelen plaatsvindt, moet worden opengebroken. Verbreding van het debat is nodig om burgers hierin een stem te geven. Het gaat tenslotte om hun veiligheid en privacy.

· Bw. Studie 49 23-01-2007 14:39 Pagina 13


Cameratoezicht

· Bw. Studie 49 23-01-2007 14:39 Pagina 15

1 Inleiding

Sinds enige jaren staat de bestrijding van terrorisme en zware criminaliteit hoog op de nationale en internationale politieke agenda's. De bevoegdheden van politie, justitie en veiligheidsdiensten zijn in hoog tempo uitgebreid. Wetenschappelijke en publieke discussies over de consequenties die deze uitbreidingen hebben voor de grondrechten, in het bijzonder de privacy van de burger, worden hoofdzakelijk gevoerd naar aanleiding van afzonderlijke maatregelen. Naar het totaaleffect wordt nauwelijks gekeken. Studies hierover zijn zeldzaam of beperken zich tot een bepaald type maatregelen. Vermeulen (2005) kijkt bijvoorbeeld uitsluitend naar vijf recente wetten en wetsvoorstellen in het kader van de terreurbestrijding. In meer journalistieke bijdragen hebben Brouwer (2006) en Spaink (2006) een eerste aanzet gegeven tot een schets van het cumulatieve effect van veiligheidsmaatregelen.

Vaak wordt verder voetstoots aangenomen dat de uitbreidingen van de bevoegdheden van opsporingsdiensten zijn begonnen na 11 september 2001, de dag dat de Verenigde Staten werden getroffen door grootscheepse terroristische aanslagen. Een zelfs maar oppervlakkige blik op de data van inwerkingtreding van verschillende maatregelen, leert echter dat enkele belangrijke bevoegdheidsuitbreidingen ruim voor 11 september 2001 zijn ingevoerd. Andere zijn lang voor die datum voorbereid en opgesteld.

Deze studie is gericht op het cumulatieve effect van de veiligheidsmaatregelen. Tevens wordt ingegaan op hun achtergronden. Inzicht in het cumulatieve effect is van belang voor zowel een zorgvuldige beoordeling van de afzonderlijke maatregelen, als voor een doordachte afweging van de opsporings- of preventiebelangen tegen de privacy van burgers. In het licht van het cumulatieve effect kan het beeld immers aanzienlijk anders uitvallen dan wanneer uitsluitend naar de afzonderlijke maatregelen wordt gekeken.

Daartoe worden de opsporings- en veiligheidsmaatregelen in kaart gebracht die de afgelopen jaren zijn ingevoerd en die voor de komende jaren nog te verwachten zijn. Bijzondere aandacht gaat uit naar de consequenties daarvan voor de privacy van burgers. Er wordt gekeken naar zowel de afzonderlijke maatregelen, als naar hun gezamenlijke effect.

Vanuit de vooronderstelling dat technologische ontwikkelingen grote invloed hebben op de invoering of uitbreiding van opsporingsbevoegdheden, komen in deze studie vooral technologiegerelateerde ontwikkelingen aan bod. Veel maatregelen hangen immers direct of indirect

· Bw. Studie 49 23-01-2007 14:39 Pagina 16

samen met de introductie van nieuwe technologieën. Denk bijvoorbeeld aan de invoering van het biometrisch paspoort, de instelling van een databank met DNA-profielen of het gebruik van hoogwaardige afluisterapparatuur of zogeheten slimme camera's.

Een tweede afbakening van de studie is de nadruk die wordt gelegd op de gevolgen voor de privacy van de 'gewone' burger. Opsporings- en veiligheidsdiensten richten hun inspanningen steeds vaker niet alleen op verdachten, maar ook op onverdachte personen. Burgers kunnen er daardoor steeds minder van op aan dat ze niets te vrezen hebben en wel buiten schot zullen blijven.

Deze afbakeningen betekenen dat een controversieel onderwerp als het voorgenomen 'apologieverbod', een verbod op de verheerlijking van terroristen en hun daden, geen deel uitmaakt van het onderzoek.[1] Het apologieverbod is immers niet gerelateerd aan het gebruik van bestaande of nieuwe technologieën. Evenmin wordt aandacht besteed aan het zogenoemde 'verstoren', het door de politie stelselmatig extra controleren en bezoeken van personen die van terroristische of criminele handelingen worden verdacht.[2] Dit heeft weliswaar grote consequenties voor de privélevens van de betrokkenen, maar het is een maatregel die zich richt op specifieke personen en groepen waartegen concrete verdenkingen bestaan. In deze studie gaat het daarentegen om bevoegdheden en maatregelen die in principe alle burgers raken.

Om beter zicht te krijgen op de gevolgen van de veiligheidsmaatregelen voor de privacy van burgers, zal tevens nader worden ingegaan op het privacybegrip. Dit begrip zal in deze studie aanvankelijk relatief open en intuïtief worden gebruikt. Daarmee wordt aangesloten bij wat gangbaar is in het alledaagse taalgebruik en in de discussies over de maatregelen en bevoegdheden die het onderwerp van deze studie vormen. In het slothoofdstuk zal uitvoerig worden ingegaan op het privacybegrip. Dit is nodig omdat privacyoverwegingen in de genoemde discussies gaandeweg steeds verder naar de achtergrond zijn verdwenen. Dat hangt samen met de vaagheid van het begrip, alsook met een vaak gesuggereerde kentering in de opvattingen van de burger. De burger zou de afgelopen jaren minder gewicht zijn gaan toekennen aan privacy en meer aan veiligheidsbelangen.

Leeswijzer

Het eerste deel van deze studie geeft een overzicht van de ontwikkelingen op het gebied van veiligheid en opsporing uit de afgelopen jaren en die in de nabije toekomst zijn te verwachten.

Hoofdstuk 2 begint met een kort overzicht van opsporingsbevoegdheden zoals die golden tot aan het begin van de jaren negentig van de vorige eeuw. Vervolgens worden de ontwikkelingen uit de laatste vijftien jaar beschreven en wordt stilgestaan bij de omstandigheden die

· Bw. Studie 49 23-01-2007 14:39 Pagina 17

aanleiding gaven tot deze ontwikkelingen. Hoofdstuk 3 gaat in op de maatregelen die Nederland in de komende jaren nog kan verwachten. Daarbij gaat het zowel om concrete maatregelen die al praktisch voor invoering klaarliggen, als om maatregelen die in de nabije toekomst mogelijk worden, bijvoorbeeld door nieuwe technologische ontwikkelingen.

Het tweede deel van het onderzoek heeft een evaluatief karakter. In hoofdstuk 4 komen de in hoofdstuk 2 besproken wetten weer terug, in die zin dat nu uitvoerig wordt ingegaan op de maatschappelijke reacties die ze opriepen. Ook wordt gekeken welke kenmerken de reacties gemeen hebben en wat dit zegt over de stand van het publieke debat in Nederland over deze kwesties. In hoofdstuk 5 wordt ten slotte geprobeerd deze bevindingen te vertalen naar een agenda voor het debat over veiligheidsmaatregelen. Belangrijk daarvoor is dat niet langer uitsluitend naar de privacyeffecten van de afzonderlijke maatregelen wordt gekeken, maar ook naar de optelsom van alle effecten en maatregelen tezamen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 18

· Bw. Studie 49 23-01-2007 14:39 Pagina 19

Deel I
De ontwikkelingen in kaart gebracht

· Bw. Studie 49 23-01-2007 14:39 Pagina 21

2 Toenemende controle

Een van de doelen van deze studie is in kaart te brengen welke (technologiegerelateerde) opsporingsbevoegdheden de laatste jaren zijn verruimd en welke nieuwe maatregelen zijn genomen. Alvorens dit te doen wordt een kort overzicht gegeven van de opsporingsbevoegdheden zoals die golden tot aan het begin van de jaren negentig van de vorige eeuw. Daarna komen de ontwikkelingen van de laatste vijftien jaar aan bod en wordt stilgestaan bij de context waarin ze tot stand zijn gekomen.

2.1 Nederland privacyparadijs: 1960-1985

Vanaf het einde van de jaren zestig tot ver in de jaren tachtig van de twintigste eeuw is Nederland op het gebied van de preventie en bestrijding van de misdaad een toonbeeld van rust en stabiliteit. Bezien in het licht van de situatie aan het begin van de 21ste eeuw – wanneer terreur een dominant politiek thema is en regelmatig aanleiding geeft voor aanscherping van het veiligheidsbeleid – mag dit verwondering wekken. In de jaren zeventig en tachtig wordt Nederland immers, net als andere Europese landen, geplaagd door terreur van zowel binnenlandse als buitenlandse groeperingen. IJveraars voor een zelfstandige republiek op de Zuid-Molukken en het Japanse Rode Leger voeren gijzelingsacties uit, links-radicalen van de Revolutionaire Anti-Racistische Actie (RaRa) plegen bomaanslagen en indirect krijgt Nederland te maken met het geweld van de Duitse Rote Armee Fraktion (RAF) en de Italiaanse Brigate Rosse. Toch is er in die tijd nauwelijks aanleiding de opsporing aan te scherpen en de privélevens van burgers strenger te controleren.

Drie factoren spelen hierbij mogelijk een rol. Ten eerste gaat het bij de Duitse en Italiaanse terreurgroepen om terroristen die hun toevlucht in Nederland zoeken, maar die het land zelf goeddeels met rust laten. Ten tweede lijkt het erop dat politie en justitie in het geval van de binnenlandse terreurorganisaties goed weten om welke groepen het gaat. Om die reden hebben ze mogelijk geen behoefte aan ruimere opsporings- of verkenningsmogelijkheden. Ten derde kan de terughoudende opstelling te maken hebben met het belang dat in deze tijd wordt gehecht aan privacy in het algemeen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 22

2.1.1 Politie en justitie

In de jaren zestig, zeventig en tachtig beschikken opsporingsdiensten vooral over aloude bevoegdheden als huiszoeking, observatie en het bevel tot uitlevering van voorwerpen. Er bestaan slechts enkele specifiek techniekgerelateerde bevoegdheden, en wel voor het onderzoek van telefonie (Koops, 2002, Smits, 2006). Al in 1926 was een bevoegdheid ingevoerd om inlichtingen te vorderen van de telefoonaanbieder over gevoerde gesprekken (wat tegenwoordig wordt aangeduid als 'verkeersgegevens').[3] Deze bevoegdheid was een min of meer terloops bijproduct. Ze werd ingesteld als aanhangsel bij de bevoegdheid om bij de posterijen verkeersgegevens op te vragen over post, en is nergens toegelicht door de wetgever en evenmin bediscussieerd in het parlement.[4] Begin jaren zeventig wordt aan deze bevoegdheid de beperkende voorwaarde verbonden dat het slechts mag gaan om gesprekken waaraan vermoedelijk een verdachte deelneemt.

In de jaren zestig ontstaat maatschappelijke onrust door de opkomst van richtmicrofoons, onder andere door advertenties die 'geluidsgeweren' aanprijzen om geluid 1 miljoen keer te versterken. Het tumult is voor de wetgever aanleiding om voor het eerst een wet ter bescherming van de privacy uit te vaardigen.[5] Daarbij worden diverse strafbepalingen ingevoerd rond het afluisteren van gesprekken en telefonie, maar ook nieuwe bevoegdheden geschapen.[6] Zo krijgt justitie in 1971 de bevoegdheid om telefoongesprekken af te luisteren of op te nemen waarvan het vermoeden bestaat dat de verdachte eraan deelneemt.[7] De wetgever ziet het als een ingrijpende bevoegdheid. De verwachting wordt uitgesproken dat de bepalingen waarschijnlijk geen veelvuldige toepassing zullen vinden.[8]

Tegelijkertijd wordt besloten om justitie geen bevoegdheid te geven om met richtmicrofoons direct gesprekken af te luisteren. Van de ene kant acht men dit niet nodig; van de andere kant vindt men dat het afluisteren van privégesprekken bijzonder diep in de persoonlijke levenssfeer doordringt.[9] Uitdrukkelijk stelt men echter dat dit in de toekomst, bijvoorbeeld bij een grote toename van zware, georganiseerde criminaliteit, anders zal kunnen worden.[10]

In de jaren tachtig dient zich voor het eerst de mogelijkheid van DNA-onderzoek aan. In concreto wordt het mogelijk een DNA-profiel uit lichaamsmateriaal vast te stellen en te vergelijken met een DNA-profiel van bij een misdrijf gevonden sporenmateriaal. Deze methode is ontwikkeld in het Verenigd Koninkrijk en wordt ook toegepast in Nederland. Dat kan echter alleen met vrijwillige medewerking van de verdachte: verplichte afname van lichaamsmateriaal voor DNA-onderzoek wordt door de rechtspraak als te ingrijpend afgekeurd.[11]

· Bw. Studie 49 23-01-2007 14:39 Pagina 23

2.1.2 Inlichtingendiensten

Voor de inlichtingen- en veiligheidsdiensten bestaan lange tijd nauwelijks specifieke wettelijke bevoegdheden (Van Buuren, Koops & Wagenaar, 2004, p. 194-196). Sinds 1949 regelt een vertrouwelijk Koninklijk Besluit het bestaan, de taken en de verantwoordelijkheden van de Binnenlandse Veiligheidsdienst (BVD), de voorloper van de huidige Algemene Inlichtingen- en Veiligheidsdienst, AIVD. Dit besluit wordt pas in 1972 openbaar. De bevoegdheidsomschrijving in dit besluit blijkt summier. Het regelt bijvoorbeeld dat de BVD zich tot andere overheidsdiensten kan wenden met het verzoek tot verstrekking van gegevens, waaronder verkeersgegevens van de PTT.[12]

Voor afluisteren door de BVD wordt door middel van een zogenoemde strafuitsluitingsgrond een regeling getroffen waardoor de dienst verdergaande bevoegdheden krijgt dan justitie.[13] Een belangrijke reden hiervoor is dat staatsgevaarlijke activiteiten zich veelal in het verborgene afspelen en dat er geen alternatieven voorhanden zijn om voor de staatsveiligheid wezenlijke gegevens te verkrijgen.[14] Voor toepassing van deze bevoegdheden heeft de BVD overigens wel toestemming nodig van de minister-president en de ministers van Justitie en Binnenlandse Zaken. Als het om aftappen van telecommunicatie gaat moet ook de minister van Verkeer en Waterstaat toestemming geven.

2.2 Verlies van onschuld: 1985-2006

Vormt in de jaren zeventig en tachtig respect voor de privacy van burgers voor de wetgever een belangrijke reden om vergaande opsporingsbevoegdheden af te wijzen, vanaf de jaren negentig lijkt privacy steeds minder gewicht in de schaal te leggen. Tegelijkertijd nemen de bevoegdheden stormachtig toe. In deze paragraaf wordt ingegaan op de afzonderlijke maatregelen die in dit verband relevant zijn. De maatregelen zijn thematisch geclusterd en worden zo veel mogelijk chronologisch behandeld. Eerst zal echter kort iets worden gezegd over de van kracht zijnde wetgeving op het gebied van privacybescherming.

2.2.1 Privacywetgeving

De Wet persoonsregistraties (WPR) en de Wet bescherming persoonsgegevens (WBP) zijn van groot belang binnen het geheel van de privacywetgeving in Nederland.

De WPR treedt in 1988 in werking en wordt in 2001 vervangen door de WBP.[15] De WPR stelt de regels vast voor de omgang met persoonsgegevens. De WBP is tot stand gekomen als implementatie van de Europese Richtlijn van 1995 over de bescherming van persoonsgegevens.[16] Deze richtlijn introduceert een nieuw en aan de tijd aangepast begrippenkader en maakt herziening van de WPR nodig. Wat het normerende kader betreft lopen de WPR en de WBP echter niet ver uiteen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 24

Kenmerkend zijn de volgende uitgangspunten:
- de betrokkenen moeten worden geïnformeerd over het gebruik van hun gegevens,
- de betrokkenen moeten daarin toestemmen,
- de betrokkenen moeten in staat worden gesteld na te gaan welke gegevens over hen geregistreerd zijn,
- de betrokkenen hebben het recht onjuistheden in die gegevens te laten corrigeren,
- de gegevens mogen alleen worden gebruikt voor een gespecificeerd doel (doelbinding),
- de gegevens mogen slechts onder zeer beperkte voorwaarden worden verstrekt aan derden waarbij voor gevoelige gegevens (onder meer ras, sekse, gezondheidstoestand) strengere voorwaarden gelden dan voor andere.

Tevens bevatten de WPR en de WBP bepalingen die uitzonderingen op deze uitgangspunten mogelijk maken. Uitzonderingen zijn onder meer toegestaan als deze kunnen bijdragen aan:
- de voorkoming, opsporing of vervolging van strafbare feiten,
- de bescherming van belangrijke economische en financiële belangen van de staat en andere openbare lichamen, en
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

In deze gevallen berust de verantwoordelijkheid voor de beslissing om gegevens over te dragen bij de instelling die de desbetreffende registratie voert. Er kunnen echter wettelijke verplichtingen van kracht zijn om gegevens aan derden (bijvoorbeeld politie, justitie of veiligheidsdiensten) over te dragen. In dergelijke gevallen ligt de verantwoordelijkheid voor de overdracht van de gegevens niet bij degene die de registratie voert, maar bij politie, justitie of de veiligheidsdienst.

Deze uitzonderingsbepalingen zijn van groot belang. De bevoegdheidsuitbreidingen die hieronder worden besproken stellen namelijk politie, justitie en veiligheidsdiensten in staat om gegevens te verzamelen en te bewerken waarover zij *zonder* die bepalingen niet, of alleen met vrijwillige medewerking van de houders van de registraties zouden kunnen beschikken.

2.2.2 DNA-onderzoek

In 1990 keurt de Hoge Raad de gedwongen afname van lichaamsmateriaal nog af als een niet-wettige inbreuk op de lichamelijke integriteit.[17] De wetgever besluit in reactie hierop voor justitie de bevoegdheid te creëren voor het verrichten van DNA-onderzoek. Deze wet treedt op 1 september 1994 in werking.[18] Sindsdien mag de rechter-commissaris in het geval van zware misdrijven (grofweg misdrijven met zes jaar of meer gevangenisstraf) en dringende noodzakelijkheid, het bevel geven om bloed af te nemen van een verdachte.

· Bw. Studie 49 23-01-2007 14:39 Pagina 25

Met het voortschrijden van de DNA-technologie – waardoor ook uit wangslijm voldoende DNA-materiaal kan worden gehaald voor een DNA-profiel – wordt de bevoegdheid verruimd. De wetgever acht het afnemen van wangslijm een kleinere inbreuk op de lichamelijke integriteit dan het afnemen van bloed.[19] Sinds 2001 mag ook de officier van justitie het bevel geven tot afname van lichaamsmateriaal voor DNA-onderzoek. Bovendien mag DNA-onderzoek bij meer misdrijven worden uitgevoerd dan voorheen (grofweg misdrijven met vier jaar of meer gevangenisstraf).[20]

De mogelijkheden om DNA-onderzoek toe te passen zijn sindsdien ook nog in twee andere opzichten uitgebreid. In de eerste plaats is de bevoegdheid geschapen om uit DNA-materiaal dat bij een misdrijf is gevonden uiterlijk waarneembare kenmerken af te leiden van de verdachte.[21] Door het afleiden van geslacht en ras (dat wil zeggen de geografische herkomst) – en wellicht in de toekomst kenmerken als haarkleur, kleur ogen en lengte – kan een daderprofiel of signalement worden opgesteld. Hoewel het wetsvoorstel ruim een maand na 11 september 2001 wordt ingediend (en de wet in 2003 van kracht wordt) is de aanleiding niet gelegen in terrorismebestrijding, maar veeleer in de wens onopgeloste moord- en zedenzaken opnieuw te onderzoeken.

De tweede uitbreiding betreft het aanleggen en vullen van een DNA-databank.[22] In deze databank worden sinds de jaren negentig profielen bewaard van veroordeelde personen van wie tijdens het opsporingsonderzoek DNA-materiaal is afgenomen. Omdat bij lang niet alle strafzaken DNA-onderzoek nodig of mogelijk is, blijft het aantal DNA-profielen in de databank relatief beperkt. Dit verandert door de wetswijziging. Door standaard een DNA-profiel op te slaan van ieder die wordt veroordeeld tot gevangenis- of taakstraf voor een misdrijf waarop een straf *mogelijk* is van vier jaar of meer (ongeacht of een straf van die omvang feitelijk is toebedeeld), breidt het aantal opgeslagen profielen zich aanzienlijk uit. Sinds de inwerkingtreding is het aantal persoonsprofielen in de DNA-databank bijna verviervoudigd, van circa zesduizend tot circa 24.000.[23] Indien de verdenking vervalt of in geval van vrijspraak dient het Nederlands Forensisch Instituut (NFI), dat de databank beheert, het desbetreffende DNA-profiel uit de databank te verwijderen.

De wet is in 2004 in werking getreden, maar al voor september 2001 aangekondigd.[24] Ook hier vormen terreur en georganiseerde misdaad niet de aanleiding voor de bevoegdheidsuitbreiding. Nadrukkelijk worden woninginbraken als voorbeeld genoemd van een misdrijf dat de nieuwe wet zal helpen oplossen en voorkomen.[25]

2.2.3 Cameratoezicht

Het gebruik van camera's om toezicht te houden in het publieke domein is in Nederland een betrekkelijk nieuw fenomeen. Rond 1999 begonnen lokaal de eerste experimenten[26] en sindsdien is het gebruik van camera's

· Bw. Studie 49 23-01-2007 14:39 Pagina 26

in de openbare ruimte alleen maar toegenomen. Medio 2006 lijkt de camera bijna een vast onderdeel te zijn van de inrichting van straten en pleinen.

