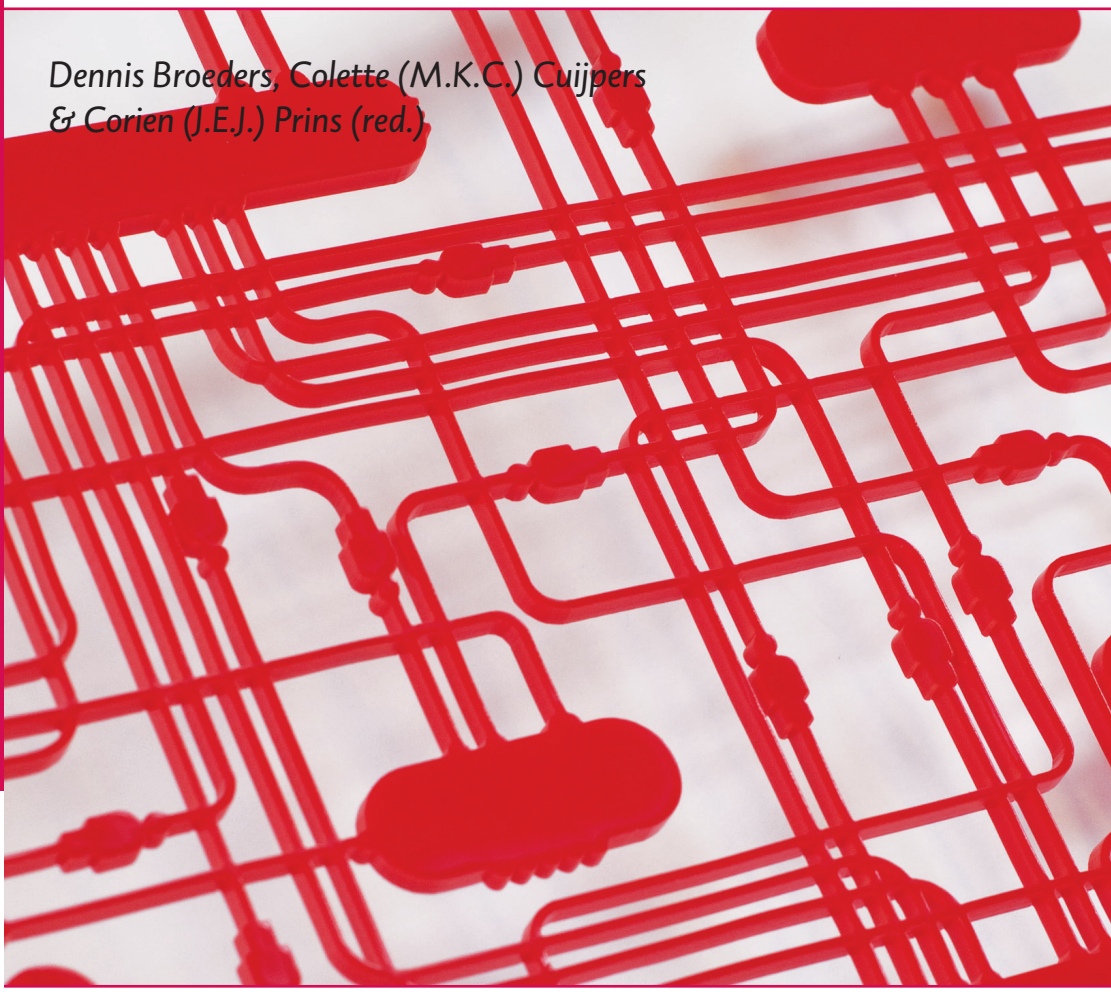
WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

Dennis Broeders, Colette (M.K.C.) Cuijpers & Corien (J.E.J.) Prins (red.)



De staat van informatie

AMSTERDAM UNIVERSITY PRESS

De staat van informatie

De serie 'Verkenningen' omvat studies die in het kader van de werkzaamheden van de WRR tot stand zijn gekomen en naar zijn oordeel van zodanige kwaliteit en betekenis zijn dat publicatie gewenst is. De verantwoordelijkheid voor de inhoud en de ingenomen standpunten berust bij de auteurs.

Wetenschappelijke Raad voor het Regeringsbeleid
De WRR is gevestigd:
Lange Vijverberg 4-5
Postbus 20004
2500 EA 's-Gravenhage
Telefoon 070-356 46 00
Telefax 070-356 46 85
E-mail info@wrr.nl
Website http://www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

De staat van informatie

Dennis Broeders, Colette (M.K.C.) Cuijpers & Corien (J.E.J.) Prins (red.)