De Wet cameratoezicht, in werking getreden in januari 2006, reguleert het gebruik van camera's op openbare plaatsen.[27] De gemeenteraad kan de burgemeester de bevoegdheid verlenen om, in het kader van de handhaving van de openbare orde, camera's te laten plaatsen. De burgemeester bepaalt de duur van de plaatsing en wijst de openbare plekken aan waar de camera's zullen worden geplaatst. Ook stelt hij de periode vast waarin de geregistreerde beelden rechtstreeks worden bekeken. Het cameratoezicht moet voor burgers kenbaar worden gemaakt, bijvoorbeeld door het aanbrengen van borden in het desbetreffende gebied. De camerabeelden vallen onder de Wet politieregisters en kunnen worden gebruikt voor de opsporing of vervolging van strafbare feiten.[28]

Ook in de private en de semiprivate sector is het gebruik van camera's enorm toegenomen. Particulieren en bedrijven hanteren camera's steeds vaker voor de veiligheid rondom hun pand, hun terrein of ter bescherming van private eigendommen. Hieronder valt ook het gebruik van camera's door bedrijven als de Nederlandse Spoorwegen en andere vervoersbedrijven. De Wet cameratoezicht is hierop niet van toepassing.[29] Deze vormen van cameratoezicht vallen onder de Wet bescherming persoonsgegevens. Overeenkomstig de uitzonderingscondities waarin deze wet voorziet kunnen de eigenaren van de camera's worden verplicht hun beelden af te staan aan politie, justitie of veiligheidsdiensten.

Het Wetboek van Strafrecht bevat een strafbaarstelling van heimelijk cameratoezicht die per 1 januari 2004 is uitgebreid. Daarmee wordt beoogd te voorkomen dat op ongecontroleerde wijze gebruik kan worden gemaakt van verborgen camera's. Dit sluit echter niet uit dat politie en inlichtingendiensten voor hun taakuitoefening verborgen camera's mogen gebruiken.

2.2.4 Computeronderzoek

De opkomst van de personal computer in de jaren tachtig roept de vraag op of de wetgeving moet worden aangepast aan de mogelijkheden van computercriminaliteit. In opdracht van de minister van Justitie voert de in 1985 ingestelde Commissie computercriminaliteit een 'leemteanalyse' uit, waarbij niet alleen het Wetboek van Strafrecht maar ook het Wetboek van Strafvordering wordt doorgelicht op de noodzaak voor nieuwe bepalingen.[30] Dit is de aanzet voor het traject dat leidt tot de Wet computercriminaliteit van 1993.

· Bw. Studie 49 23-01-2007 14:39 Pagina 27

Deze wet regelt het aftappen van de telecommunicatie en de justitiële bevoegdheden voor onderzoek in computersystemen (Simmelink & Wiemans, 1990).[31] De bevoegdheden houden onder meer in dat ook online onderzoek mag worden verricht in systemen die zich elders dan op de plaats van de doorzoeking bevinden. De Wet computercriminaliteit II, die in september 2006 in werking is getreden, past de bestaande wetgeving aan met hogere straffen voor computercriminaliteit, uitbreiding van de strafbaarstelling van enkele delicten en aanscherping van de bevoegdheden van justitie en politie.

De nieuwe wet gaat in op de vernietiging van computergegevens, medewerking aan de ontsleuteling van met encryptie bewerkte gegevens, het onderscheid tussen 'opgeslagen' en 'stromende' gegevens, onderzoek van e-mail en opsporingsonderzoek op openbare computernetwerken.[32] De belangrijkste uitbreiding is dat het nu ook mogelijk wordt om communicatie via private netwerken (bijvoorbeeld van bedrijfsnetwerken) te onderscheppen. Dat betekent dat ook bedrijfsgeheimen, vertrouwelijke communicatie en gegevens van werknemers die gebruikmaken van het desbetreffende netwerk voorwerp van onderzoek kunnen worden.[33]

2.2.5 Bijzondere opsporingsbevoegdheden

Als rechtstreeks uitvloeisel van de parlementaire enquête naar opsporingsmethoden (de Commissie-Van Traa), treedt begin 2000 de Wet bijzondere opsporingsbevoegdheden (Wet BOB) in werking. Deze wet heeft betrekking op een breed scala aan opsporingsmethoden, waaronder observatie, infiltratie, pseudokoop, inkijkoperaties, inzetten van informanten, direct afluisteren en tappen.[34] De Wet BOB beoogt de normen vast te stellen waaraan opsporingsonderzoeken moeten voldoen, zodat ze ook beter controleerbaar worden. De wet geeft aan dat de bijzondere opsporingsbevoegdheden uitsluitend mogen worden ingezet voor de opsporing en strafrechtelijke afhandeling van strafbare feiten. Andere doeleinden, zoals verbetering van de informatievoorziening van de politie of de ontmanteling van een criminele organisatie zonder dat dit leidt tot strafrechtelijke vervolging, vallen erbuiten. Ook moet het desbetreffende misdrijf een ernstige inbreuk op de rechtsorde vormen.

Volgens de Wet BOB is het voortaan de officier van justitie die de leider is van het opsporingsonderzoek. Hij neemt ook de beslissing om bijzondere opsporingsbevoegdheden te gebruiken, iets wat tot dan toe was voorbehouden aan de rechter-commissaris. De officier van justitie draagt tevens zorg voor het bewaren en vernietigen van de aldus verkregen gegevens.

Een andere belangrijke verandering is dat, indien relevant voor het opsporingsonderzoek, de bijzondere bevoegdheden mogen worden ingezet tegen zowel verdachten als niet-verdachten. Zo is bij het aftappen van telecommunicatie de voorwaarde komen te vervallen dat de

· Bw. Studie 49 23-01-2007 14:39 Pagina 28

verdachte zelf aan de communicatie moet deelnemen. Het gevolg is dat justitie in een bredere kring rond een verdachte de communicatie kan aftappen en dat niet-verdachte burgers sneller dan voorheen in het vizier komen.

Wel is het zo dat de wet de zogeheten notificatieplicht uitbreidt tot alle bijzondere opsporingsbevoegdheden. Deze verplichting houdt in dat, zodra het onderzoeksbelang het toelaat, de officier van justitie personen die onderwerp zijn van een opsporingsonderzoek daarover informeert. Zo wordt voorkomen dat wanneer het onderzoek niet leidt tot een strafproces, de toepassing van de bijzondere opsporingsbevoegdheden geheim blijft.

De bijzondere opsporingsbevoegdheden kunnen niet alleen worden toegepast om een concreet misdrijf op te lossen, maar ook bij onderzoeken naar de georganiseerde misdaad. In dit verband is het van belang te wijzen op de mogelijkheid van een verkennend onderzoek. Dat houdt in dat opsporingsdiensten behalve uit de politieregisters ook uit andere registers, zoals van de Kamer van Koophandel, gegevens kunnen verzamelen, combineren en analyseren – ook van niet-verdachten.[35]

Soortgelijke bevoegdheden komen aan de orde in de Wet op de inlichtingen- en veiligheidsdiensten (WIV) van 2002. Hierin worden bevoegdheden van de inlichtingen- en veiligheidsdiensten geregeld met betrekking tot onder meer het aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht.[36] De desbetreffende gegevens dienen daarbij in beginsel geheim te blijven. Hoewel de wet de mogelijkheid van kennisneming regelt, wordt de inwilliging van een verzoek tot kennisneming afhankelijk gemaakt van het belang van de informatie voor de nationale veiligheid.

2.2.6 Identificatieplicht

Op 1 januari 2005 is de Wet op de identificatieplicht ingevoerd. Deze wet verplicht iedereen vanaf 14 jaar om een identiteitsbewijs te tonen op verzoek van politie of toezichthouders. Het gaat om een functionele identificatieplicht. De politie mag niet om een identiteitsbewijs vragen alleen maar om te zien of iemand het bij zich heeft.[37]

2.2.7 Koppeling bestanden

Vanaf het einde van de jaren tachtig koppelt de overheid in toenemende mate de bestanden die zijzelf bijhoudt en de bestanden van uitvoeringsorganisaties zoals de sociale dienst voor opsporingsdoeleinden. De koppeling wordt mogelijk gemaakt door de voortschrijdende informatietechnologie en vergemakkelijkt door het gebruik van een uniek persoonsnummer. In eerste instantie wordt om de belastinginning te vereenvoudigen een fiscaal nummer ingevoerd. Al snel wordt dit nummer verbonden met het socialezekerheidsnummer dat uitkerings-

· Bw. Studie 49 23-01-2007 14:39 Pagina 29

instanties en zorginstellingen gebruiken om hun klanten te identificeren (Van Dijk, 1993). Dit 'sofinummer' maakt het voor het eerst mogelijk om te controleren of iemand behalve een werkloosheidsuitkering ook inkomen uit werk ontvangt, door in de klantenadministraties van de ziekenfondsen de verzekeringsgrondslag voor de betrokken persoon op te zoeken.

Omdat gemeenten het sofinummer gaan gebruiken voor de Gemeentelijke Basisadministratie persoonsgegevens (GBA) – het vroegere bevolkingsregister, waarin de persoonsgegevens zijn opgenomen van iedereen die rechtmatig in Nederland verblijft – en het nummer op gemeentelijke identiteitskaarten verschijnt, ontwikkelt het zich al snel tot een algemeen identificatienummer. Het doel van de GBA is overheidsinstanties te voorzien van persoonsgegevens die nodig zijn voor de uitvoering van hun taken, zoals het verstrekken van uittreksels, vergunningen, rijbewijzen en paspoorten. Hiervoor zijn niet alleen naam- en adresgegevens nodig, maar bijvoorbeeld ook gegevens over huwelijkse staat, nationaliteit, ouders en kinderen.

2.2.8 Inschakelen van derden

Vanaf het midden van de jaren negentig valt een groeiende tendens waar te nemen om derden in te schakelen bij opsporingsactiviteiten. Deze tendens komt voort uit een groeiende behoefte van opsporings- en veiligheidsdiensten aan informatie over uiteenlopende kenmerken van de burgers. Daarnaast speelt de informatisering van de jaren negentig een belangrijke rol, alsook de privatiserings- en verzelfstandigingsgolf van de jaren tachtig en negentig. De laatstgenoemde ontwikkeling maakt het noodzakelijk om de verhouding tussen overheidsinstanties zoals politie en justitie en de nieuwe verzelfstandigde of geprivatiseerde organisaties te regelen. Dit geldt ook voor de overdracht van informatie tussen die verzelfstandigde organisaties en politie en justitie.

2.2.9 Aftappen telecommunicatie

Tot de jaren negentig was het technisch gezien nauwelijks een probleem om telecommunicatie af te tappen. De privatisering en liberalisering van allerlei telefoniediensten en technische ontwikkelingen brengen hier verandering in. Om deze reden is een verplichting ingevoerd voor aanbieders van openbare telecommunicatie om hun netwerken en diensten aftapbaar te maken. Deze verplichting is in 1994 ingevoerd voor mobiele telefonie,[38] in 1998 voor alle vormen van openbare telecommunicatie[39] en sinds 2001 geldt ze ook voor internetproviders.[40] De aanbieders moeten ervoor zorgen dat hun telecommunicatie vanaf het moment van introductie technisch aftapbaar is.

Daarnaast zijn de aanbieders verplicht gehoor te geven aan bevelen van justitie en veiligheidsdiensten tot aftappen, en tot overhandigen van gebruikersgegevens, dat wil zeggen naam- en nummergegevens.

· Bw. Studie 49 23-01-2007 14:39 Pagina 30

Sinds 2004 is daar de verplichting bijgekomen mee te werken aan bevelen tot het overhandigen van verkeersgegevens.[41] Verkeersgegevens bevatten geen inhoudelijke gespreksinformatie, maar vertellen iets over de route waarlangs communicatie heeft plaatsgevonden. Het gaat dan bijvoorbeeld om de locatie van een mobiele telefoon, gebelde nummers, gespreksduur, tijdstippen waarop is gebeld of oproepen zijn ontvangen, geadresseerden en onderwerpregels van e-mails en bezochte websites.

Sinds enige tijd bestaat een databank voor alle telefoonnummers in Nederland, zowel vast als mobiel. Bij het Centraal Informatiepunt Opsporing Telecommunicatie (CIOT) kunnen opsporingsambtenaren bij elk telefoonnummer de namen en adressen van de eigenaren verkrijgen.[42] Er is gesuggereerd dat het ministerie van Justitie tevens zou werken aan een databank met IP-nummers, naam- en adresgegevens en wellicht ook eventuele e-mailadressen van alle Nederlanders.[43] Het is onduidelijk of een dergelijk bestand al werkelijk is ontwikkeld.

Met de inwerkingtreding van de Wet vorderen gegevens telecommunicatie verandert ook de wettelijke basis voor het verstrekken van gebruikersgegevens door telecomaanbieders. Voordien waren de bepalingen van de Wet persoonsregistraties (WPR) en later de Wet bescherming persoonsgegevens (WBP) daarop van toepassing. Deze wetten legden de beslissing over de verstrekking van gegevens bij de houder van die gegevens. De houder diende te beoordelen of de verstrekking noodzakelijk was voor het opsporingsonderzoek. Uiteraard was hij daarvoor afhankelijk van informatie afkomstig van de verzoekende partij. Ook de verantwoordelijkheid voor de verstrekking lag bij de houder van de gegevens. Deze was tevens aansprakelijk voor eventuele schade bij de persoon wiens gegevens werden verstrekt, mocht de beoordeling achteraf onjuist blijken. Met de inwerkingtreding van de nieuwe wet verandert dit en is niet langer de houder van de gegevens verantwoordelijk voor de afweging, maar de opsporingsambtenaar.

Voorts is van belang dat het aftappen niet langer alleen betrekking heeft op openbare telecommunicatie. Ook besloten telecommunicatienetwerken en -diensten kunnen nu door justitie worden afgetapt. Voor een tap op openbare telecommunicatie is in principe nog steeds de medewerking van de telecomaanbieder nodig, maar de wet maakt nu een uitzondering voor gevallen waarin dat ‘niet mogelijk’ is of waarin het belang van de strafvordering zich daartegen verzet. Bij besloten telecommunicatie stelt justitie – behoudens dezelfde uitzonderingsgevallen – de aanbieder in de gelegenheid medewerking te verlenen, maar hij is hiertoe niet verplicht. Al met al komt het neer op een verdere uitbreiding van het opsporingsarsenaal, omdat justitie nu in principe ook zelfstandig mag aftappen zonder medewerking of medeweten van de telecomaanbieder.

· Bw. Studie 49 23-01-2007 14:39 Pagina 31

De aftapbevoegdheid wordt in Nederland op grote schaal gebruikt. Uit Duits onderzoek van medio 2003 blijkt dat Nederland na Italië het hoogste aantal telefoontaps kent van Europa en de Verenigde Staten (Albrecht, Dorsch & Krüpe, 2003).[44] Het gaat hier overigens om taps voor justitiële doeleinden. Het aantal taps door inlichtingendiensten kon niet worden achterhaald.

2.2.10 Vorderen gegevens

De Wet vorderen gegevens financiële sector maakt deel uit van een pakket aan maatregelen ter vergroting van de mogelijkheden tot opsporing van terroristische misdrijven. De wet is aangekondigd in het Actieplan terrorismebestrijding en veiligheid.[45] De wet vloeit voort uit een in oktober 2001[46] tot stand gekomen protocol van de Europese Unie. Dit protocol heeft tot doel de wederzijdse rechtshulp tussen lidstaten te verbeteren met het oog op de bestrijding van de georganiseerde en financiële criminaliteit (waaronder 'witwassen').[47]

In verband met de aanslagen van 11 september 2001 is binnen de Europese Unie besloten tot een versnelde totstandkoming van het protocol. Dit bepaalt dat lidstaten elkaar informatie moeten verstrekken over rekeningen, rekeningnummers en financiële transacties van natuurlijke of rechtspersonen tegen wie strafrechtelijk onderzoek is ingesteld. De wet verleent justitiële autoriteiten de bevoegdheid gegevens te vorderen bij instellingen in de financiële sector. De instellingen zijn verplicht deze gegevens te verstrekken. Deze bevoegdheden zijn nieuw. Tot dan toe kon een financiële instelling op basis van de bepalingen in de Wet bescherming persoonsgegevens zelf beslissen om de gegevens al dan niet te verstrekken.[48]

Inmiddels zijn met de Wet vorderen gegevens uit 2006 de bevoegdheden alweer verder uitgebreid.[49] Deze nieuwe wet is gebaseerd op de voorstellen van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (Commissie-Mevis).[50]

Een opsporingsambtenaar mag voortaan in het belang van het onderzoek zogenoemde identificerende gegevens vorderen. Hieronder vallen gegevens over naam, adres, woonplaats, geboortedatum, geslacht, rekeningnummers en andere administratieve kenmerken. Daarnaast mag een officier van justitie ook andere gegevens vorderen. In dringende gevallen mag hij bovendien 'gevoelige' gegevens vorderen, dat wil zeggen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. De officier heeft hiertoe voorafgaande machtiging door de rechter-commissaris nodig.

Identificerende gegevens kunnen worden gevorderd als sprake is van verdenking van een misdrijf. De overige gegevens kunnen worden gevorderd bij verdenking van een misdrijf waarvoor voorlopige hechtenis

· Bw. Studie 49 23-01-2007 14:39 Pagina 32

is toegelaten en dat een ernstige inbreuk op de rechtsorde oplevert. Hieronder vallen bijvoorbeeld terroristische misdrijven en ernstige misdrijven in georganiseerd verband.[51] In deze gevallen is het ook toegestaan om 'toekomstige' gegevens te vorderen; dat wil zeggen dat gegevens die in een komende periode van vier weken ontstaan, dienen te worden doorgegeven aan justitie. In dringende gevallen moeten zelfs, met toestemming van de rechter-commissaris, toekomstige gegevens direct na het moment van ontstaan ('real-time') worden doorgegeven.

2.2.11 Buitenlandse druk

Onder druk van buitenlandse overheden, met name van de Verenigde Staten, zijn in Nederland enkele maatregelen genomen die in dit overzicht niet mogen ontbreken: de doorgifte van passagiersgegevens op vluchten naar de Verenigde Staten en de invoering van een biometrisch paspoort. Bij de verstrekking van passagiersgegevens gaat het overigens niet om het scheppen of uitbreiden van bevoegdheden van opsporingsdiensten: het zijn de luchtvaartmaatschappijen zelf die deze gegevens verstrekken aan de Amerikaanse autoriteiten. De Nederlandse overheid staat, op verzoek van de Europese Commissie, de verstrekking toe en maakt haar mogelijk.

De Amerikaanse overheid eist sinds maart 2003 online toegang tot de zogenoemde *Passenger Name Records* (PNR's) die de Europese vliegtuigmaatschappijen bijhouden van vluchten op de Verenigde Staten. Door screenen van de gegevens willen de Amerikaanse autoriteiten de kans verminderen dat terroristen vanuit Europa de Verenigde Staten binnendringen. De PNR's bevatten uiteenlopende gegevens, zoals namen, geboortedata en telefoonnummers. Tevens kunnen ze informatie bevatten over creditcardnummers, stoelnummers en maaltijdvoorkeuren. Ook willen de Amerikaanse autoriteiten informatie uit het *Advanced Passenger Information System*, zoals het geslacht, het paspoortnummer en de nationaliteit van passagiers.

Uit angst voor boetes en het verlies van landingsrechten, werkten de luchtvaartmaatschappijen vrijwel van meet af aan mee. Omdat de passagiersgegevens onder de Europese privacyregels vallen, moest wel een speciale regeling worden getroffen. De Europese Unie en de Verenigde Staten bereikten hierover in 2004 een akkoord,[52] dat het Europese Hof van Justitie in mei 2006 echter op formele gronden nietig verklaarde.[53] In oktober 2006 is een nieuw akkoord bereikt.

2.3 Achtergronden

De terreuraanslagen in de Verenigde Staten van 11 september 2001 worden vaak als keerpunt gezien als het gaat om de uitbreiding van de bevoegdheden van politie, justitie en veiligheidsdiensten. Vanaf die

· Bw. Studie 49 23-01-2007 14:39 Pagina 33

datum zou het aantal veiligheids- en antiterreurmaatregelen exponentieel zijn toegenomen. Het bovenstaande overzicht maakt duidelijk dat dit voor Nederland in elk geval niet opgaat. De oorsprong van veel van de beschreven bevoegdheden en uitbreidingsmaatregelen ligt in het tijdvak voor 11 september 2001. Dit geldt voor DNA-onderzoek, cameratoezicht, aftappen en andere bijzondere opsporingsmethoden en voor veel van de bevoegdheden ten aanzien van het vorderen van gegevens. Zelfs een zeer vergaande en pas in januari 2006 in werking getreden wet als de Wet vorderen gegevens stoelt grotendeels op een rapport dat dateert van mei 2001. De aanleiding voor de nieuwe Wet op de inlichtingen- en veiligheidsdiensten van 2002 ligt evenmin in de gebeurtenissen van 11 september, maar in kritiek van de Raad van State op de oude wettelijke regeling. Deze kritiek en de voornemens om de wet te wijzigen dateren al van het midden van de jaren negentig.

Van alle besproken maatregelen lijken slechts twee een direct verband te hebben met de aanslagen van september 2001: de bevoegdheid tot het vorderen van gegevens van financiële instellingen en het verstrekken van passagiersgegevens door Europese vliegtuigmaatschappijen aan de Amerikaanse overheid. Daarbij moet worden aangetekend dat eerstgenoemde aanpassing weliswaar is gepresenteerd als een antiterrorismemaatregel, maar dat zij mede een gevolg is van het Europese Verdrag aangaande de wederzijdse rechtshulp (dat dateert van voor 2001). Wel vond de invoering versneld plaats ten behoeve van de terrorismebestrijding. Bij de tweede maatregel gaat het niet om een bevoegdheid van de nationale opsporingsdiensten, maar om private bedrijven die onder druk van de Amerikaanse autoriteiten gegevens over hun passagiers afstaan. De Europese en Nederlandse overheden hebben er slechts voor gezorgd dat dit niet op clandestiene wijze hoeft te gebeuren.

Dit alles neemt niet weg dat de aanslagen van 11 september 2001 de invoering van de bevoegdheidsuitbreidingen en andere maatregelen waarschijnlijk wel hebben vergemakkelijkt. Voor Europa en Nederland zijn in dit opzicht de moord op Theo van Gogh (2004) en de aanslagen op het treinstation van Atocha in Madrid (2004) en de metro van Londen (2005) eveneens van belang. Hoe groot de invloed van deze gebeurtenissen precies is geweest, valt echter moeilijk vast te stellen. Slechts in sommige gevallen zijn er aanwijzingen te vinden, zoals bij de discussie over de bewaarplicht van verkeersgegevens, waarover de Nederlandse regering na 11 september 2001 duidelijk positiever oordeelde dan daarvoor (Koops, 2002, p. 136).[54]

Als de aanslagen op het World Trade Center en het Pentagon niet doorslaggevend zijn geweest, hoe kan dan wel worden verklaard dat Nederland in tien jaar tijd veranderde van een land waarin de privacy van burgers een serieuze rol speelde bij de besluitvorming, tot een land dat opsporingsbevoegdheden aan alle kanten uitbreidt? In elk geval de

volgende factoren lijken van belang: de opkomende aandacht voor de georganiseerde criminaliteit en, daarmee samenhangend, de uitkomsten van de parlementaire enquête naar opsporingsmethoden (de Commissie-Van Traa); de heroriëntatie van de veiligheidsdiensten op interne gevaren na het einde van de Koude Oorlog; de Europese beleidsvorming; de voortschrijdende ontwikkeling van de technologie, met name de voortschrijdende informatisering. Hieronder worden deze factoren nader besproken.

2.3.1 Georganiseerde misdaad

In het midden van de jaren tachtig stellen misdaadanalisten vast dat de zware georganiseerde criminaliteit in Nederland oprukt. Als antwoord daarop stelt de top van de Amsterdamse politie voor om Interregionale Rechercheteams (IRT's) te vormen, die zich speciaal op de georganiseerde misdaad moeten richten. Deze teams komen inderdaad van de grond. Als thema dat serieuze aandacht behoeft, plaatst minister van Justitie Ernst Hirsch Ballin (1989-1994) de bestrijding van de zware criminaliteit voor het eerst op de politieke agenda.

De opkomst van de georganiseerde misdaad is op twee manieren van invloed op de hierboven besproken uitbreiding van de opsporingsbevoegdheden. Allereerst is Hirsch Ballin erin geslaagd om aan de politiek duidelijk te maken dat de georganiseerde misdaad in Nederland een probleem is dat serieuze aandacht behoeft. Daarmee heeft hij ongetwijfeld draagvlak geschapen voor de uitbreiding van een aantal bevoegdheden.

Daarnaast is er een meer indirecte invloed geweest. Ongeveer vijf jaar na zijn oprichting raakt najaar 1993 het IRT Noord-Holland/Utrecht in opspraak als bekend wordt dat jarenlang onder politieregie partijen verdovende middelen zijn ingevoerd, in de hoop zo te kunnen doordringen tot de top van de misdaadorganisatie van wijlen Klaas Bruinsma. In 1994 besluit de Tweede Kamer een parlementaire enquête in te stellen naar de gang van zaken bij dit IRT en naar de toelaatbaarheid van justitiële opsporingsmethoden in het algemeen. Begin 1996 presenteert de enquêtecommissie, die bekend staat als de Commissie-Van Traa, haar bevindingen. De commissie beveelt onder meer aan om de opsporingsmethoden inzichtelijk te maken en te normeren. De Wet BOB en de regelingen rond het vorderen van telecommunicatiegegevens vloeien mede voort uit deze voorstellen.

2.3.2 Einde Koude Oorlog

Met de val van het IJzeren Gordijn, de zwaarbewaakte grens tussen Oost- en West-Europa, in 1989 en het uiteenvallen van het machtsimperium van de voormalige Sovjet-Unie in de jaren daarna, komt een einde aan de Koude Oorlog. De inlichtingen- en veiligheidsdiensten verliezen daarmee hun traditionele communistische vijand, die ze ruim veertig jaar lang hebben bestreden. In rap tempo heroriënteren ze zich op hun

· Bw. Studie 49 23-01-2007 14:39 Pagina 35

taken. Zo oppert in de jaren negentig de BVD, de voorloper van de huidige AIVD, een taak te kunnen vervullen in de strijd tegen de georganiseerde misdaad. Of dit ook is gebeurd, is niet bekend. Inmiddels is echter wel duidelijk dat sinds het begin van dit millennium de AIVD een grote rol speelt in de terreurbestrijding. En het ziet ernaar uit dat deze rol in de komende jaren alleen maar groter zal worden.

2.3.3 Europa

Nog steeds zijn binnen de Europese Unie de meeste bevoegdheden op het gebied van politie, justitie en de inlichtingendiensten primair een zaak van de nationale staten. De Europese Commissie is niet gemachtigd om op deze gebieden richtlijnen uit te vaardigen die door de lidstaten in wetgeving moeten worden geïmplementeerd. Wel kan de Europese Raad van Ministers, bij unanimiteit, besluiten tot strafrechtelijke maatregelen, zoals is gebeurd bij de aftapbaarheidsplicht van telecommunicatie.

Verder is Europa van invloed op het Nederlandse beleid doordat het nationale wetgevers kan inspireren; doordat het maatregelen kan nemen ter facilitering van de taken van de nationale politie en justitie; en doordat Europa op sommige aanpalende terreinen wel beleid kan opleggen. Dit laatste is bijvoorbeeld het geval bij privacywetgeving en bij grensoverschrijdend verkeer. Dit is ook de reden dat de Europese Commissie met de Amerikaanse autoriteiten is gaan onderhandelen over de verstrekking van passagiersgegevens.

Een voorbeeld van faciliterend beleid is de eerder genoemde Wet vorderen gegevens financiële sector. Deze wet is mede tot stand gekomen als implementatie van een protocol betreffende de wederzijdse rechtshulp tussen de lidstaten van de Europese Unie. Zoals eerder is vermeld, dient dit protocol de bestrijding van de georganiseerde en financiële criminaliteit.[55]

Europese beleidsvorming is ook van belang bij enkele binnenkort te verwachten ontwikkelingen: invoering van het biometrisch paspoort, de opslag van verkeersgegevens en het wederzijds toegankelijk maken van de databanken van politie en justitie. Hierbij kan worden opgemerkt dat een deel van de controverses die deze maatregelen hebben opgeroepen minder betrekking heeft op inhoudelijke bezwaren, maar wel op de vraag of de beslissingen daarover op Europees niveau moeten worden genomen.

2.3.4 Technologische ontwikkelingen

Van grote betekenis op de bevoegdheidsuitbreidingen in Nederland zijn de voortgaande technologische ontwikkelingen, met name die in de informatisering. Bij de bevoegdheden betreffende cameratoezicht, DNA-onderzoek en computercriminaliteit is dit evident. Maar ook waar het gaat om het vorderen van gegevens speelt de techniek een grote

· Bw. Studie 49 23-01-2007 14:39 Pagina 36

rol. Vanaf de jaren negentig hebben zich in dit verband belangrijke ontwikkelingen voorgedaan: de inburgering van de pc, de opkomst van internet, de exponentiële groei in de opslagcapaciteit van computers en de mogelijkheden om verschillende bestanden op eenvoudige wijze aan elkaar te koppelen, waardoor grootschalige *datamining* en *profiling* opeens tot de mogelijkheden gaan behoren.

Bij datamining speurt een computer door enorme gegevensbestanden, op zoek naar onderlinge patronen en verbanden die vaak op geen enkele andere manier kunnen worden gevonden, zoals het gemiddelde gezondheidsrisico in een bepaald postcodegebied. De patronen en verbanden die zo worden gevonden kunnen weer worden gebruikt voor het maken van groepsprofielen, het zogeheten profiling. De groepskenmerken zijn vaak alleen bekend bij de personen die de profielen maken. Behalve opsporingsinstanties maken ook bedrijven veelvuldig gebruik van deze technieken, bijvoorbeeld om de doelgroep van een *direct marketing*-campagne te bepalen.

Deze technologische ontwikkelingen hebben ertoe geleid dat zowel overheidsinstellingen, private organisaties als burgers steeds meer informatie over elkaar kunnen verwerven, verwerken en opslaan. Het gebruik dat de overheid van deze mogelijkheden maakt of wil maken in het kader van de opsporing en preventie van misdaad en terreur, komt tot uiting in het geheel aan bevoegdheden ten aanzien van het vorderen en verstrekken van gegevens.

2.4 Trends

Hierboven zijn de ontwikkelingen geschetst op het gebied van opsporingsbevoegdheden vanaf de jaren negentig. Deze ontwikkelingen kunnen worden samengevat in de volgende zes trends:

1. Het onderzoek wordt steeds vaker uitgebreid tot personen op wie zelf geen verdenking rust, in de omgeving van verdachten.

2. Het onderzoek neemt in toenemende mate de vorm aan van een verkenning, waarin op basis van risicoprofielen potentieel verdachte groepen worden gevolgd.

3. Er is een tendens om wettelijke beperkingen die gelden voor het gebruik van bepaalde opsporingsmethoden te verlichten of weg te nemen.

4. Opsporingsdiensten krijgen, zowel juridisch als technologisch, steeds meer mogelijkheden om (zelfstandig) onderzoek te verrichten.

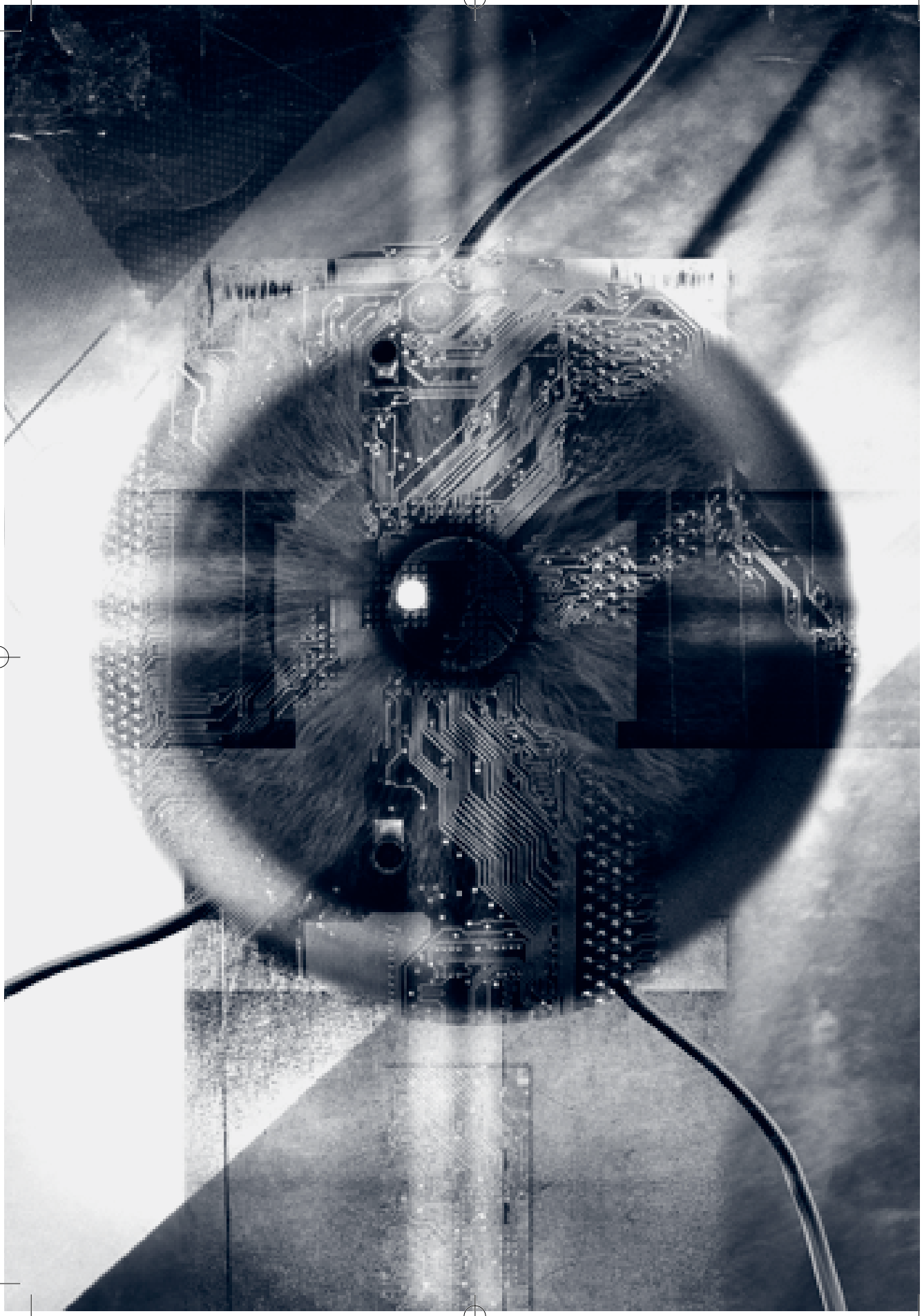
· Bw. Studie 49 23-01-2007 14:39 Pagina 37

5. Opsporingsdiensten kunnen in toenemende mate beschikken over persoonsgegevens afkomstig van andere (semi)overheidsdiensten, die voor andere dan opsporingsdoeleinden zijn verzameld.

6. Opsporingsdiensten dwingen steeds vaker andere partijen tot medewerking aan onderzoek.

Deze tendensen hebben zowel elk afzonderlijk als in samenhang effect op de privacy van burgers. Een belangrijke consequentie is dat de privacy van aanzienlijk meer mensen dan voorheen in het geding is. Niet langer zijn alleen personen die redelijkerwijs als verdachte kunnen worden aangemerkt voorwerp van onderzoek. Steeds vaker komen ook niet-verdachte, 'gewone' burgers in beeld.

Doordat daarnaast de technische middelen die gebruikt mogen worden aanzienlijk zijn uitgebreid, kan grootschaliger en ingrijpender informatie worden verzameld. Denk daarbij aan de uiteenlopende soorten van informatie die kunnen worden verkregen via DNA-onderzoek, cameraobservatie, telefoontaps en gegevens van internetverkeer. Door de uitgebreidere mogelijkheden wordt het scala aan persoonsgegevens die toegankelijk zijn voor politie, justitie en de veiligheidsdiensten groter, en kunnen de opsporingsdiensten dieper en ingrijpender doordringen in het privéleven van burgers. In het slothoofdstuk wordt hier uitgebreid op teruggekomen.



· Bw. Studie 49 23-01-2007 14:39 Pagina 39

3 Toekomstige ontwikkelingen

Nu in het vorige hoofdstuk een overzicht is gegeven van de huidige wettelijke regelingen rond opsporingsbevoegdheden en privacy, kan in dit hoofdstuk worden ingegaan op de ontwikkelingen die Nederland in de nabije toekomst te wachten staan. Allereerst gaat het daarbij om concrete maatregelen, die in een dusdanig stadium van voorbereiding zijn dat ze nog dit jaar, of binnen een paar jaar, in werking treden. Vervolgens wordt ingegaan op de stappen die *denkbaar* zijn, waarbij wordt teruggegrepen op de in het vorige hoofdstuk gesignaleerde trends en de ontwikkelingen die daaraan ten grondslag liggen. Het hoofdstuk wordt afgesloten met een beschouwing over veranderende beleidsopvattingen.

3.1 Binnenkort te verwachten

De komende jaren krijgt Nederland te maken met vier nieuwe ontwikkelingen die van belang zijn voor opsporing en veiligheid: er komt een zogeheten burgerservicenummer (BSN) dat het sofinummer als identificatiemiddel vervangt en dat door alle overheidsdiensten te gebruiken is; de bevoegdheden van de AIVD worden opnieuw verder uitgebreid; het biometrisch paspoort wordt in gebruik genomen; aanbieders van telecommunicatiediensten krijgen te maken met een uitgebreidere bewaarplicht voor verkeersgegevens. Deze maatregelen worden al geruime tijd voorbereid. Met uitzondering van het burgerservicenumer wordt terreurbestrijding als belangrijkste motivatie aangevoerd.

3.1.1 Burgerservicenummer

Op dit moment gebruiken de afzonderlijke overheidsinstanties en uitvoeringsorganen nog verschillende nummers om hun cliënten te identificeren. De nadelen hiervan zijn dat burgers lastig door de verschillende administraties heen te volgen zijn, en dat zij ook telkens weer hun persoonsgegevens moeten verstrekken, zodra ze met een nieuwe instelling te maken krijgen. Het burgerservicenummer introduceert een en hetzelfde nummer in alle sectoren, van Belastingdienst tot Vreemdelingendienst en van sociale dienst tot zorginstelling. Het is een algemeen geldig, uniek persoonsnummer voor alle burgers en zal het huidige sofinummer vervangen. De Wet burgerservicenummer[56] moet ervoor zorgen dat alle overheidsorganisaties het nummer kunnen gaan gebruiken en er wordt een nieuw centraal informatiesysteem

· Bw. Studie 49 23-01-2007 14:39 Pagina 40

gebouwd.[57] Overigens zal het burgerservicenummer in de verschillende sectoren wel verschillende namen krijgen.

Het burgerservicenummer wordt ingevoerd om doelmatigheidsredenen en om het aantal administratieve fouten terug te dringen. Het nummer vergemakkelijkt het koppelen van gegevens uit verschillende databanken aanzienlijk. Dit maakt het ook een stuk eenvoudiger om gegevens die oorspronkelijk zijn opgeslagen voor bijvoorbeeld de uitvoering van zorgtaken, tevens te gebruiken voor opsporingsdoeleinden (zie ook paragraaf 2.2.7).

Het burgerservicenummer is nu al onderdeel van tal van voorstellen en projecten van het ministerie van Binnenlandse Zaken om gegevens te koppelen en burgers te identificeren. Voorbeelden zijn DigiD, een uniforme authenticatie voor online overheidsdiensten,[58] en eNIK, de infrastructuur voor de elektronische identiteitskaart.[59]

3.1.2 Bevoegdheden AIVD

Het tweede kabinet-Balkenende heeft in 2006 een wijziging op de Wet op de inlichtingen- en veiligheidsdiensten 2002 (WIV) ingediend bij de Tweede Kamer.[60] Deze wijziging is onderdeel van een pakket aan beleidsmaatregelen dat is geformuleerd naar aanleiding van de aanslagen op het station van Atocha in Madrid op 11 juni 2004.[61] De aanpassing maakt het voor de AIVD mogelijk om bij telecommunicatiebedrijven, financiële instellingen en vervoersbedrijven individuele gegevens en zelfs hele bestanden te vorderen. De nieuwe bevoegdheden stellen de AIVD in staat om op grote(re) schaal aan *datamining* te doen, om zo door middel van profilering uiteenlopende aspecten van personen, groepen en organisaties in kaart te brengen.

Behalve bij telecommunicatiebedrijven, is de AIVD voor het verkrijgen van gegevens tot nu toe aangewezen op de vrijwillige medewerking van de houders van de gegevens. De voorgenomen wetswijziging legt nu ook informatieverplichtingen op aan de financiële sector en aan vervoersbedrijven. De bevoegdheidsuitbreiding ten aanzien van de vervoersbedrijven is vooral interessant, omdat binnenkort de strippenkaart en het papieren treinkaartje vervangen worden door de OV-chipkaart. Met de OV-chipkaart is het moeilijker dan voorheen, zij het niet onmogelijk, om anoniem te reizen. Het gekozen chipkaartsysteem zal van de meeste reizigers het reisgedrag zeer nauwkeurig vastleggen en dat bovendien verbinden met hun persoonsgegevens.

3.1.3 Bewaartermijn verkeersgegevens

In maart 2006 is de Europese Richtlijn Dataretentie ingevoerd, die verplicht tot opslag van verkeersgegevens door telecommunicatiebedrijven voor een periode van een half tot twee jaar. Het doel is om politie, justitie en inlichtingendiensten langer dan nu het geval is, in staat te stellen gegevens te kunnen vorderen. De richtlijn moet voor 15 september

· Bw. Studie 49 23-01-2007 14:39 Pagina 41

2007 in Nederland zijn geïmplementeerd, maar voor internetgegevens kunnen lidstaten uitstel bedingen tot 15 maart 2009; Nederland heeft verklaard van deze uitstelmogelijkheid gebruik te maken.[62]

Oorspronkelijk zou de maatregel in de vorm van een kaderbesluit worden ingevoerd. Hiervoor is unanimiteit vereist in de Raad van Ministers van de Europese Unie, maar geen medebeslissing van het Europees Parlement. De maatregel was echter niet onomstreden. Mede onder druk van het parlement, besloot de Europese Commissie zelf met een voorstel te komen in de vorm van een richtlijn. In deze procedure heeft het Europees Parlement medebeslissingsrecht, waardoor de legitimiteit van de maatregel zou worden vergroot.

3.1.4 Buitenlandse toegang politieregisters

In paragraaf 2.2.10 is al gesproken over het Europese verdrag aangaande wederzijdse rechtshulp in strafzaken. Een van de andere manieren waarop de Europese Commissie de bestrijding van georganiseerde misdaad en terrorisme wil verbeteren is door de politiediensten van de afzonderlijke lidstaten toegang te geven tot elkaars databanken. Ook de overkoepelende Europese rechtshandhaver Europol moet directe toegang krijgen tot de nationale politieregisters. In eerste instantie moeten zes soorten van (persoons)gegevens uitwisselbaar worden: DNA-profielen; vingerafdrukken; ballistische informatie (gegevens over bij misdrijven gebruikte vuurwapens); voertuigregistratiegegevens; telefoonnummers en andere communicatiegegevens; de zogeheten identificerende gegevens (onder meer NAW-gegevens, rekeningnummers en andere administratieve kenmerken). De toegang tot deze informatie moet online kunnen plaatsvinden. Het Europese voorstel heeft de steun van het Nederlandse kabinet.[63]

3.1.5 Biometrisch paspoort

Al sinds de late jaren negentig van de vorige eeuw denken Nederlandse bewindslieden over het toevoegen van biometrische kenmerken aan het paspoort. Na de terreuraanslagen van 11 september 2001 zijn de ontwikkelingen in een stroomversnelling gekomen. Sinds eind 2004 is ook een verordening van de Europese Unie van kracht die bepaalt aan welke veiligheidscriteria de paspoorten van de lidstaten moeten voldoen en welke biometrische kenmerken moeten zijn opgenomen.[64] Het nieuwe Europese paspoort moet onder meer een chip bevatten met daarop opgeslagen een vingerafdruk en gelaatsscan van de drager. De Europese Unie komt hiermee tegemoet aan het verlangen van de Amerikaanse overheid om strengere eisen te stellen aan de identificeerbaarheid van buitenlanders die de Verenigde Staten willen binnenreizen. Op 28 augustus 2006 ontving de toenmalige minister van Bestuurlijke Vernieuwing het eerste exemplaar van het nieuwe Nederlandse paspoort. De chip op het paspoort bevat voorlopig alleen dezelfde informatie als ook in het paspoort staat, inclusief de foto. Vanaf 2009 zal ook een vingerafdruk van de drager worden toegevoegd.

· Bw. Studie 49 23-01-2007 14:39 Pagina 42

De Europese Unie laat het aan de lidstaten zelf over of ze de biometrische informatie centraal willen opslaan in een databank, of alleen op het paspoort zelf. De Nederlandse regering wil – met een beroep op de strijd tegen het terrorisme – een landelijk register aanleggen met biometrische gegevens, maar hierover is discussie ontstaan. Indien volstaan wordt met uitsluitend registratie van de biometrische gegevens op de chip in het paspoort zelf, is identificatie alleen mogelijk met behulp van het paspoort. Als de gegevens daarnaast centraal worden bewaard in een databank, is het mogelijk personen te identificeren zonder dat het paspoort wordt gebruikt. Dit vergemakkelijkt bijvoorbeeld online-identificatie, maar vermindert ook de mogelijkheid voor het betrokken individu om zijn gegevens te controleren. Inmiddels wordt op Europees niveau wel gewerkt aan een centrale database met biometrische gegevens van visahouders. Dit Visa Information System[65] wordt in 2007 ingevoerd.[66]

3.2 Op langere termijn

In het vorige hoofdstuk is aangegeven dat de technologische ontwikkeling van grote invloed is op de manier waarop opsporingsbevoegdheden worden uitgebreid. Zonder al te veel te speculeren, worden nu enkele technologische ontwikkelingen besproken die waarschijnlijk tot een verdere uitbreiding van de opsporingsbevoegdheden zullen leiden, of in elk geval tot een bredere toepassing van de reeds bestaande bevoegdheden. Opsporings- en veiligheidsdiensten zullen daardoor dieper kunnen doordringen in de privélevens van gewone mensen. In veel gevallen gaat het hierbij om informatie die door andere partijen dan de opsporingsinstanties zelf worden verzameld, opgeslagen of verwerkt.

3.2.1 Slimme camera's

Door beveiligingscamera's met software en sensoren uit te rusten en ze aan databases te koppelen, kunnen ze zelfstandig afwijkingen herkennen in van tevoren vastgestelde patronen. Constateert een camera een afwijking, dan begint ze automatisch met opnemen of geeft ze een alarmsignaal af aan de controlekamer, ten teken dat de bewaker naar zijn monitor moet kijken. Zo'n 'slimme' camera kan bijvoorbeeld 'vaststellen' dat in een bepaalde ruimte ruzie ontstaat, simpelweg omdat het gemiddelde geluidsniveau plotseling toeneemt of omdat mensen niet langer doorlopen maar stil blijven staan of samenklonteren, en zo een afwijkende vlek vormen in het geprogrammeerde patroon. Door de camera met een databank te verbinden met daarin bijvoorbeeld nummerplaatgegevens van gestolen auto's of foto's van gezochte criminelen, kan ze voertuigen of verdachte personen identificeren.

· Bw. Studie 49 23-01-2007 14:39 Pagina 43

Op dit moment worden slimme camera's nog betrekkelijk weinig gebruikt in Nederland, waar, zoals eerder gezegd, ook 'traditioneel' cameratoezicht nog een betrekkelijk nieuw verschijnsel is (zo is de Wet cameratoezicht pas sinds januari 2006 van kracht). Maar het aantal slimme camera's zal de komende jaren snel toenemen. De Commissie Criminaliteit en Technologie wees in 2005 in een advies aan de Minister van Justitie al op slimme camera's als het meest veelbelovende hulpmiddel voor opsporing en preventie.[67]

3.2.2 RFID

Een andere technologische ontwikkeling is de introductie van de zogenoemde *Radio Frequency Identifier* (RFID), een computerchip die zo klein kan zijn als een zandkorrel en die een uniek nummer bevat. Via een radiosignaal kunnen het nummer en de andere informatie op de chip op afstand worden uitgelezen en in sommige gevallen ook worden bewerkt. Met de chips wordt tot nu toe voornamelijk geëxperimenteerd in winkels om de logistiek te verbeteren en producten te volgen. De producten voorzien van een RFID-chip worden bij de kassa gescand, waarna aan het unieke nummer een prijs of andere informatie wordt gekoppeld, net zoals bij de 'ouderwetse' streepjescode gebeurt. Op deze manier kan zeer flexibel met informatie worden omgegaan en kan de verwerking van producten vrijwel geheel machinaal plaatsvinden.

Het gebruik van RFID-chips in supermarktartikelen of gebruiksvoorwerpen kan informatie opleveren over de personen die ze aanschaffen of gebruiken. Zo leverden Duitse en Britse experimenten met de chips veel informatie op over het koop- en winkelgedrag van individuele klanten. Zelfs als geen koppeling tot stand werd gebracht tussen een product en een individuele klant, was het vaak al mogelijk om in de verzamelde gegevens patronen te ontdekken die overeenstemden met het koopgedrag van afzonderlijke klanten en op basis waarvan een klantprofiel kon worden gemaakt. Het is niet ondenkbaar dat overheden in het kader van misdaad- en terreurbestrijding gebruik zouden willen maken van dergelijke gegevens.

In principe kunnen ook mensen worden voorzien van een RFID-chip. De chip kan in een bril, horloge, of kledingstuk worden verwerkt, maar ook via een injectienaald onder de huid worden ingespoten. In het biometrisch paspoort zit eveneens een RFID-chip, met daarop de persoonsgegevens en een kleurenfoto van de drager. Ook de nieuwe OV-chipkaart zal een RFID-chip bevatten. Door personen te voorzien van een RFID-chip kan de nodige informatie over hen worden vergaard. Zo kunnen ze gemakkelijk worden geïdentificeerd in een omgeving waarin ze voorheen nog een grote mate van anonimiteit kenden. Het is ook niet uit te sluiten dat derden de informatie op de chip kunnen uitlezen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 44

3.2.3 Ambient Intelligence

Door de mogelijkheid om computers steeds kleiner te maken – terwijl hun geheugencapaciteit alleen maar toeneemt –, door het steeds snellere informatieverkeer en de toenemende mogelijkheden om apparaten onderling te laten communiceren in netwerken, ontstaat een situatie waarin computers steeds meer in hun omgeving opgaan; een situatie bovendien waarin traditionele interfaces (zoals de muis of het toetsenbord) verdwijnen en waarin computers zelfstandig beslissingen nemen.

Dit toekomstbeeld wordt ook wel *ambient intelligence* of *ubiquitous computing* genoemd. Via allerlei sensoren verzamelen de computers, apparaten en netwerken gegevens over mensen en voorwerpen in hun omgeving en zetten die met behulp van *intelligent agents* (software) om in gewenste activiteiten. Mensen geven zelf geen directe opdrachten meer aan de computer, maar de computer bepaalt aan de hand van zijn eigen 'waarnemingen' wat van hem wordt verwacht.

Vooralsnog is het toekomstmuziek, maar wanneer *ambient intelligence* werkelijkheid wordt, valt te verwachten dat het aantal aspecten en dimensies van het privéleven waarvan gegevens worden geregistreerd – en die daarmee in principe ook (voor anderen) beschikbaar zijn – andermaal zal zijn uitgebreid.

3.3 Veranderende beleidsopvattingen

De technologische ontwikkelingen leiden ook tot andere ideeën over hoe opsporingsdiensten hun werk moeten doen. Een rapport van de Raad van Hoofdcommissarissen uit 2004 laat deze verandering goed zien.[68] In het rapport wordt – naar voorbeeld van het Britse *intelligence-led policing* – het idee van 'informatiegestuurde opsporing' geïntroduceerd, als sleutelbegrip voor het toekomstige politiebeleid.[69] Toepassing van geavanceerde technologieën en een goed informatiebeheer moeten de politie in staat stellen het opsporingswerk optimaal te sturen, op zowel strategisch als tactisch niveau. Een zorgvuldige analyse van de opsporingsinformatie staat daarbij centraal.

De Raad van Hoofdcommissarissen stelt nadrukkelijk dat het begrip 'opsporing' ruim moet worden geïnterpreteerd: behalve voor de traditionele, reactieve opsporing in geval van een misdrijf, moet er meer ruimte komen voor proactieve en op preventie gerichte opsporingsactiviteiten. De Raad voorziet ook dat de politie zich veel meer zal richten op groepen van potentiële verdachten dan op individuen.

De Raad van Hoofdcommissarissen geeft verder aan dat nieuwe technologieën zullen worden ingezet om traditionele beperkingen weg te nemen, zoals afstand of duisternis. De politie zal volgens de raad veel vaker gebruik gaan maken van zaken als *Global Positioning Systems*,

· Bw. Studie 49 23-01-2007 14:39 Pagina 45

integrale informatiesystemen, geavanceerde afluistertechnieken, nachtkijkers en sensoren voor de waarneming van gassen, explosieven, wapens, drugs of nucleair materiaal. Voorheen gescheiden informatiestromen en besluitvormingslijnen zullen vaker met elkaar worden verbonden, zodat een betere gegevensuitwisseling ontstaat. Technologische innovaties zoals miniaturisering, draadloze communicatie, vergroting van de reken- en opslagcapaciteit van computers, breedbandcommunicatie en de koppeling van bestanden moeten de doelmatigheid van de opsporingsmethoden vergroten.

Om de informatiegestuurde opsporing te optimaliseren moet er volgens de Raad nog veel gebeuren, zowel binnen het politieapparaat als op ambtelijk en politiek niveau.[70] De politie moet beter vertrouwd raken met de techniek en de samenwerking met de private sector, waarin veel nieuwe en voor de politie relevante technologieën reeds worden toegepast, moet worden geïntensiveerd. Ten slotte moeten ook wettelijke regelingen verder worden aangepast om het politieonderzoek te vergemakkelijken, bijvoorbeeld in situaties waarin (nog) geen sprake is van directe verdachten.

Volgens de hoofdcommissarissen vormt op dit moment de privacywetgeving te vaak een hindernis bij het politiewerk. Zo zou de politie voor strafrechtelijk onderzoek gebruik moeten kunnen maken van de databank met vingerafdrukken van vreemdelingen, iets wat de Wet bescherming persoonsgegevens op dit moment verbiedt. Om aan te tonen dat hier ook maatschappelijk draagvlak voor is, citeert de raad een enquête naar de mening van burgers over de afname van DNA-materiaal bij verdachten van misdrijven. Hieruit zou blijken dat burgers meer dan ooit van mening zijn dat een inperking van de privacy nodig is om criminaliteit en terreur effectief te bestrijden.[71]

De toekomstvisie van de Raad van Hoofdcommissarissen sluit aan bij de in het vorige hoofdstuk gesignaleerde trends om de opsporingsbevoegdheden verder uit te breiden. Sommige trends lijkt de raad zelfs extra te willen aanzetten: de vermindering van beperkende voorwaarden op het opsporingsonderzoek, de uitbreiding van het onderzoek tot verkenningen en proactieve analyses en de verbreding van de kring van te onderzoeken personen. Opvallend is ook de centrale rol die de raad hierbij toebedeelt aan de technologie, en vooral de informatietechnologie. In hoofdstuk 5 wordt op deze trends teruggekomen.

· Bw. Studie 49 23-01-2007 14:39 Pagina 46

· Bw. Studie 49 23-01-2007 14:39 Pagina 47

Deel II
De ontwikkelingen nader bezien


ID
RIGHT
NE
D
EE
ID

· Bw. Studie 49 23-01-2007 14:39 Pagina 49

4 Maatschappelijke bezwaren

De in deel 1 beschreven maatregelen en bevoegdheidsuitbreidingen op het gebied van opsporing en veiligheid hebben ook maatschappelijke reacties losgemaakt. Academici, opiniemakers en politici hebben kanttekeningen geplaatst bij de ontwikkelingen. Dit hoofdstuk geeft, zonder uitputtend te willen zijn, een beeld van de belangrijkste kritiek. De discussies ontstonden hoofdzakelijk naar aanleiding van afzonderlijke maatregelen en meestal in reactie op concrete beleidsvoornemens of wetsvoorstellen. De commentaren zijn daarom gegroepeerd naar het type maatregel, waardoor dit hoofdstuk een soortgelijke opbouw kent als hoofdstuk 2. Afsluitend wordt ingegaan op de aard van de reacties en de kenmerken die ze met elkaar gemeen hebben, inclusief de consequenties hiervan voor het maatschappelijke debat.

4.1 Kritiek op de maatregelen

4.1.1 DNA-onderzoek

Het College Bescherming Persoonsgegevens (CBP) heeft zich in 2004 kritisch uitgelaten over de reikwijdte van de Nederlandse wetgeving inzake DNA-onderzoek voor opsporingsdoeleinden.[72] De Nederlandse Vereniging voor Rechtspraak (NVvR) bracht verder naar voren dat de procedure van het DNA-onderzoek mogelijk in strijd zou zijn met het Europees Verdrag voor de Rechten van de Mens. Volgens de NVvR kan de toepassing van dwangmiddelen om DNA af te nemen, worden opgevat als de toepassing van een strafmaatregel op zich. De NVvR vreesde dat hierdoor het recht op een eerlijk proces in het gedrang zou kunnen komen.[73]

4.1.2 Cameratoezicht

In een achtergrondstudie over het wetsvoorstel Cameratoezicht op openbare plaatsen vraagt het College Bescherming Persoonsgegevens zich af hoe effectief dat toezicht is en in hoeverre de veiligheid ermee wordt vergroot (Smeets, 2004). Voorts moet volgens het CBP als hoofdregel worden gehanteerd dat cameratoezicht slechts kan worden ingezet als dit noodzakelijk is voor de handhaving van de openbare orde. Het opsporen van strafbare feiten valt daar niet onder.

Het CBP heeft ook een aantal vuistregels opgesteld voor het gebruik van cameramateriaal. Zo wil het college dat de beelden afdoende worden beveiligd, dat ze niet langer mogen worden bewaard dan strikt

· Bw. Studie 49 23-01-2007 14:39 Pagina 50

noodzakelijk en dat ze niet zomaar voor andere doelen mogen worden gebruikt dan waarvoor ze zijn opgenomen. Het CBP loopt tevens vooruit op de introductie van slimme camera's. Ten tijde van het verschijnen van het rapport in 2004 zijn de technologische ontwikkelingen echter nog niet zover dat betrouwbare identificatie van personen via deze camera's mogelijk lijkt.[74]

Filosofe Lynsey Dubbeld (2004) waarschuwt in haar dissertatie verder tegen het oneigenlijke gebruik van bewakingscamera's door bewakingspersoneel. Uit haar onderzoek komt onder meer naar voren dat personeel dat beelden van bewakingscamera's observeert soms functioneel onnodige aandacht heeft voor uiterlijke kenmerken van personen die voor beveiligingsdoeleinden minder relevant zijn.

Over webcams die gebeurtenissen in de openbare ruimte opnemen zonder een functie in het toezicht te vervullen – denk aan webcams die de gebeurtenissen in een winkelstraat registreren en verspreiden via internet – lijkt men zich geen al te grote zorgen te maken. Tweede Kamerlid Martijn van Dam vindt bijvoorbeeld dat wat hem betreft webcams op straat onder 'vrije nieuwsgaring' vallen. Wel voegt hij eraan toe dat het tijd wordt voor discussie over de grenzen van privacy.[75]

4.1.3 Bijzondere opsporingsbevoegdheden

De Wet bijzondere opsporingsbevoegdheden (Wet BOB) is van verschillende kanten kritisch onder de loep genomen. Sinds de inwerkingtreding is de wet in twee fasen geëvalueerd door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Justitie. De evaluaties (verschenen in 2002 en 2004) bestaan voornamelijk uit inventarisaties en analyses van de ervaringen uit de uitvoeringspraktijk in de eerste jaren dat de wet van kracht was.

Een belangrijke uitkomst is dat de notificatieplicht – die stelt dat personen naar wie onderzoek is gedaan, daarvan op gegeven moment op de hoogte worden gesteld – weinig wordt nagekomen. De onderzoekers wijzen hiervoor twee oorzaken aan. Allereerst hoeven personen waarover informatie is vergaard daarover alleen in kennis te worden gesteld als het belang van het onderzoek dat toelaat. Ten tweede staat op het achterwege laten van die kennisgeving geen sanctie.

De onderzoekers stellen ook dat de notificatieplicht bij het Openbaar Ministerie nog weinig prioriteit heeft. Er is angst dat door notificatie de gebruikte opsporingstechnieken in brede kring bekend worden, waardoor ze minder effectief zouden kunnen worden. Bovendien zou notificatie de veiligheid van informanten in gevaar kunnen brengen. De minister van Justitie stelt in zijn reactie op de evaluaties dat hij de uitvoering van de notificatieplicht nader wil bezien. Hij geeft daarbij echter meteen aan dat het opsporingsbelang inderdaad niet in het gedrang mag komen.[76]

· Bw. Studie 49 23-01-2007 14:40 Pagina 51

De Commissie Bestuurlijke Evaluatie AIVD (de Commissie-Havermans) heeft eind 2004 een rapport gepubliceerd over het functioneren van de Algemene Inlichtingen- en Veiligheidsdienst.[77] Volgens de Commissie houdt de AIVD te veel informatie te lang voor zichzelf. Daardoor profiteren andere diensten die betrokken zijn bij de bestrijding van misdaad en terreur, onvoldoende van de inspanningen van de veiligheidsdienst. Naar aanleiding van het rapport zijn er initiatieven genomen om de samenwerking te verbeteren. Zo is bijvoorbeeld de Contraterrorisme-infobox in het leven geroepen, een bijzonder samenwerkingsverband van AIVD, Militaire Inlichtingen- en Veiligheidsdienst (MIVD), het Korps Landelijke Politiediensten (KLPD), de Immigratie- en Naturalisatiedienst (IND) en het Openbaar Ministerie (OM).

In de nasleep van de aanslagen in Madrid is overigens herhaaldelijk vastgesteld dat de samenwerking van de Europese inlichtingendiensten evenmin optimaal is. Zo bleek de Noorse geheime dienst al over inlichtingen te beschikken die wezen op een mogelijke aanslag in Madrid. Deze informatie werd echter niet doorgespeeld aan de Spaanse veiligheidsdiensten. Ook moest de Nederlandse Minister van Binnenlandse Zaken in een Spaanse krant lezen dat moslimfundamentalisten volgens de Italiaanse veiligheidsdiensten in Nederland waren geweest om een aanslag voor te bereiden.

Volgens de Commissie-Havermans laat ook het toezicht op de AIVD te wensen over. Hoewel de AIVD en de minister van Binnenlandse Zaken de Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) van de Tweede Kamer ruimhartig informeren, constateert de Commissie-Havermans dat er sprake is van een beperkte parlementaire controle. Er vinden in de CIVD nauwelijks inhoudelijke debatten plaats over de wijze waarop de AIVD zou moeten functioneren. Alleen de Algemene Rekenkamer beschikt over de – generieke – bevoegdheid om incidenteel de organisatie en het functioneren van de inlichtingendienst te controleren.

De jurist Anton Ekker (2002) is van mening dat de bevoegdheden van de veiligheidsdiensten volgens de WIV 2002 door hun ruime omschrijving ongrijpbaar zijn. Ekker is vooral kritisch over het feit dat het toezicht op de veiligheidsdiensten afhankelijk wordt gemaakt van het belang van nationale veiligheid.

De Raad van State heeft zich ten slotte kritisch uitgelaten over de recente voornemens om de AIVD bevoegdheid te geven om meer gegevens te kunnen vorderen. De Raad vraagt zich af of het grootschalig invoeren van een informatieplicht noodzakelijk is. Ook bekritiseert de Raad het ontbreken van garanties voor de bescherming van de gegevens en het ontbreken van een vergoeding voor de door de verstrekker gemaakte kosten.

· Bw. Studie 49 23-01-2007 14:40 Pagina 52

4.1.4 Identificatieplicht

Jarenlang is de invoering van een identificatieplicht in Nederland bijzonder omstreden geweest. De in hoofdstuk 2 besproken wet is in dat licht met opvallend veel gemak aangenomen. De Rotterdamse hoogleraar strafrecht Paul Mevis, tevens voorzitter van de commissie wier rapport aan de basis lag van de Wet bevoegdheden vorderen gegevens, stelde in 2003 in een interview met het internettijdschrift *Netkwesties* dat bij de Wet identificatieplicht in hoge mate sprake is van symboolwetgeving, die tegemoetkomt aan de wensen van een groep binnen de overheid die graag iets zichtbaars wil doen.[78] Volgens Mevis wil de overheid met deze wet vooral een signaal afgeven en maakt het niet zoveel uit of hij ook werkelijk effectief is.

Uit onderzoek dat *de Volkskrant* in 2006 uitvoerde blijkt dat de nieuwe identificatieplicht inderdaad geen merkbare invloed heeft op de criminaliteitsbestrijding. Het Openbaar Ministerie zegt tegenover *de Volkskrant* geen voorbeelden te kennen van ernstige delicten die op grond van de nieuwe wet zijn voorkomen. Er is daarentegen wel een fors aantal boetes uitgedeeld voor het niet kunnen tonen van een identiteitsbewijs. Voorts is het aantal vermiste en gestolen identiteitsbewijzen aanmerkelijk gegroeid sinds januari 2005 – hetgeen geweten wordt aan de invoering van de identificatieplicht (Trommelen, 2006a).

Een groep vrijwilligers die eveneens betwijfelt of de identificatieplicht de veiligheid van de Nederlandse samenleving vergroot, heeft op internet het Meldpunt Misbruik Identificatieplicht opgezet. De groep verspreidt daarnaast ook actiemateriaal waarin hij waarschuwt dat de identificatieplicht de persoonlijke vrijheid in gevaar brengt.[79]

4.1.5 Koppeling bestanden

Het College Bescherming Persoonsgegevens en zijn voorganger de Registratiekamer waarschuwen sinds de jaren negentig met enige regelmaat voor te ruime mogelijkheden om bestanden te koppelen, vooral met behulp van een uniek identificatienummer voor burgers.[80] De Raad van State sprak bij de behandeling van het wetsvoorstel burgerservicenummer in 2005 zijn verbazing uit over het feit dat het voorstel alleen over burgers spreekt als object en weinig aandacht heeft voor hun rechten. Daarnaast maakte de Raad zich zorgen over de gevolgen voor de privacy, ook al bevat het burgerservicenummer op zichzelf geen informatie. De Raad is vooral bezorgd over de mogelijkheid om met het burgerservicenummer uit de meest uiteenlopende bronnen allerlei informatie te verzamelen over individuen.

Deze kritiek wordt gedeeld door informatierechtspecialist Laurens Mommers (2006), die ervoor waarschuwt dat met behulp van het burger-servicenummer zeer gemakkelijk allerlei gevoelige persoonsgegevens te achterhalen zijn. Er wordt volgens hem ook te gemakkelijk

· Bw. Studie 49 23-01-2007 14:40 Pagina 53

van uitgegaan dat gebruikers van het nummer altijd volstrekt betrouwbaar zullen zijn.

Daarnaast denkt Mommers dat de toenemende informatisering de Nederlandse samenleving steeds vaker met 'informationele dwangbuizen' confronteert. Hiermee bedoelt hij dat burgers steeds vaker worden gedwongen om informatie aan te leveren en uit te wisselen volgens geünificeerde patronen. Het burgerservicenummer is volgens hem een voorbeeld van een dergelijke dwangbuis. Mommers pleit daarom voor een tegenbeweging die streeft naar 'compartementalisering' van persoonsgegevens, waarbij de betrokkenen zelf de regie houden.

Hoogleraar informatiseringsrecht Corien Prins (2003) waarschuwt eveneens voor een blind vertrouwen in de techniek. Volgens haar wordt door de voorstanders van het burgerservicenummer te weinig rekening gehouden met het risico dat fouten binnensluipen in de bewerkingen waarbij het nummer wordt gebruikt.

Publiciste Karin Spaink (2005) verbaast zich ten slotte over het gemak waarmee het burgerservicenummer wordt opengesteld voor allerlei doeleinden waarvoor het oorspronkelijk niet bestemd was.

4.1.6 Vorderen financiële gegevens

Over de Wet vorderen gegevens financiële sector is weinig ophef geweest. Als gevolg van de gebeurtenissen op 11 september 2001 is de wet versneld ingevoerd, zelfs zonder tussenkomst van een kabinetsstandpunt. Wel stellen leden van de Eerste Kamer bij de behandeling van het wetsvoorstel vragen over de controleerbaarheid van de nieuwe bevoegdheden en de waarborgen tegen eventueel misbruik. De Kamerleden pleiten voor een notificatieplicht jegens personen van wie naam, adres en woonplaats zijn opgevraagd. Daarbij merken ze op dat het wetsvoorstel weliswaar een beklagregeling bevat, maar dat betrokkenen daar geen gebruik van zouden kunnen maken zolang zij er niet van op de hoogte worden gesteld dat hun gegevens zijn opgevraagd. De minister weigert echter de notificatieplicht, omdat deze te belastend zou zijn voor het opsporingsapparaat.[81]

4.1.7 Vorderen telecommunicatiegegevens

De Wet vorderen telecommunicatiegegevens is al sinds de voorbereidende fase onderwerp van hevige debatten. De Registratiekamer oordeelde al in 2000 in een advies dat het wetsvoorstel voor telefoonbedrijven en internetaanbieders te ver dreigde door te schieten.[82] Aan verkeersgegevens zou niet categorisch de bescherming van het telefoongeheim (zoals vastgelegd in artikel 13 van de Grondwet) moeten worden onthouden. Daarnaast zou de reikwijdte van de voorgestelde maatregelen te onbepaald zijn. De tekst zou bijvoorbeeld ruimte bieden om gegevens te vorderen van gesprekken waaraan de

· Bw. Studie 49 23-01-2007 14:40 Pagina 54

te onderzoeken persoon zelf niet had deelgenomen, maar waarin hij slechts gespreksonderwerp was.

De Eerste Kamer heeft eveneens moeite met het standpunt dat verkeersgegevens niet onder het telefoongeheim zouden vallen. Volgens de Kamerleden heeft het Europees Hof voor de Rechten van de Mens in verschillende uitspraken laten blijken dat verkeersgegevens een integraal bestanddeel vormen van de mededelingen per telefoon. De Kamerleden stellen daarnaast ook nu weer vragen over de controleerbaarheid van de nieuwe bevoegdheden en de waarborgen tegen misbruik. Ook pleiten ze wederom tevergeefs voor een notificatieplicht. De minister doet hierop wel de toezegging om jaarlijks te rapporteren over het aantal opvragingen.[83]

Juriste Sjoera Nas van de privacyorganisatie Bits of Freedom spreekt in het internettijdschrift *Netkwesties* haar verbazing uit over het gemak waarmee het wetsvoorstel ten slotte toch door de Kamer is geloodst.[84] Volgens Nas is een gevolg van de wet dat alle veertigduizend Nederlandse opsporingsambtenaren vrijuit mogen snuffelen in de adressenbestanden van internet- en telefoonaanbieders, zelfs zonder dat er concrete verdenkingen zijn tegen specifieke personen. Evenmin is ze te spreken over wat zij noemt de *upgrading* van de officieren van justitie. Voor het opvragen van verkeersgegevens hebben deze immers niet langer toestemming nodig van de rechter-commissaris.

4.1.8 Wet bevoegdheden vorderen gegevens

Ook de Wet bevoegdheden vorderen gegevens veroorzaakt nauwelijks maatschappelijke ophef. Een uitzondering vormen de bibliotheken, die met een conferentie in maart 2005 de publiciteit zoeken en met brieven aan het parlement de wetgeving proberen te beïnvloeden. Wel leidt de wet onder juristen tot stevige debatten. Het meest omstreden daarbij is het feit dat praktisch alle gegevens die over mensen verkrijgbaar zijn binnen het bereik van politie en justitie komen. In het bovengenoemde interview met *Netkwesties* merkt strafrechtdeskundige Paul Mevis – tevens de voorzitter van de commissie wier rapport aan de basis lag van deze wet – op dat vooral de mogelijkheid om allerhande gegevens te combineren een groot gevaar kan opleveren voor burgers.[85] Hij relativeert dat evenwel door te stellen dat digitaal rechercheren bij de politie niet optimaal is georganiseerd. Misdaadanalyse zou volgens hem een van de minst ontwikkelde onderdelen van de politie zijn. Volgens Mevis komt de Wet bevoegdheden vorderen gegevens dan ook neer op een vorm van ‘symboolwetgeving’.

Het College Bescherming Persoonsgegevens deelt de zorgen van Mevis. Volgens het college legt de wet een te grote informatieverplichting op aan bedrijven en (overheids)organisaties, die bovendien niets te maken heeft met hun eigenlijke taakuitoefening. Elk bedrijf en elke overheidsinstelling wordt zo de facto een verlengstuk van politie of justitie.

· Bw. Studie 49 23-01-2007 14:40 Pagina 55

In zijn advies op het wetsvoorstel dringt het CBP er daarom op aan om bedrijven of instanties bij wie gegevens worden opgevraagd de mogelijkheid te geven die vordering vooraf door de rechter te laten toetsen. Daarnaast pleit het college voor periodieke audits om de betrouwbaarheid van de politieregisters te verbeteren.

Jurist Edwin MacGillavry (2001) levert al in een vroeg stadium kritiek op het wetsvoorstel. Met de nieuwe bevoegdheden zou zowel over verdachte als onverdachte personen meer informatie dan ooit te vergaren zijn. De onverdachte burger is hierbij kind van de rekening. In toenemende mate raakt hij betrokken bij de verstrekking van persoonsgegevens, zonder dat hij het zelf zal weten. Burgers en bedrijven kunnen bovendien worden verplicht gegevens ter beschikking te stellen die ook betrekking hebben op andere personen dan de verdachte. Tevens kunnen de houders van gegevens worden verplicht tot het aanmaken van nieuwe (persoons)gegevens door middel van datamining en registervergelijking. Beide laatste verplichtingen staan volgens MacGillavry op gespannen voet met de uitgangspunten van strafvordering (zie ook de kritiek van Asscher & Koops, 2004).

Hoogleraar informatiseringsrecht Corien Prins (2004) maakt zich zorgen over het feit dat met de komst van de wet een extern – 'extra' – afwegingsmoment van de baan is. Hiermee doelt zij op het feit dat de instanties die de gegevens beheren niet langer zelf de afweging maken over het al dan niet verstrekken van gegevens aan justitie en politie, zoals de Wet bescherming persoonsgegevens bepaalt. De belangenafweging wordt volledig in de handen van justitie gelegd.

Ook wijst zij op de nieuwe bevoegdheid van de officier van justitie om 'andere dan identificerende' gegevens op te vragen. Het gaat dan bijvoorbeeld om informatie over iemands koopgedrag of uitleenvoorkeuren bij bibliotheken. En ook nu kan het uitleveringsverzoek toekomstige gegevens betreffen. Deze bevoegdheid mag alleen worden gebruikt bij verdenking van zwaardere misdrijven, maar ze is niet beperkt tot uitsluitend gegevens van verdachten.

Journalist Frank Kuitenbrouwer vraagt zich in een reactie op het wetsvoorstel af of dit wel past bij een beschaafde samenleving.[86] Het strafrecht is van oudsher terughoudend met het in het leven roepen van directe antwoordverplichtingen, iets wat met deze wet overboord wordt gegooid. In de ogen van Kuitenbrouwer leidt dat tot een moderne inquisitie. Volgens hem vormt de wet een breuk met de beginselen van de wetgeving voor de elektronische snelweg, zoals de regering die in 1998 heeft geformuleerd.[87] De hoofdregel luidde toen: wat offline geldt, moet ook online gelden. Hij stelt dat nu met een beroep op het uitzonderlijke karakter van ICT nieuwe overheidsbevoegdheden worden gecreëerd. Deze worden zonder slag of stoot geïmporteerd in de klassieke rechts

· Bw. Studie 49 23-01-2007 14:40 Pagina 56

orde, terwijl men er tot voor kort niet over zou hebben gepiekerd om dergelijke vergaande bevoegdheden in te voeren.

Ook vindt Kuitenbrouwer dat de Commissie-Mevis in haar eindrapportage heel ver is gegaan door de bescherming van gevoelige gegevens opzij te schuiven. Het beroepsgeheim van de arts of advocaat wordt door de commissie weliswaar erkend, maar medische gegevens, seksuele details of criminele informatie zijn ook op andere manieren te verkrijgen, bijvoorbeeld door verschillende gegevens over één persoon te combineren, iets wat in de wet wordt toegestaan. Volgens Kuitenbrouwer betekent toestaan in het informatietijdperk: maximaal benutten.

De Wet bevoegdheden vorderen gegevens is inmiddels enige tijd van kracht en er is tot op heden één geval bekend waarin hij is toegepast.[88] Bij een onderzoek naar een gewapende overval op een juwelier in Vught heeft de officier van justitie in maart 2006 de gegevens van tweehonderdvijftig bezoekers van de nabijgelegen bibliotheek opgeëist. Interessant is in dit verband dat de bibliothecaire branchevereniging FOBID een aanwijzing heeft opgesteld aan bibliothecarissen om zo terughoudend mogelijk om te gaan met verzoeken tot gegevensverstrekking.[89]

4.1.9 Bewaartermijn verkeersgegevens

De Richtlijn Dataretentie heeft de nodige reacties opgeroepen wegens de vergrote kwetsbaarheid bij een verlengde bewaring van gegevens. Een brede coalitie van burgerrechtengroepen en de telecommunicatiebedrijven heeft gelobbyd tegen de bewaarplicht als zodanig.[90] Naast kritiek op de veiligheidsrisico's en de ermee gemoeide kosten, wordt ook gewaarschuwd tegen *function creep*, bijvoorbeeld door publiciste Karin Spaink: "Wat begon als anti-terreurmaatregel eindigde als een maatregel tegen allerlei klein grut, tegen 'normale' overtredingen, maar met onveranderde grootse consequenties: alle burgers worden in de gaten gehouden." (Spaink, 2006)

Daarnaast is er veel kritiek uitgeoefend op de wijze waarop de richtlijn tot stand is gekomen. In het najaar van 2005 is het voorstel voor de richtlijn behandeld in het Europees Parlement. Het gaat hier om een extreem versnelde procedure, die weinig tijd laat voor overleg en waarbij zelfs de vertalingen ontbraken. De technische consequenties worden niet geëvalueerd en er is geen onderzoek gedaan naar de gevolgen voor de interne markt. Een comité onder leiding van de Duitse liberale Europarlementariër Alexander Alvaro stelt daarop enkele amendementen voor die tegemoetkomen aan eerdere bezwaren van de Europese Toezichthouder voor Gegevensbescherming. Het parlement keurt de richtlijn in december 2005 goed, maar negeert hierbij het advies van de Europese Toezichthouder.

De richtlijn is sinds mei 2006 van kracht, maar zestien van de 25 EU-leden hebben verklaard dat zij implementatie ervan zullen uitstellen.

· Bw. Studie 49 23-01-2007 14:40 Pagina 57

De belangrijkste reden daarvoor is de bijna gelijktijdige onthulling dat de Amerikaanse geheime dienst NSA telefoongegevens heeft verzameld van miljoenen Amerikanen.[91] Volgens de Duitse oppositiepartij Die Grünen/Bündnis 90 is de legaliteit van de Richtlijn betwistbaar. Volgens de partij had de Richtlijn moeten worden behandeld als een kaderbesluit, dat een unanieme beslissing van de EU Ministerraad vereist en bovendien veel meer vrijheid laat aan de nationale parlementen.[92]

4.1.10 Biometrisch paspoort

De Richtlijn Dataretentie is niet de enige regeling waarvan de totstandkoming ter discussie staat. Ook op de procedure voor de Europese verordening inzake biometrische gegevens op paspoorten is veel kritiek geuit. In de eerste plaats heeft die betrekking op de welwillende wijze waarmee is gereageerd op de Amerikaanse druk om paspoorten te voorzien van gelaatsscans, en op de verplichting om vingerafdrukken op te nemen (iets wat trouwens niet door de Amerikaanse overheid werd gevraagd). In de tweede plaats wordt opnieuw de snelheid van de procedure bekritiseerd en het gebrek aan dialoog tussen ministers en Europees Parlement. De ministerraad legt echter zonder zorgvuldige onderbouwing de door het parlement voorgestelde amendementen naast zich neer. Zo wordt een amendement van het parlement om de oprichting tegen te houden van een centrale database van EU-paspoorten en reisdocumenten, inclusief alle (biometrische) gegevens, niet overgenomen.

Zoals al in hoofdstuk 3 kort is opgemerkt, roept de centrale opslag van biometrische gegevens ook op nationaal niveau weerstand op. Het College Bescherming Persoonsgegevens vindt een centrale databank overbodig en bovendien onveilig. Andere critici waarschuwen ervoor dat centrale opslag het gevaar vergroot dat de gegevens worden gebruikt voor een ander doel dan waarvoor ze zijn verkregen,[93] en dat zo'n databank wel eens het doelwit van criminelen zou kunnen worden.[94] Het is in dit verband interessant om op te merken dat de Duitse regering na soortgelijke bezwaren van de Duitse privacytoezichthouder heeft afgezien van een centrale databank.

4.2 Kenmerken van het debat

Uit het bovenstaande moge duidelijk worden dat de verruiming van de bevoegdheden van politie, justitie en veiligheidsdiensten, net als de overige maatregelen in het kader van de misdaad- en terreurbestrijding, niet onbesproken zijn gebleven. Bij politici en instellingen als het College Bescherming Persoonsgegevens hebben ze reacties losgemaakt. Die reacties zijn hierboven afzonderlijk weergegeven en lopen soms sterk uiteen. Ze variëren van twijfels over de praktische uitvoerbaarheid, tot kritiek over onheldere besluitvormingsprocessen en een vrees dat de fundamenten onder de rechtsstaat vandaan worden geslagen.

· Bw. Studie 49 23-01-2007 14:40 Pagina 58

Wanneer de reacties in hun samenhang worden bestudeerd, blijkt dat ze ook een aantal gemeenschappelijke kenmerken hebben, waardoor het mogelijk is iets te zeggen over het maatschappelijke debat over dit onderwerp in het algemeen.

Wat allereerst opvalt is dat het merendeel van de reacties betrekking heeft op afzonderlijke bevoegdheidsuitbreidingen en maatregelen. Dit is ook de reden geweest om ze hierboven telkens per onderwerp te bespreken. Die nadruk op afzonderlijke maatregelen is niet verwonderlijk. De reacties zijn nu eenmaal sterk afhankelijk van de mate waarin voornemens tot en voorstellen voor bevoegdheidsuitbreidingen openbaar worden. Als bijna vanzelf gaat de discussie dan al snel uitsluitend over de specifieke bevoegdheid of maatregel die op dat moment in het nieuws is. Desondanks hebben veel commentaren wel degelijk een bredere strekking dan alleen de direct betrokken maatregel en bepaalde kritiek blijkt ook telkens weer terug te komen. Vooralsnog leidt dit echter niet of nauwelijks tot bredere beschouwingen, waarin wordt stilgestaan bij de gevolgen van de optelsom van maatregelen.

Een uitzondering vormt publiciste Karin Spaink, die na een overzicht te hebben gegeven van allerlei maatregelen, begin dit jaar in een bijdrage in *de Volkskrant* oproept tot de strijd tegen Big Brother, om vervolgens somber te eindigen met de conclusie dat privacy misschien wel dood is. Tegenover *NRC Handelsblad* uiten recentelijk enkele rechters van de Hoge Raad der Nederlanden hun bezorgdheid over de verhouding tussen recente antiterreurmaatregelen en de uitgangspunten van het strafrecht. Hoewel het de rechters minder gaat om de gevolgen voor de privacy, lijkt het een begin om de ontwikkelingen in samenhang te zien.[95]

Opvallend is verder dat veel van de reacties afkomstig zijn van vakjuristen, ook als de commentaren komen van buiten de kring van direct bij het wetgevingsproces betrokken partijen. Uiteraard laten ook journalisten, publicisten en burgerrechtenorganisaties als Bits of Freedom van zich horen, maar in meerderheid komt de kritiek toch uit rechtsgeleerde hoek en heeft ze een juridische strekking. Dit betekent dat de discussie in vrij beperkte kring wordt gevoerd.

Tot slot moet worden opgemerkt dat, opnieuw met Karin Spaink als uitzondering, privacy nauwelijks een rol van betekenis speelt in de commentaren. De zorgen gaan vooral uit naar specifieke grondrechten (anders dan privacy) of naar concrete nadelen die burgers kunnen ondervinden. Het lijkt er soms zelfs op dat de notie van 'privacy' angstvallig wordt gemeden. De maatschappelijke reacties weerspiegelen hiermee het wetgevingsproces op het gebied van opsporing en veiligheid; ook hier lijkt immers niet of nauwelijks aandacht te bestaan voor de privacy van burgers.

· Bw. Studie 49 23-01-2007 14:40 Pagina 59


32

· Bw. Studie 49 23-01-2007 14:40 Pagina 61

5 Een agenda voor debat

In de vorige hoofdstukken is een overzicht gegeven van zowel reeds ingevoerde, als voor de nabije toekomst te verwachten maatregelen en bevoegdheidsverruimingen in het kader van de misdaad- en terreurbestrijding. Tevens is een beeld geschetst van de discussie die deze maatregelen hebben opgeroepen, waarbij de kanttekening is geplaatst dat deze in vrij beperkte kring is gevoerd. In dit afsluitende hoofdstuk wordt een agenda opgesteld voor het maatschappelijke debat over de inzet van maatregelen voor het opsporings- en veiligheidsbeleid. Een belangrijk accent ligt daarbij op de gevolgen van de optelsom van de maatregelen voor de privacy van 'gewone' burgers.

Voordat aan die agenda kan worden begonnen, zal nader worden ingegaan op het begrip 'privacy'. Op het eerste gezicht lijkt dit misschien een theoretische zijsprong, maar het maakt het mogelijk om duidelijker aan te geven waarin de bedreigingen van privacy precies schuilen. Vervolgens wordt bekeken hoe de afzonderlijke maatregelen op elkaar ingrijpen, welk beeld te voorschijn komt uit hun optelsom en welke privacyrisico's deze optelsom met zich meebrengt. Op grond hiervan wordt een agenda voor het debat opgesteld.

5.1 Privacy onder de loep

Tot nog toe is het begrip 'privacy' in dit boek min of meer intuïtief gebruikt, zoals dat ook gebeurt in het dagelijks taalgebruik en in de publieke discussies over de veiligheidsmaatregelen die in het vorige hoofdstuk zijn besproken. Nu is echter het moment gekomen om dieper op het begrip in te gaan, in het bijzonder op de complexiteit ervan, die het lastig maakt om de precieze betekenis van privacy onder woorden te brengen.

5.1.1 Wat is privacy?

In de ethische en rechtstheoretische literatuur circuleren talrijke definities van privacy. De meeste delen – impliciet of expliciet – één gemeenschappelijke vooronderstelling: het besef dat er zoiets bestaat als een persoonlijke levenssfeer, die het waard is om te beschermen. Tot die persoonlijke levenssfeer worden in elk geval de volgende aspecten gerekend: het lichaam, de woning, seksuele relaties, correspondentie en andere communicatie. Ook informatie over deze zaken en de vrijheid om zelfstandig daarover te beslissen, vallen onder de persoonlijke levenssfeer (Vedder, 1998, 2000, 2001, 2004, Vedder & Blok, 2005). Deze elementen komen ook terug in de privacyopvattingen zoals

verwoord in de Nederlandse Grondwet en het Europees Verdrag voor de Rechten van de Mens.[96]

De notie van privacy omvat twee centrale begrippen: het toepassingsbereik van de persoonlijke levenssfeer en de beschermwaardigheid van dat bereik. Over het algemeen gaat men ervan uit dat privacy alleen van toepassing is binnen een bepaald privédomein: bepaalde onderdelen, dimensies of aspecten van een persoon. De persoonlijke levenssfeer moet hierbij niet al te letterlijk, als een louter ruimtelijke dimensie worden genomen. Privacy kan bijvoorbeeld ook betrekking hebben op intimiteit, ongeacht de plaats waar die intimiteit zich voordoet. De beschermwaardigheid van de persoonlijke levenssfeer heeft betrekking op de specifieke kwetsbaarheden van het individu die gerelateerd zijn aan de diverse dimensies van de privésfeer. Op beide begrippen wordt teruggekomen.

In de hedendaagse literatuur bestaat brede overeenstemming over de status die aan privacy moet worden toegekend. De beschermwaardigheid van de privésfeer is van principiële aard, maar heeft geen absolute gelding. Er kunnen, met andere woorden, goede redenen bestaan die een inbreuk op de privacy rechtvaardigen. Een gevolg hiervan is dat de reikwijdte en betekenis van het begrip contextueel bepaald zijn. In de literatuur zijn diverse pogingen te vinden om de betekenis van privacy te herleiden tot waarden als zelfbeschikking, vrijheid of individualiteit. Johnson (1989a, 1989b, 2001) heeft er herhaaldelijk op gewezen dat naast deze waarden ook conventies een belangrijke rol spelen. Deze claim kan nog verder worden uitgebreid. Zowel de precieze reikwijdte van de persoonlijke levenssfeer als de redenen om de privésfeer te beschermen hangen samen met een ingewikkeld samenspel van conventies, algemene waarden en sociaal-economische en technische factoren.

Deze contextuele factoren spelen als het ware een 'negatieve' rol in de betekenisgeving van privacy. Zij roepen bij individuen specifieke kwetsbaarheden op. Anders gezegd: conventies en sociaal-economische en technologische ontwikkelingen kunnen situaties creëren waarin personen worden geschaad of in hun vrijheid beperkt. Algemene waarden als individueel welzijn, individualiteit en zelfbeschikking kunnen vervolgens motiveren waarom individuen bescherming behoeven tegen deze schade of vrijheidsinperking. Zo maken bestaande conventies ten aanzien van ziekte en lijden zieke mensen kwetsbaar voor stigmatisering. Ook kunnen institutionele arrangementen, zoals verzekeringen die selecteren op gezondheidscriteria, de behoefte oproepen aan bescherming van de persoonlijke levenssfeer. Meer in algemene zin geldt dat het maatschappelijk verkeer bij mensen de behoefte teweegbrengt om zich terug te kunnen trekken en ongestoord invulling te kunnen geven aan hun eigen leven.

De betekenis van privacy is dus gerelateerd aan diverse waarden, conventies, maatschappelijke omstandigheden en technologische arrangementen. Privacy dient derhalve ook niet één welomschreven doel of belang, maar is een knecht van vele meesters. De eenheid van privacy ligt enkel in het gemeenschappelijke element van de idee van de beschermwaardigheid van de persoonlijke levenssfeer.

5.1.2 Privacy en 'gewone' mensen

Veel gewone burgers blijken de mening van de geleerden te delen. Zo toont sociologisch onderzoek aan dat Nederlandse burgers veel belang hechten aan privacy, maar het niet zien als iets wat absolute bescherming behoeft (Koops & Vedder, 2001; Samson, Schildmeijer & Koot, 2005). De spreekwoordelijke 'man in de straat' is bijvoorbeeld niet op voorhand tegen de verwerking van persoonsgegevens. Hij maakt zich echter wel zorgen over misbruik van zijn gegevens. Als hij wordt geconfronteerd met situaties waarin privacy en opsporingsbelangen op gespannen voet staan, is hij geneigd sneller iets van zijn privacy op te geven naarmate hij meer vertrouwen heeft in de betrokken instantie (Koops & Vedder, 2001; Samson, Schildmeijer & Koot, 2005).

Dit wil echter niet zeggen dat burgers een goed gearticuleerd begrip hebben van wat privacy inhoudt. In conflictsituaties lijken ze geneigd voorrang te geven aan gemakkelijk te benoemen belangen, zoals bescherming van hun gezondheid of vergroting van de veiligheid op straat. Privacy lijkt in dit soort situaties de betekenis te krijgen van een 'tegenwaarde': behalve met dat ene concrete belang (gezondheid, veiligheid op straat), dient ook rekening te worden gehouden met 'iets anders'. Wat dat andere dan inhoudt, blijft echter onuitgesproken. Dat heeft waarschijnlijk te maken met het moeilijk grijpbare – immers contextafhankelijke – karakter van het privacybegrip. Maar dat burgers vaak niet goed in staat zijn de betekenis van privacy onder woorden te brengen, wil niet zeggen dat ze geen waarde hechten aan de bescherming van hun persoonlijke levenssfeer. Wel roept het de vraag op of een complexe en fragiele waarde als privacy op de lange termijn bestand is tegen een dergelijk gebrek aan uitdrukkingsvermogen.

5.1.3 Afwegingen bij privacyconflicten

De beschermwaardigheid van de privésfeer is van principiële aard, maar niet absoluut. Hierin stemmen 'gewone' burgers en privacytheoretici overeen. Inbreuken op privacy kunnen derhalve gerechtvaardigd zijn. Zelfs Warren en Brandeis (1890, p. 195-196), die leefden in een tijd waarin het idee van absolute rechten gangbaarder was dan tegenwoordig, onderkennen in het artikel waarmee zij het privacybegrip in het moderne recht introduceerden, mogelijke rechtvaardigingsgronden voor inbreuken op de privacy.

Het is echter van belang om de rechtvaardigingsgronden voor een inbreuk op de privacy niet bij voorbaat deel uit te laten maken van de

· Bw. Studie 49 23-01-2007 14:40 Pagina 64

notie van privacy, zoals bijvoorbeeld de Amerikaanse socioloog Amitai Etzioni (1999) lijkt te doen. Zo kan duidelijk worden gemaakt dat er altijd waardevolle privacy verloren gaat wanneer inbreuk wordt gemaakt op de persoonlijke levenssfeer, en dat dergelijke inbreuken altijd bijzondere rechtvaardiging vereisen.

Bij conflicten tussen het belang van privacy en andere belangen (zoals opsporings- of veiligheidsbelangen) dient een afweging plaats te vinden. Dat wil niet zeggen dat er een duidelijke maatstaf is waarmee die afweging kan worden gemaakt. De moderne samenleving wordt immers gekenmerkt door een veelheid aan en ongelijksoortigheid van waarden en belangen. Dat betekent dat iedere afweging gepaard zal moeten gaan met een goede onderbouwing.

Daarbij moet uiteraard allereerst worden gespecificeerd welke waarden en belangen in het geding zijn die onder de privacy vallen. Vervolgens moeten de volgende overwegingen worden meegenomen:

- Overwegingen van *effectiviteit*: vormt een maatregel een inbreuk op de privacy, maar draagt zij aantoonbaar niet bij aan de realisatie van het concurrerende belang, dan is er geen reden om de inbreuk te plegen.

- Overwegingen van *subsidiariteit*: als het belang dat gemoeid is met de inbreuk op privacy ook op een andere manier kan worden bereikt dan door privacyaantasting, dan dient de voorkeur uit te gaan naar dat alternatief.

- Overwegingen van *de minste inbreuk*: als een inbreuk op de privacy eenmaal onvermijdelijk is, dient te worden gekozen voor die maatregel die met de minste inbreuk gepaard gaat. Factoren die hierbij een rol spelen zijn de specifieke waarden die vanuit privacyoogpunt in het geding zijn en het aantal betrokken personen.

- Overwegingen betreffende *bijkomende maatregelen*: bij een noodzakelijk geachte inbreuk op de privacy moeten extra maatregelen worden overwogen die de consequenties van de inbreuk beperkt houden of compenseren. Hieronder vallen bijvoorbeeld regels om betrokkenen in te lichten dat informatie over hen is ingewonnen, of die hun de mogelijkheid bieden de gegevens op hun juistheid te controleren. Ook kan gedacht worden aan compensatie voor geleden schade als gevolg van openbaarmaking van (onjuiste) informatie.

Het belang van deze overwegingen wordt overigens breed onderkend; zelfs door iemand als Etzioni, die over het algemeen weinig gewicht toekent aan privacynormen (zie onder meer Etzioni, 1999, p. 12-14).

· Bw. Studie 49 23-01-2007 14:40 Pagina 65

Normatieve conflicten over privacy zijn lastig, maar zeker niet per definitie onoplosbaar. Wel moet er bereidheid zijn om de discussie aan te gaan, waarbij bovenstaande overwegingen nadrukkelijk moeten worden meegenomen. Een open debat leidt ook tot een groter bewustzijn van de waarden en belangen die op het spel staan en draagt aldus bij aan een betere articulatie van de betekenis van privacy.

5.1.4 Gaten in de muur

De beschermwaardigheid van de privésfeer komt tot uitdrukking in een veelheid aan normen en regels. Hierbij gaat het niet alleen om wettelijke bepalingen, zoals de Wet bescherming persoonsgegevens, maar ook om gewoonten en fatsoensregels; bijvoorbeeld om sanitaire ruimtes af te sluiten bij gebruik, of om niet meteen naar het salaris van de nieuwe buurman te vragen. Alle regels en gebruiken tezamen vormen een verdedigingswerk rond de persoonlijke levenssfeer. Het is de vraag hoeveel stenen uit deze vestingmuur kunnen worden gemorreld, zonder dat hij instort.

De optelsom van een reeks maatregelen kan, zeker op de lange termijn, grotere gevolgen hebben dan die maatregelen afzonderlijk doen vermoeden. Elke inbreuk op de privacy – gerechtvaardigd of niet – maakt elke volgende inbreuk gemakkelijker. Is één steen uit de muur gewrikt, dan is het eenvoudiger om een volgende los te halen. Zo kan eenmaal vastgelegde informatie over het privédomein van individuen gemakkelijk een eigen leven gaan leiden. Ze kan worden gebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk is verzameld, en ze kan worden doorgegeven aan andere instanties dan de oorspronkelijke gebruikers. Bij de verzameling, opslag en bewerking van persoonsgegevens zijn daarom bijkomende, beperkende maatregelen nodig, die hergebruik of gebruik voor andere doeleinden reguleren of onmogelijk maken.

Dit besef is een van de redenen geweest waarom juist rond de bescherming van persoonsgegevens zoveel aanvullende juridische regelingen zijn getroffen. Wat echter opvalt bij de in deel 1 besproken maatregelen en bevoegdheidsuitbreidingen, is dat de meeste regelingen de verzameling, opslag en verwerking van persoonsgegevens vereenvoudigen, maar dat de waarborgen voor een zorgvuldige omgang met de gegevens weinig zijn uitgewerkt. En voor zover deze waarborgen al bestaan, worden ze amper nageleefd.

Ook op een meer indirecte manier kan worden gemorreld aan het algehele verdedigingswerk rondom de persoonlijke levenssfeer, en wel via de publieke opinie. Al eerder is erop gewezen dat een gebrekkige articulatie van privacykwesties kan leiden tot een verminderd privacybewustzijn. Als gevolg hiervan zullen mensen sneller nieuwe aantastingen van hun persoonlijke levenssfeer accepteren.

· Bw. Studie 49 23-01-2007 14:40 Pagina 66

Politici en beleidsmakers beroepen zich in discussies over nieuwe bevoegdheden en bevoegdheidsuitbreidingen regelmatig op diezelfde publieke opinie. Het is daarom niet ondenkbaar dat het algehele beschermingsniveau van de privésfeer, inclusief de wettelijke normen, op deze manier in een neerwaartse spiraal terechtkomt. Het losbikken van stenen zal in dat geval op steeds minder protesten stuiten.

5.2 De optelsom van maatregelen

De metafoor van de vestingmuur maakt nogmaals duidelijk hoe belangrijk het is om niet alleen naar de effecten van de afzonderlijke veiligheidsmaatregelen te kijken, maar ook naar de wijze waarop zij op elkaar ingrijpen en elkaar versterken. In deze paragraaf worden de contouren geschetst van een dergelijke optelsom, inclusief de consequenties daarvan voor de privacy van burgers.

5.2.1 Privacy en technologie

In hoofdstuk 2 is reeds gewezen op de zes trends die zijn waar te nemen bij de maatregelen en bevoegdheidsuitbreidingen van de afgelopen tien tot vijftien jaar. We noemen ze hier nogmaals:

1. Het onderzoek wordt steeds vaker uitgebreid tot personen op wie zelf geen verdenking rust, in de omgeving van verdachten.

2. Het onderzoek neemt in toenemende mate de vorm aan van een verkenning, waarin op basis van risicoprofielen potentieel verdachte groepen worden gevolgd.

3. Er is een tendens om wettelijke beperkingen die gelden voor het gebruik van bepaalde opsporingsmethoden te verlichten of weg te nemen.

4. Opsporingsdiensten krijgen, zowel juridisch als technologisch, steeds meer mogelijkheden om (zelfstandig) onderzoek te verrichten.

5. Opsporingsdiensten kunnen in toenemende mate beschikken over persoonsgegevens afkomstig van andere (semi)overheidsdiensten, die voor andere dan opsporingsdoeleinden zijn verzameld.

6. Opsporingsdiensten dwingen steeds vaker andere partijen tot medewerking aan onderzoek.

Het merendeel van deze trends wordt mogelijk gemaakt door het (toenemende) gebruik van nieuwe technologieën door politie, justitie en veiligheidsdiensten en de voortschrijdende digitalisering van gegevensbestanden.

· Bw. Studie 49 23-01-2007 14:40 Pagina 67

Met de inzet van steeds weer nieuwe technieken (onder andere DNA-onderzoek, slimme camera's, datamining, koppeling van bestanden en systemen) kan gemakkelijker en op grotere schaal dan voorheen informatie worden vastgelegd, verwerkt en bewerkt. Daardoor komen voorheen onbereikbare aspecten en dimensies van de persoonlijke levenssfeer binnen handbereik van opsporings- en veiligheidsdiensten.

Zo kunnen uit DNA-materiaal niet alleen allerlei persoonsgegevens en kenmerken worden afgeleid van een verdachte, maar ook van zijn familieleden. Met behulp van profiling en datamining kan informatie over personen of groepen worden gegenereerd die bij de betrokkenen zelf niet bekend is. Zo kunnen (potentieel verdachte) patronen worden gevonden in gedragingen of persoonskenmerken, waarvan de betreffende individuen zelf geen weet hebben. Een individu kan bijvoorbeeld deel uitmaken van een 'groep', omdat hij zonder daarvan op de hoogte te zijn, in de omgeving van een verdachte is geweest.

Daarnaast kan er met behulp van de nieuwe technieken informatie worden verkregen over steeds meer individuen. Camera's kunnen langduriger meer personen gadeslaan dan een mens. Datamining en de koppeling van bestanden en systemen maken het mogelijk om veel meer gegevens over veel meer mensen te analyseren, dan ooit zou kunnen met behulp van een traditionele zoekopdracht in een gegevensbestand. Veel van de hierboven besproken bevoegdheden en maatregelen hebben dan ook betrekking op het toegang krijgen tot gedigitaliseerde gegevensbestanden. Het hoeft dan ook geen verwondering te wekken dat de Raad van Hoofdcommissarissen wil dat geïntegreerd informatiebeheer in de toekomst centraal komt te staan in de opsporing. Ook de relatief nieuwe neiging van justitie en de veiligheidsdiensten om gegevens van derden te vorderen lijkt voort te komen uit het steeds groter wordende gemak waarmee deze gegevens beschikbaar kunnen worden gemaakt.

5.2.2 Privacyrisico's

Als de hierboven geschetste trends zich doorzetten – en gelet op de bevoegdheidsuitbreidingen die op stapel staan, is er weinig reden daaraan te twijfelen – komt de privacy van burgers in een aantal opzichten verder onder druk te staan.

Zoals al eerder gezegd, moeten burgers er rekening mee houden dat ze veel gemakkelijker dan voorheen betrokken kunnen raken bij opsporingsonderzoeken door politie, justitie en veiligheidsdiensten. De bevoegdheidsuitbreidingen hebben onder meer tot gevolg dat onderzoek zich kan richten op *potentiële* verdachten. Hieronder kunnen personen vallen die op een of andere manier in relatie staan tot een verdachte. Maar in het kader van de 'proactieve' verkenningen waarvan de Raad van Hoofdcommissarissen voorstander is, kan het ook gaan om 'gewone' burgers die niets met een verdachte te maken hebben, maar toevallig op het verkeerde moment op de verkeerde plaats zijn, in het verkeerde

· Bw. Studie 49 23-01-2007 14:40 Pagina 68

bestand staan genoteerd, of tot een bepaalde etnische of religieuze groep behoren.

Daarbij komt dat de manieren waarop burgers bij dergelijke onderzoeken betrokken kunnen raken, gevarieerder zijn dan voorheen. Ze kunnen worden gefilmd of afgeluisterd; verkeersgegevens van telefoon- of internetcommunicatie mogen worden opgeslagen en geanalyseerd, net als gegevens over financiële transacties, reisgedrag of leengedrag bij bibliotheken. Al deze gegevens kunnen worden vergeleken met bepaalde risicoprofielen, bijvoorbeeld om na te gaan of iemand 'aanleg' heeft om terreurdaden of andere misdrijven te plegen. Burgers worden als gevolg hiervan steeds doorzichtiger voor speurders en terreurbestrijders.

Door de beperkte transparantie van het informatiebeheer bij justitiële diensten en de beperkte wettelijke verplichtingen tot inzage en notificatie – en de slechte naleving daarvan – zullen betrokkenen vaak niet weten dat zij worden onderzocht. Maar alleen al het besef steeds vaker onderworpen te *kunnen* worden aan justitiële onderzoeken vormt reeds een bedreiging voor de privacy. Dit verkleint de mogelijkheden van mensen om ongestoord en onbespied zichzelf te zijn en te doen waar ze zin in hebben. Waarden als vrijheid en individualiteit komen zo in het geding.

Door de steeds toenemende omvang en de langere bewaartermijn van gegevensbestanden neemt ook de kans toe dat er achterhaalde of anderszins onjuiste informatie in staat. Dit is niet alleen nadelig voor de opsporings- en veiligheidsdiensten, maar treft ook de privacy van de betrokken personen. Over het algemeen hebben mensen bij de registratie van persoonsgegevens recht op inzage en correctie. Dat recht kan in dit geval echter nauwelijks worden uitgeoefend, omdat betrokkenen veelal niet op de hoogte zullen zijn van het feit dat ze in een bestand voorkomen. Maar door een onjuiste gegevensregistratie – of een onjuiste interpretatie van die gegevens – bestaat wel de kans dat ze ten onrechte met veiligheidsmaatregelen worden geconfronteerd. Met het groeien van de databanken en het verlengen van bewaartermijnen, neemt het risico op dergelijke fouten alleen maar toe. Bovendien zullen de enorme bestanden met persoonsgegevens een steeds aantrekkelijker prooi vormen voor criminelen.

Ten slotte bestaat het risico van function creep, het geleidelijk aan veranderen van de doelstellingen waarvoor informatie wordt verzameld. Op dezelfde wijze als nu informatie van derden door politie, justitie en de veiligheidsdiensten kan worden gebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk is verzameld, kan diezelfde informatie omdat ze 'toch al' bij de genoemde diensten aanwezig is, worden gebruikt voor nog weer andere doeleinden.

· Bw. Studie 49 23-01-2007 14:40 Pagina 69

5.3 Thema's voor het debat

Het in dit boek gegeven overzicht van veiligheidsmaatregelen, de trends die daaruit naar voren komen en de mogelijke gevolgen die de ontwikkelingen tezamen hebben voor de privacy van burgers, onderstrepen de noodzaak van een maatschappelijke discussie over de huidige en de voorgenomen bevoegdheidsuitbreidingen. Essentieel is dat daarbij niet uitsluitend wordt gekeken naar de afzonderlijke maatregelen, maar vooral ook naar hun cumulatieve effect. Hierboven is al betoogd dat de bevoegdheidsuitbreidingen een steeds omvangrijker deel van het persoonlijke leven blootleggen en dat ze het potentieel hebben om daarin steeds dieper door te dringen. Dit betekent dat elk van de maatregelen niet meer afzonderlijk op zijn gevolgen kan worden beoordeeld, maar dat tevens moet worden gekeken naar het versterkende effect dat hij heeft op de privacyaantasting van andere maatregelen. Dan zou kunnen blijken dat de gevolgen van een afzonderlijke maatregel nog wel aanvaardbaar zijn, maar dat zij in combinatie met de gevolgen van andere maatregelen een te grote inbreuk op de privacy betekenen.

Hierbij aansluitend is aandacht nodig voor de nog altijd voortschrijdende informatisering. De toenemende toegankelijkheid van persoonsgegevens en de enorme groei van informatie over individuen die in de nabije toekomst kan worden gegenereerd, plaatsen de huidige bevoegdheden en maatregelen met betrekking tot het vorderen van gegevens in een nieuw perspectief. De reeds bestaande bevoegdheden om gegevens te vorderen bij derden, geven opsporingsdiensten nu al bijna ongehinderde toegang tot alle mogelijke informatie die over burgers verkrijgbaar is. Het wachten is slechts op ontwikkelingen in de technologie die de hoeveelheid informatie en de kwaliteit ervan nog verder vergroten of de toegang daartoe vergemakkelijken.

De effectiviteit van de maatregelen op het gebied van opsporing en veiligheid verdient nader onderzoek. Vergroten deze maatregelen inderdaad de veiligheid? Hierover is maar weinig bekend. Als een van de weinigen heeft de Rotterdamse strafrechtdeskundige Paul Mevis in reactie op de Wet identificatieplicht en de Wet bevoegdheden vorderen gegevens de effectiviteit van deze maatregelen – of het gebrek daaraan – aan de orde gesteld. Mevis schildert beide maatregelen af als symboolwetgeving, die vooral bedoeld is om een signaal af te geven en waarvan de effectiviteit van ondergeschikt belang is. Dergelijke kritiek verdient serieuze aandacht. Dit is eens te meer van belang vanwege de inbreuk op privacy die deze maatregelen met zich meebrengen en de zorgvuldige argumentatie die nodig is om dergelijke inbreuken te kunnen rechtvaardigen. Niets ontbreekt echter duidelijker in de discussie dan inzicht in de – veronderstelde – effectiviteit.

· Bw. Studie 49 23-01-2007 14:40 Pagina 70

Tevens is aandacht nodig voor de procedures via welke de bevoegdheden en maatregelen inzake opsporingsmethoden tot stand komen. Dit geldt vooral voor de regelgeving op Europees niveau. Het is niet zonder betekenis dat, zoals we in het vorige hoofdstuk konden zien, zowel Eerste Kamerleden als leden van het Europees Parlement kritiek uiten op de ondoorzichtige wijze waarop besluiten zijn genomen over bevoegdheidsuitbreidingen. Dit gebrek aan transparantie sluit burgers de facto uit van deelname aan een discussie die over hun rechten gaat.

De discussie over de maatregelen is tot nu toe slechts in beperkte kring gevoerd en sterk juridisch van karakter. Het debat is doorspekt met juridisch jargon, concentreert zich op grondrechten en op de uitgangspunten van het strafrecht. Privacy lijkt nauwelijks een rol te spelen. Omdat de maatregelen zo'n grote betekenis hebben voor de privacy van burgers, zou de discussie daar ook expliciet over moeten gaan.

Politici en beleidsmakers zijn in dit verband snel geneigd te verwijzen naar uitkomsten van publieksonderzoek, waaruit zou blijken dat burgers heden ten dage weinig moeite hebben met maatregelen, zolang die maar ten goede komen aan hun veiligheid. Juist dit beroep op de mening van de burger vraagt echter om vernieuwing van de discussie. Het is immers de vraag of burgers werkelijk in staat zijn gesteld om een weloverwogen oordeel te vellen. Zoals gezegd is er weinig bekend over de effectiviteit van de opsporings- en veiligheidsmaatregelen en is er tot nu toe weinig aandacht geweest voor het cumulatieve effect van de maatregelen. Burgers zijn vaak ook nauwelijks op de hoogte van wat er allemaal speelt. Van een doordachte afweging kan van hun kant dan ook nauwelijks sprake zijn. Zoals we in dit hoofdstuk hebben kunnen zien, is het recht op privacy geen absolute waarde. Inbreuken op privacy behoeven echter wel een zorgvuldige argumentatie – juist omdat privacy zo'n fragiele waarde blijkt te zijn. Dat vereist dat over alle argumenten – voor en tegen – in alle openheid wordt gediscussieerd.

· Bw. Studie 49 23-01-2007 14:40 Pagina 71

Summary

The control of organized crime and terrorism is high on the national and international political agenda. Over the past few years, the Dutch government has approved numerous laws that have drastically increased the intelligence-gathering powers of the police, judiciary and intelligence services.

The extension of these powers can have far-reaching consequences for the constitutional rights and privacy of individuals. Yet to date, the public discussions about these measures have been very limited. And if a discussion arises, it mostly concerns just one individual measure; how these measures interact and possibly reinforce each other is not considered. However, a well-considered opinion about the security measures and how these affect the privacy of individuals requires an understanding of these cumulative effects. This study meets this need.

The scope of the research is defined by two considerations. Based on the assumption that the availability of intelligence-gathering and investigation techniques forms an important factor in the extension of powers, the research mainly focuses on technology-related measures. Additionally the consequences of security measures for the 'ordinary' member of the public form a central theme.

Overview of measures

The study provides an overview of the government measures in the area of intelligence and security policy. Three periods are distinguished in relation to this.

The period from the 1960s through to the mid-1980s was relatively stable and quiet. The police and the judiciary used well-known and long-established practices such as house searches, observation and warrants to hand over material. More far-reaching detection methods (eavesdropping and tapping phone lines) were considered to be highly intrusive and – partly in view of the consequences for individual privacy – were subject to restrictive measures. This picture largely applied to the powers of the security services as well.

Since about 1990 the situation has changed drastically. Laws and amendments to extend existing powers or introduce new ones were adopted in quick succession. These made it easier for the police, judiciary and security services to use DNA tests, camera surveillance, taps, covert entry operations and computer research, and made it possible to link files and to obtain data from third parties. The terrorist attacks in the United States, Spain and the United Kingdom

and the murder of Theo van Gogh served to strengthen this trend. However, a large number of these security measures were in preparation or even in force well before 2001.

Finally, the study provides a brief description of developments that can be expected over the next few years, including the introduction of the citizen service number and the biometric passport, and a further extension of the powers of the intelligence services.

Trends

The overview of the intelligence and security measures reveals a number of trends that seem likely to continue over the next few years:

- Intelligence gathering is increasingly extending to people who are not suspects but are part of the suspects' environment.
- The research is increasingly adopting an exploratory character, in which potentially suspect groups are being monitored on the basis of risk profiles.
- Legal restrictions on the use of certain detection methods are being eased or lifted.
- Intelligence services are acquiring more and more opportunities, both legal and technical, to carry out (independent) investigations.
- Intelligence services increasingly have access to information from other government and semi-privatized services that has been collected for purposes other than intelligence.
- Intelligence services are increasingly forcing other parties to cooperate in investigations.

For the average private individual not under suspicion two developments are important: the use of new technologies (DNA tests, cameras, data mining, linking of files) and the use that the police, judiciary and security services make of the advancing digitization of the administrations of government and private organizations. Thanks to these technological advances it is easier to collect information on a bigger scale than ever before. Consequently people can more quickly become the subject of an investigation, without them knowing anything about this.

Public responses

A number (but by far not all) of security measures have led to public responses. These mainly allude to the potentially problematic integration of the measures within the basic principles of criminal law and the limited transparency of the national and European political decision-making process. Three things are striking:

- Almost without exception the discussion focuses on individual measures and not on the sum effect of measures.
- The discussion mainly takes place within closed legal circles.
- Individual privacy scarcely plays a significant role in the debate.

· Bw. Studie 49 23-01-2007 14:40 Pagina 73

Consideration for privacy

To gain a better understanding of the consequences of security measures for individual privacy, the study considers the concept of privacy in greater detail. The authors characterize privacy as the principle value of the protection of the personal life sphere. However this protection is not absolute in nature. Infringements of privacy are permitted, if good reasons can be given for this.

How the balance between privacy and other interests should be sought, depends upon the exact context concerned. Accordingly various cautionary criteria should be observed. Yet finding the right balance requires an open discussion of all aspects, in which all arguments for and against are heard. It should not be forgotten that infringements of privacy damage personal rights or interests and therefore require careful justification.

An agenda for debate

In the present political and public debate about intelligence and security measures such an openness is lacking. As a result there is no well-considered opinion about the security measures and the effects of this for individual privacy. In view of the ongoing extension of powers of the police, judiciary and security services, the need for a discussion about this is greater than ever before.

The debate should at least consider the following subjects:

- It is essential that the cumulative effect of the intelligence and security measures is examined. Individual measures must be assessed for the extent to which they strengthen the privacy-infringement of other measures.
- Following on from this, attention should be given to the advancing digitization of data files. The existing powers to obtain data from third parties, already provide intelligence services with almost unlimited access to all information that can be obtained about private individuals.
- The efficacy of security measures also demands attention. Do increased measures really lead to improved security? This is important due to the infringement of privacy associated with these measures and the careful argumentation needed to justify such infringements.
- More transparency is needed with respect to the national and European procedures through which the extended powers come into being. These procedures are characterized by a considerable veil of secrecy, which excludes the public from the discussion.
- The closed circles in which the debate about security measures takes place need to be opened up. The debate needs to be extended in order to give the public a say. After all it is their privacy and safety that are at stake.

· Bw. Studie 49 23-01-2007 14:40 Pagina 74

· Bw. Studie 49 23-01-2007 14:40 Pagina 75

Noten

1 Wetsvoorstel Strafbaarstelling verheerlijking zeer ernstige misdrijven en ontzetting uit het beroep.
2 Wetsvoorstel Verruiming bevoegdheden bij opsporing en vervolging terroristische misdrijven, Wetsvoorstel Bestuurlijke maatregelen nationale veiligheid.
3 Bij de inwerkingtreding van het nieuwe Wetboek van Strafvordering; art. 100 lid 3 Sv.
4 Kamerstukken II 1913/14, 286, nr. 3, p. 92.
5 Wet van 7 april 1971, houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer, *Staatsblad,* 1971, 180. Bij deze wet werd ook de bevoegdheid tot het vorderen van telefonie-inlichtingen verplaatst naar art. 125f Sv en geherformuleerd, onder andere door toevoeging van de eis van vermoedelijke deelname van de verdachte aan het desbetreffende telefonieverkeer.
6 Kamerstukken II 1966/67, 8911, nr. 3, p. 7.
7 Art. 125g Sv.
8 Kamerstukken II 1966/67, 8911, nr. 3, p. 7.
9 Kamerstukken II 1967/68, 9419, nr. 3, p. 6.
10 Kamerstukken II 1967/68, 9419, nr. 3, p. 6.
11 HR 2 juli 1990, NJ 1990, 751 ('Wangslijm').
12 Art. III-3 lid 3.
13 Afluisteren van telefoongesprekken: art. 139c lid 2 Sr, direct afluisteren: art. 139a tweede lid onder 3° en art. 139b tweede lid Sr (Wet van 7 april 1971, houdende enige strafbepalingen tot bescherming van de persoonlijke levenssfeer, *Staatsblad,* 1971, 180).
14 Kamerstukken II 1967/68, 9419, nr. 3, pp. 5-6.
15 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Staatsblad,* 2000, 302.
16 Richtlijn 95/46/EC van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
17 Het zogenoemde Wangslijmarrest: HR 2 juli 1990, NJ 1990, 751 ('Wangslijm').
18 Wet van 8 november 1993, *Staatsblad,* 1993, 596.
19 Kamerstukken II 1998/99, 26271, nr. 3, p. 1.
20 Wet van 5 juli 2001, *Staatsblad,* 2001, 335.
21 Wet van 8 mei 2003 tot wijziging van de regeling van het DNA-onderzoek in strafzaken in verband met het vaststellen van uiterlijk waarneembare persoonskenmerken uit celmateriaal, *Staatsblad,* 2003, 201.

· Bw. Studie 49 23-01-2007 14:40 Pagina 76

22 Wet van 16 september 2004, houdende regeling van DNA-onderzoek bij veroordeelden, *Staatsblad,* 2004, 465.
23 Cijfers over de forensische DNA-databank zijn te vinden op <http://www.dnasporen.nl>.
24 *Staatsblad,* 2005, 18 en *Staatsblad,* 2006, 220.
25 Kamerstukken II 2002/03, 28 685, nr. 3, p. 10.
26 Notitie Cameratoezicht, Kamerstuk 1997-1998, 25760, nr. 1, Tweede Kamer, Cameratoezicht; Brief minister en staatssecretaris; Kamerstuk 2003-2004, 29440, nr. 3, Tweede Kamer, Wijziging Gemeentewet en Wet politieregisters in verband met cameratoezicht op openbare plaatsen; Memorie van toelichting, p.1.
27 'Cameratoezicht op openbare plaatsen' (29440). <http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vgyunkpw3vbj>.
28 De Vereniging van Nederlandse Gemeenten (VNG) heeft een Handreiking Cameratoezicht opgesteld om gemeenten inzicht te verschaffen in de mogelijkheden en beperkingen van cameratoezicht en in de wettelijke eisen waaraan het gemeentelijk cameratoezicht moet voldoen: Handreiking cameratoezicht Uitgave 2006, VNG. <http://www.vng.nl/Documenten/Extranet/Bjz/Oov/toezichthandreikingcameratoezicht.pdf>.
29 In dergelijke gevallen, waarbij steeds een concrete aanleiding kan worden aangewezen, kan de bevoegdheid tot – kortstondig toegepast – cameragebruik worden ontleend aan artikel 2 van de Politiewet 1993.
30 Commissie computercriminaliteit 1987.
31 Kamerstuk 21551, nr. 3, Tweede Kamer.
32 Kamerstuk 1998-1999, 26671, nr. 3, Tweede Kamer, Wijziging wetten i.v.m. nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II); Memorie van toelichting.
33 Kamerstuk 1998-1999, 26671, nr. 3, Tweede Kamer, Wijziging wetten i.v.m. nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II); Memorie van toelichting, pp. 2-3.
34 Het betreft een wijziging van het Wetboek van Strafvordering, officieel aangeduid als Wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden); *Staatsblad,* 1999, 245.
35 Factsheet Wet bijzondere opsporingsbevoegdheden (BOB), ministerie van Justitie. <http://www.justitie.nl/publicaties/brochures_en_factsheets/factsheets/wet_bob.asp>.
36 Artikel 25 en 26 WIV 2002.
37 Wet op de uitgebreide identificatieplicht. <http://www.eerstekamer.nl/9324000/1/j9vvgh5ihkk7kof/vgm4jptfvuyk>.
38 Wet van 16 juni 1994 (mobiele telecommunicatie), *Staatsblad,* 1994, 628, en Wet van 23 november 1995 (aftappen van GSM), *Staatsblad,* 1995, 594.

· Bw. Studie 49 23-01-2007 14:40 Pagina 77

39 Zie hoofdstuk 13 Telecommunicatiewet, Wet van 19 oktober 1998 (Telecommunicatiewet), *Staatsblad,* 1998, 610, gebaseerd op het 'Beleidsvoornemen bevoegd aftappen telecommunicatie' uit 1995, Kamerstukken II 1995/96, 24679, nr. 1.

40 <http://www.xs4all.nl/nieuws/bericht.php?taal=nl&id=616&msect=nieuws> en <http://www.xs4all.nl/nieuws/pdf/XS4ALLdagvaarding.pdf>.

41 Wet vorderen gegevens telecommunicatie, *Staatsblad,* 2004, 105. Voor die tijd waren aanbieders overigens ook al verplicht mee te werken op basis van art. 125f/126n/126u Sv juncto art. 184 Sr.

42 Zie ook: *Opzet CIOT in proeffase verantwoord*, CBP. <http://www.cbpweb.nl/documenten/adv_z1999-0270.stm>, <http://www.cbpweb.nl/documenten/adv_z1999-0655.stm>.

43 Volgens artikel 11 Besluit verstrekking gegevens telecommunicatie (*Staatsblad,* 2000, 71, inwerkingtreding 1 september 2004) hoeven internetaanbieders niet mee te werken met het CIOT; deze ontheffing geldt voor een periode van twee jaar (art. 12 lid 2 Besluit), dus tot 1 september 2006.

44 Tapcijfers Nederland 1998. <http://www.bof.nl/docs/aftapbrief.gif>.

45 Kamerstuk 2001-2002, 27925, nr. 10, Tweede Kamer, Bestrijding internationaal terrorisme; Brief ministers met 'Actieplan terrorismebestrijding en veiligheid', p.14; de wet is opgenomen in *Staatsblad* 109 van 25 maart 2004 en is per 1 juni 2004 in werking getreden.

46 Tractatenblad 2001, 187, Protocol bij Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen lidstaten Europese Unie; 16 oktober 2001.

47 Tractatenblad 2000, 96, Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen lidstaten Europese Unie; 29 mei 2000.

48 Kamerstuk 2001-2002, 28353, nr. 3, Tweede Kamer, Wijziging Wetboek Strafvordering i.v.m. regeling bevoegdheden tot vorderen gegevens financiële sector; Memorie van toelichting; Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, ministerie van Justitie. <http://www.justitie.nl/pers/persberichten/archief/2001/gegevens.pdf > [Rapport "Commissie-Mevis"].

49 De wet is opgenomen in *Staatsblad* 390 van 2 augustus 2005 en is per 1 januari 2006 in werking getreden.

· Bw. Studie 49 23-01-2007 14:40 Pagina 78

50 Rapport van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, ministerie van Justitie. <http://www.justitie.nl/pers/persberichten/archief/2001/gegevens.pdf>; Kamerstuk 2001-2002, 28366, nr. 1, Tweede Kamer, Gegevensvergaring in strafvordering; Kabinetsstandpunt over het rapport 'Gegevensvergaring in strafvordering' van de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij; Kamerstuk 2003-2004, 29441, nr. 3, Tweede Kamer, Wijziging Wetboek van Strafvordering en enkele andere wetten in verband met bevoegdheden tot het vorderen van gegevens; Memorie van toelichting.
51 Kamerstuk 2001-2002, 28353, nr. 3, Tweede Kamer, Wijziging Wetboek Strafvordering i.v.m. regeling bevoegdheden tot vorderen gegevens financiële sector; Memorie van toelichting, pp. 2-3.
52 <http://ec.europa.eu/comm/external_relations/us/intro/pnr.htm>.
53 <http://curia.eu.int/nl/actu/communiques/cp06/aff/cp060046nl.pdf>.
54 Kamerstukken II 2001/02, 21 501-10, nr. 72, p. 5.
55 Tractatenblad 2000, 96, Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen lidstaten Europese Unie; 29 mei 2000.
56 Wet burgerservicenummer (voorstel, Memorie van toelichting, Advies en nader rapport), Recht.nl. <http://www.recht.nl/22064>.
57 Wetsvoorstel burgerservicenummer, *Bits of Freedom Nieuwsbrief*, nr. 3.18, 28 september 2005. <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_18.html>; Programmabureau Burgerservicenummer. <http://www.programmabsn.nl/>.
58 Website DigiD. <http://www.digid.nl/>.
59 <http://almanak.overheid.nl/WPSServlet?action=document&id=97507>.
60 Kamerstuk 2005-2006, 30553, nr. 2, Tweede Kamer, Wijziging Wet op de inlichtingen- en veiligheidsdiensten 2002 i.v.m. onderzoek naar en maatregelen tegen terrorisme; Voorstel van wet. <http://www.bof.nl/docs/KST97274.pdf>; Kamerstuk 2005-2006, 30553, nr. 3, Tweede Kamer, Wijziging Wet op de inlichtingen- en veiligheidsdiensten 2002 i.v.m. onderzoek naar en maatregelen tegen terrorisme; Memorie van toelichting. <http://www.bof.nl/docs/KST97275.pdf>; Kamerstuk 2005-2006, 30553, nr. 4, Tweede Kamer, Wijziging Wet op de inlichtingen- en veiligheidsdiensten 2002 i.v.m. onderzoek naar en maatregelen tegen terrorisme; Advies en nader rapport <http://www.bof.nl/docs/KST97276.pdf>; Conflict over tapvergoedingen loopt hoog op (16 mei 2006). <http://automatiseringgids.sdu.nl/ag/nieuws/nieuws/toon_nieuwsbericht.jsp?di=190819>; AIVD mag databestanden opeisen (29.03.2006) <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2006_7.html>.

61 Kamerstuk 2003-2004, 29200 VII, nr. 61, Tweede Kamer, Vaststelling begroting van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2004; Brief minister over wetgeving m.b.t. inlichtingen- en veiligheidsdiensten.
62 Richtlijn 2006/24/EG, *PubEG* L105/54, 13 april 2006.
63 Kaderbesluit betreffende uitwisseling van informatie volgens beschikbaarheidsbeginsel (Ministerie van BuZa). <http://www.minbuza.nl/default.asp?CMS_ITEM=95F809B601B04E438B485EB62693B986X3X39891X83>.
64 Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten. <http://europapoort.eerstekamer.nl/9345000/1/j9vvgy6i0ydh7th/vgbwr4k8ocw2/f=/vgwvieggthwf.pdf>.
65 EU Visa Information System gets go-ahead, IDABC. <http://europa.eu.int/idabc/en/document/2186/330>.
66 Databank achter de schermen, IKON. <http://www.ikonrtv.nl/daw/uitzending.asp?lIntItem=2&lIntEntityId=9>.
67 Commissie Criminaliteit en Technologie, 2005, p. 11.
68 Projectgroep Forensische Opsporing Raad van Hoofdcommissarissen (2004).
69 Ib., pp. 20-26.
70 Ib., pp. 37-43.
71 Ib., pp. 41-42.
72 Brief CBP. <http://www.recht.nl/proxycache.html?cid=28125>.
73 Nederlandse Vereniging voor Rechtspraak (2002).
74 Working Party on Police, Workshop video surveillance, Greater Manchester Police, 1 oktober 2003.
75 'Cameratoezicht, steeds goedkoper, rukt op'. *Netkwesties*, 14 januari 2005. <http://www.netkwesties.nl/editie118/artikel1.html>.
76 Beleidsreactie evaluatie Wet bijzondere opsporingsbevoegdheden, ministerie van Justitie. <http://www.recht.nl/proxycache.html?cid=34797>.
77 'De AIVD in verandering'. Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst, ministerie van BZK. <http://www.minbzk.nl/contents/pages/10430/aivdinveranderingbw.pdf>.
78 'Mevis erkent schaduwzijden van advies: "Het gevaar zit vooral in de perfectie" ', *Netkwesties*, Editie 72, 30 oktober 2003.
79 <http://www.id-nee.nl/algemeen.html>.
80 Memorie van toelichting Wet Bescherming persoonsgegevens. <http://www.cbpweb.nl/downloads_wetten/wbp_mvt.pdf >; CBP, Advies 'Rode Lamp' (9 september 2002). <http://www.cbpweb.nl/downloads_uit/z2001-1157.pdf>.

· Bw. Studie 49 23-01-2007 14:40 Pagina 80

81 'Twee wetsvoorstellen vorderen gegevens aangenomen'. *Bits of Freedom Nieuwsbrief*, nr. 2.6, 17 maart 2004. <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2004_6.html>; zie ook: Kamerstuk 2002-2003, 28353, nr. 83a, Eerste Kamer, Wijziging Wetboek Strafvordering i.v.m. regeling bevoegdheden tot vorderen gegevens financiële sector; Voorlopig verslag; Kamerstuk 2002-2003, 28353, nr. 83b, Eerste Kamer, Wijziging Wetboek Strafvordering i.v.m. regeling bevoegdheden tot vorderen gegevens financiële sector; Memorie van antwoord.

82 *Advies Wetsvoorstel vorderen gegevens telecommunicatie*, Den Haag: Registratiekamer, 16 november 2000. <http://www.cbpweb.nl/downloads_adv/z2000-0478.pdf>.

83 Kamerstuk 2003-2004, 28059, nr. A, Eerste Kamer, Wijziging van o.a. Wetboek van Strafvordering i.v.m. aanpassing bevoegdheden vorderen gegevens telecommunicatie; Memorie van antwoord.

84 'Een garantie voor de toekomst'. *Netkwesties*, Editie 60, 1 mei 2003. <http://www.recht.nl/proxycache.html?cid=20583>.

85 'Mevis erkent schaduwzijden van advies: "Het gevaar zit vooral in de perfectie"'. *Netkwesties*, Editie 72, 30 oktober 2003.

86 Frank Kuitenbrouwer, 'Moderne Inquisitie'. <http://rechten.uvt.nl/gegeven/html/reactie_kuitenbrouwer.htm>

87 Kamerstuk 1997-1998, 25880, nr. 2, Tweede Kamer, Wetgeving voor de elektronische snelweg; Nota 'Wetgeving voor de elektronische snelweg'.

88 'Gegevens 250 bibliotheekbezoekers opgeëist bij strafrechtelijk onderzoek'. <http://recht.nl/24262>.

89 <http://sitegenerator.bibliotheek.nl/fobid/overig33/overig33.asp#Aanwijzingen>.

90 Zie bijvoorbeeld <http://www.bezwaarplicht.nl/>.

91 <http://www.nnm-ev.de/show/135496.html>.

92 <http://www.edri.org/docs/German-Parliament_Draft-DR-Resolution_18 mei 2006.pdf>.

93 Advies over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende het visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van informatie op het gebied van visa voor kort verblijf, Artikel 29 Groep Gegevensbescherming (COM(2004)835 definitief). <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_nl.pdf>.

94 'Experts: opslag paspoortgegevens doelwit crimineel'. Nieuws.nl, 27 april 2006. <http://www.beveiligingnieuws.nl/beveiliging_nieuws.php?item=3254>.

95 Gerard van Westerloo, 'Het hoogste woord: De Hoogste Raad over zijn beperkte bevoegdheden en het verlangen naar meer invloed'. In: *NRC Zaterdag Magazine*, 6 mei 2006, pp. 16-32.

96 'Een ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van de persoonlijke levenssfeer' (art. 10 lid 1 Gw); 'Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.' (art. 8 lid 1 EVRM).

· Bw. Studie 49 23-01-2007 14:40 Pagina 81

Literatuur

Albrecht, H.J., C. Dorsch & C. Krüpe (2003). *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation*. Freiburg: Max-Planck-Institut, p. 104. (http://www.iuscrim.mpg.de/verlag/online/Band_115.pdf).

Asscher, L. & B.J. Koops (2004). 'Gegevens geven: een muisstille revolutie in het strafrecht'. In: *Het Financieele Dagblad,* 1 april 2004.

Brouwer, A. (2006). 'Iedereen TBS'. In: *De Groene Amsterdammer*, 24 maart 2006, pp. 22-25.

Buuren, J. van, B.J. Koops & W. Wagenaar (2004). 'Inlichtingen- en veiligheidsdiensten en ICT'. In: B.J. Koops (red.). *Strafrecht en ICT*. Den Haag: Sdu Uitgeverij, pp. 177-213.

'Cameratoezicht, steeds goedkoper, rukt op' (2004). In: *Netkwesties*, 14 januari 2004. (http://www.netkwesties.nl/editie118/artikel1.html).

College Bescherming Persoonsgegevens (1999). *Opzet CIOT in proeffase verantwoord*. Den Haag, 6 augustus 1999.

Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst (2004). *De AIVD in verandering*. (http://www.minbzk.nl/contents/pages/10430/aivdinveranderingbw.pdf).

Commissie Computercriminaliteit (1987). *Informatietechniek & Strafrecht*. Staatsuitgeverij (z.p.).

Commissie Criminaliteit en Technologie (2005). *Technologie en misdaad. Kansen en bedreigingen van technologie bij de beheersing van criminaliteit*. Den Haag. (http://www.omv.nl/Website/Dutch/nieuws/Aktualiteiten/Advies%20Winsemius.pdf).

Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij (2001). *Gegevensvergaring in strafvordering; Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*. Den Haag: Ministerie van Justitie. (http://www.justitie.nl/pers/persberichten/archief/2001/gegevens.pdf).

Dubbeld, L. (2004). *The regulation of the observing gaze: privacy implications of camera surveillance*. Enschede: Universiteit Twente.

· Bw. Studie 49 23-01-2007 14:40 Pagina 82

Ekker, A.H. (2002). 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten'. *Computerrecht* 2002, nr. 2, p. 77.

Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.

Groep gegevensbescherming van artikel 29 (2005). *Advies 2/2005 over het voorstel voor een verordening van het Europees Parlement en de Raad betreffende het visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van informatie op het gebied van visa voor kort verblijf (COM(2004)835 definitief)*. Brussel: Directoraat Generaal Justitie. (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp110_nl.pdf).

Gunsteren, H. van (2005). 'Het gevaar schuilt in vergissingen en frustraties'. In: *NRC Handelsblad*, 25 oktober 2005.

IDABC (2004). *EU Visa Information System gets go-ahead*. (http://europa.eu.int/idabc/en/document/2186/330).

IKON (2006). *Databank achter de schermen*. (http://www.ikonrtv.nl/daw/uitzending.asp?lIntItem=2&lIntEntityId=9).

Johnson, J.L. (1989a). 'Privacy and the Judgements of Others'. In: *The Journal of Value Inquiry* 1989, pp. 157-168.

Johnson, J.L. (1989b). 'Privacy, Liberty and Integrity'. In: *Public Affairs Quarterly* 1989, pp. 15-34.

Johnson, J.L. (2001). 'Immunity from the Illegitimate Focused Attention of Others: An Explanation of Our Thinking and Talking About Privacy'. In: Vedder (ed.). *Ethics and the Internet*. Antwerpen: Intersentia.

Koops, B.J. & A. Vedder (2001). *Opsporing versus privacy: de beleving van burgers*. Den Haag: Sdu Uitgeverij.

Koops, B.J. (2002). *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*. Deventer: Kluwer, p. 335.

Koops, B.J. et al. (2005). *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*. Tilburg: TILT/Dialogic. (http://arno.uvt.nl/show.cgi?fid=46971).

Kuitenbrouwer, F. (2003). 'Moderne Inquisitie'. (http://rechten.uvt.nl/gegeven/html/reactie_kuitenbrouwer.htm).

· Bw. Studie 49 23-01-2007 14:40 Pagina 83

Lamboo, M. (2004). 'Opsporing effectiever door koppeling DNA en vingersporen'. In: *Justitie Magazine*, maart 2004. (http://dnasporen.nl/docs/nieuws/LSDB-artikel%20Justitie%20magazine.pdf).

Lamboo, M. (2005). 'Een goudmijn voor de opsporing'. In: *Justitie Magazine,* november 2005. (http://www.dnasporen.nl/docs/literatuur/Een%20goudmijn%20voor%20de%20op-sporing.pdf).

MacGillavry, E.C. (2001). 'De voorstellen van de commissie-Mevis: dwangmiddelen voor de informatiemaatschappij'. In: *Nederlands Juristenblad,* nr. 30, 31 augustus 2001.

Ministerie van Economische Zaken (2006). *Verbetering aanpak cybercrime*. (http://www.minez.nl/content.jsp?objectid=41718).

Ministerie van Justitie. *Beleidsreactie evaluatie Wet bijzondere opsporingsbevoegdheden*. (http://www.recht.nl/proxycache.html?cid=34797).

Ministerie van Justitie. *Factsheet Wet bijzondere opsporingsbevoegdheden (BOB)*. (http://www.justitie.nl/publicaties/brochures_en_factsheets/factsheets/wet_bob.asp).

Mommers, L. (2006). 'Burgerservicenummer levert weinig service en veel risico's'. In: *NRC Handelsblad*, 30 mei 2006, p. 7.

Nas, S. (2003). 'Een garantie voor de toekomst'. In: *Netkwesties*. Editie 60. (http://www.recht.nl/proxycache.html?cid=20583).

Nederlandse Vereniging voor Rechtspraak (NVvR) (2002). *Advies inzake wijziging regeling DNA-onderzoek bij verdachten*. (http://www.nvvr.org/nlNL/Content.aspx?type=RecommendationSummary&id=34&idKey=39&mid=37).

Parent, W.A. (1983). 'Recent Work on the Concept of Privacy'. In: *American Philosophical Quarterly* 1983, pp. 341-355.

Perri 6 (1998). *The Future of Privacy*. Londen: Demos.

Prins, J.E.J. (2003). 'Editorial - Het BurgerServiceNummer en de strijd tegen de Identiteitsfraude'. In: *Nederlands Juristenblad*, aflevering 1, 2003.

Prins, J.E.J. (2004). 'De stilzwijgend uitdijende opsporingsvergaarbak'. In: *Nederlands Juristenblad*, aflevering 16, 16 april 2004.

· Bw. Studie 49 23-01-2007 14:40 Pagina 84

Projectgroep Forensische Opsporing Raad van Hoofdcommissarissen (2004). *Spelverdeler in de opsporing. Een visie op forensische opsporing*. (Z.p.) (http://www.politie.nl/Overige/Images/33_144778.pdf).

Registratiekamer (2000). 'Advies Wetsvoorstel vorderen gegevens telecommunicatie'. 16 november 2000. (http://www.cbpweb.nl/downloads_adv/z2000-0478.pdf).

Rössler, B. (2001). *Der Wert des Privaten*. Frankfurt am Main: Suhrkamp.

Schildmeijer, R., C. Samson & H. Koot (2005). *Burgers en hun privacy. Opinie onder burgers.* Amsterdam: TNS NIPO.

Simmelink, J.B.H.M. & F.P.E. Wiemans (1990). 'De strafvorderlijke voorstellen'. In : F.P.E. Wiemans (red.). *Commentaren op het wetsvoorstel computercriminaliteit*. IDP (z.p.).

Smeets, A.C.H.M. (2004). *Camera's in het publieke domein. Privacynormen voor het cameratoezicht op de openbare orde.* Den Haag: College Bescherming Persoonsgegevens.

Smits, A. (2006). *Strafvorderlijk onderzoek van telecommunicatie.* Dissertatie (Tilburg). Nijmegen: Wolf Legal Publishers.

Spaink, K. (2005). 'Het sofi-nummer maakt promotie'. In: *Het Parool*, 13 december 2005. (http://blogger.xs4all.nl/kspaink/archive/2005/12/13/70402.aspx).

Spaink, K. (2006). 'Wie neemt het op tegen Big Brother?'. In: *de Volkskrant*, 28 januari 2006.

Stol, W. Ph., N. Kop & P.A. Koppenol (2005). *Eén spoor is geen spoor: naar een landelijke sporendatabank voor informatiegestuurde opsporing*. WODC (z.p.). (http://www.wodc.nl/images/1203_volledige%20tekst_tcm11-106275.pdf).

Trommelen, J. (2006a). 'Identificatieplicht is vooral boetefuik'. In: *de Volkskrant,* 22 april 2006. (http://www.volkskrant.nl/binnenland/article290577.ece).

Trommelen, J. (2006b). 'Toeval speelt rol bij ID plicht'. In: *de Volkskrant*, 22 april 2006. (http://www.volkskrant.nl/binnenland/article-290573.ece).

Trommelen, J. (2006c). 'In Tiel kun je maar beter niet je paspoort kwijtraken'. In: *de Volkskrant,* 24 april 2006. (http://www.volkskrant.nl/binnenland/article291635.ece).

· Bw. Studie 49 23-01-2007 14:40 Pagina 85

Trommelen, J. (2006d). 'Groot verschil in 'boetes' bij verlies paspoort'. In: *de Volkskrant*, 24 april 2006. (http://www.volkskrant.nl/binnenland/article291651.ece).

'Twee wetsvoorstellen vorderen gegevens aangenomen' (2004). In: *Bits of Freedom Nieuwsbrief*. Nr. 2.6, 17 maart 2004. (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2004_6.html).

Vedder, A. (1997). 'Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations'. In: Geoff Moore (ed.) *Business Ethics: Principles and Practice*. Sunderland: Business Education Publishers Ltd, pp. 215-226.

Vedder, A. (1998). 'Het einde van de individualiteit? Groepsprofilering, datamining en de vermeerdering van brute pech en dom geluk'. In: *Privacy en informatie* 1 nr. 3, pp. 115-120.

Vedder, A. (2000). 'Medical Data, New Information Technologies and the Need for Normative Principles Other than Privacy Rules'. In: Freeman and Lewis (Eds.). *Law and Medicine.* (Series Current Legal Issues). Oxford: Oxford University Press, pp. 441-459.

Vedder, A. (2004). 'KDD, Privacy, Individuality, and Fairness'. In: Spinello et al. (Eds.). *Readings in CyberEthics.* Second Edition. Sudbury, Mass. / Boston / Toronto / London / Singapore: Jones and Bartlett Publishers, pp. 462-470. (Reprint).

Vedder, A. & B.J. Koops (2001). 'Burgers over opsporing en privacy.' In: *Privacy en Informatie* 4, nr. 4, pp. 152-155.

Vedder, A. & P. Blok (2005). 'Privacy en ICT'. In: M. Lips, V. Bekkers & A. Zuurmond. *ICT en Openbaar Bestuur: Implicaties en uitdagingen van technologische toepassingen voor de overheid.* Utrecht: Lemma, pp. 623-650.

Vereniging van Nederlandse Gemeenten (VNG), de (2006). 'Handreiking cameratoezicht'. (http://www.vng.nl/Documenten/Extranet/Bjz/Oov/toezichthandreikingcameratoezicht.pdf).

Vermeulen, M.L. (2005). *Rechtsbescherming op de helling – effecten van anti-terreurwetgeving opgeteld.* Briefing-paper over de effecten van vijf (voorgestelde) anti-terreurwetten op de handhaving van mensenrechtenbepalingen. Utrecht: Humanistisch Overleg Mensenrechten.

Warren, S.D. & L.D. Brandeis (1890). 'The Right to Privacy. The implicit Made Explicit'. In: *Harvard Law Review* 1890, pp. 193-220; ook in: F.D. Schoeman (red.). *Philosophical dimensions of privacy: an anthology.* Cambridge: Cambridge University Press (1984). pp. 75-103.

· Bw. Studie 49 23-01-2007 14:40 Pagina 86

'Wetsvoorstel Burgerservicenummer' (2005). In: *Bits of Freedom Nieuwsbrief*. Nr. 3.18, 28 september 2005. (http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_18.html).

Wiegers, A. (2003). 'Het gevaar zit vooral in de perfectie'. In: *Netkwesties*. Editie 72, 30 oktober 2003.

WODC (2002). 'Evaluatie van de wet BOB – fase 1: De eerste praktijkervaringen met de Wet Bijzondere opsporingsbevoegdheden'. In: *Onderzoek en beleid*, 197, 2002.

WODC (2004). 'De wet bijzondere opsporingsbevoegdheden – eindevaluatie'. In: *Onderzoek en beleid*, 222, 2004.

· Bw. Studie 49 23-01-2007 14:40 Pagina 87

Adviescommissie

Dr. Benita Plesch (voorzitter)
Bestuurslid Rathenau Instituut

Drs. Siegfried Eschen
Ministerie van Justitie, Directie Algemene Justitiële Strategie

Prof.dr. Hans Franken
Hoogleraar Informatierecht, Rijksuniversiteit Leiden en lid van de Eerste Kamer voor het CDA

Mr.dr. Heleen Janssen
Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Directie Constitutionele Zaken en Wetgeving

Ir. Martijn Kriens
Telematica Instituut

Drs. Anita Regout
College Bescherming Persoonsgegevens

Maurice Wessling
Bits of Freedom

· Bw. Studie 49 23-01-2007 14:40 Pagina 88

· Bw. Studie 49 23-01-2007 14:40 Pagina 89

Over de auteurs

Anton Vedder studeerde wijsbegeerte en geschiedenis in Utrecht en Leuven. Hij promoveerde in 1995 aan de universiteit van Utrecht op een proefschrift over de rol van het vrijheidsbegrip in de recente ethische theorievorming en in enkele actuele maatschappelijke discussies. Sinds 1996 is hij universitair hoofddocent ethiek en recht bij de Faculteit der Rechtsgeleerdheid van de Universiteit van Tilburg.

Leo van der Wees studeerde Nederlands recht aan de Universiteit Leiden. Daarna was hij werkzaam als computerprogrammeur bij Philips en BSO (nu ATOS). Vervolgens is hij als universitair docent Informatica en Recht verbonden geweest aan het Centrum voor Informatica en Recht van de Erasmus Universiteit Rotterdam. Op dit moment is hij onderzoeker bij TILT en tevens directeur van Legal Net Services en Recht.nl, een internetportaal voor juristen.

Bert-Jaap Koops studeerde wiskunde en literatuurwetenschappen aan de Rijksuniversiteit van Groningen. Hij promoveerde in 1999 in Tilburg op een proefschrift over de regulering van encryptie. Hij is sinds 2006 hoogleraar regulering van technologie bij de Universiteit van Tilburg.

Paul de Hert studeerde recht, wijsbegeerte en theologie. Hij promoveerde in 2000 in de rechtsgeleerdheid aan de Vrije Universiteit van Brussel. Hij is momenteel verbonden aan de rechtenfaculteiten van de Vrije Universiteit Brussel en de Universiteit van Tilburg.

· Bw. Studie 49 23-01-2007 14:40 Pagina 90