Amsterdam University Press, Amsterdam 2011

Omslagafbeelding: Silo – Strategy. Concept. Design

Omslagontwerp: Studio Daniëls, Den Haag
Vormgeving binnenwerk: Het Steen Typografie, Maarssen

ISBN 978 90 8964 310 0
e-ISBN 978 90 4851 409 0
NUR 759 / 754

INHOUDSOPGAVE

Ten geleide 13

1 Inleiding 15
Dennis Broeders, Colette Cuijpers en Corien Prins
1.1 iOverheid 15
1.2 De staat van informatie 16
1.3 Beginselen 18
1.4 Opbouw 22

DEEL I

2 Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting 33
Paul de Hert
2.1 Samenvatting 33
2.2 Wie draagt welke verantwoordelijkheden in de informatiesamenleving? 33
2.2.1 Verantwoordelijkheid voor schendingen mensenrechten multinationals 34
2.2.2 De *state duty to protect*, de *corporate responsibility to respect* en *access to remedy* 35
2.3 Zes lessen voor het debat over de informatiemaatschappij 36
2.3.1 Het Europese mensenrechtenperspectief op verantwoordelijkheid in de informatiesamenleving 39
2.3.2 Regulering vereist soms strafbaarstellingen 41
2.3.3 Eindverantwoordelijkheid en de idee van verantwoordelijkheidsdistributie 42
2.4 Systeemverantwoordelijkheid inzake toegang en publieke privacy: Gaskin en Peck 46
2.4.1 Systeemverantwoordelijkheid betreffende beveiliging: I.t. Finland 47
2.5 Schadevergoeding mag nooit de enige oplossing zijn; de idee van bescherming vooraf 49
2.5.1 Als er schadevergoeding wordt toegekend moet deze redelijk doch substantieel zijn 51
2.5.2 Het arrest *Armonas t. Litouwen* uit 2008: samenvattende beschouwing 52
2.6 Het EU Handvest als opstap naar systeemverantwoordelijkheid van de wetgever 54
2.6.1 'Waarom specifieke biometriewetgeving? De Wbp is toch van toepassing!' 55

2.6.2 Technologie actief tegemoet treden: het voorbeeld van de ePrivacyrichtlijnen 56
2.6.3 Technologie actief tegemoet treden: het voorbeeld van Rfid 58
2.6.4 Spelverdeling van verantwoordelijkheden: het spel keurig afgehaspeld 60
2.7 Verantwoordelijkheden betreffende identiteitsfraude 63
2.7.1 Een niet ondergebracht verantwoordelijkheidsprobleem 63
2.7.2 Identiteit wordt beschermd via artikel 8 EVRM 64
2.7.3 De leer van de positieve plichten toegepast op identiteitsfraude: *K.U. tegen Finland* (2008) 64
2.7.4 Gevolgtrekkingen voor de verantwoordelijkheid bij identiteitsfraude 67
2.8 Verantwoordelijkheden op het gebied van informatie over maatschappelijke aangelegenheden 69
2.8.1 Keuzevrijheid als sleutel tot vergeten 69
2.8.2 De ongelovige reiziger door cyberspace 70
2.8.3 Positieve plichten tot mediapluralisme op grond van artikel 10 EVRM en artikel 11 Handvest 72
2.8.4 Gevolgtrekkingen: systeemverantwoordelijkheid voor mediapluralisme 74
2.9 Algemeen besluit 76

3 Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte 97
Albert Meijer
3.1 Overheidsverantwoordelijkheid in het informatietijdperk 97
3.2 Verantwoordelijkheid als taak, deugd, vermogen en aansprakelijkheid 98
3.3 Gebruiksverantwoordelijkheid: verantwoord gebruik van ICT door de overheid 100
3.3.1 Verantwoordelijkheid als deugd: legaal, neutraal, behoorlijk en transparant gebruik van ICT door de overheid 101
3.3.2 Verantwoordelijkheid als vermogen: nieuwste mogelijkheden benutten of kiezen voor oude zekerheden? 106
3.3.3 Verantwoordelijkheid als aansprakelijkheid: vergroten van effectiviteit of minimaliseren van risico's? 108
3.3.4 Belangrijkste vraagstukken bij gebruiksverantwoordelijkheid voor ICT 109
3.4 Systeemverantwoordelijkheid: overheidsverantwoordelijkheid voor ICT in de samenleving 110
3.4.1 Verantwoordelijkheid als taak: burgers beschermen en oplossingen voor systeemfalen 111
3.4.2 Verantwoordelijkheid als deugd: lege overheid of leiderschap? 116
3.4.3 Verantwoordelijkheid als vermogen: samenwerking of autonomie? 117

3.4.4 Verantwoordelijkheid als aansprakelijkheid: bureaucratisering? 118
3.4.5 Belangrijkste vraagstukken bij systeemverantwoordelijkheid voor ICT 119
3.5 Klassieke organisatiekundige en politiek-filosofische spanningen in een nieuw jasje 121
3.5.1 Gebruiksverantwoordelijkheden: stabiliteit versus flexibiliteit 121
3.5.2 Systeemverantwoordelijkheid: procesmatige verantwoordelijkheid geven versus verantwoordelijkheid nemen 123
3.5.3 Genormeerde experimenteerruimte: intelligent manoeuvreren door onbekend gebied 124

4 Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie 133
Michel van Eeten
4.1 Waar maken we ons druk over? 133
4.2 Is het veilig? 134
4.3 Kosten en baten van onveiligheid 135
4.4 Het nut van decentrale afwegingen rondom veiligheid 137
4.5 Externaliteiten rond veiligheidsrisico's 142
4.5.1 Opkomst van botnets 143
4.5.2 Fraude met online betalingsverkeer 145
4.5.3 Lekken uit databases 149
4.6 Rol van de overheid 151
4.6.1 Ex ante veiligheidsregulering 152
4.6.2 Ex post aansprakelijkheid 154
4.6.3 Verplichte melding van incidenten 154
4.6.4 Aansprakelijkheid van intermediaire actoren 155
4.7 Tot slot 157

5 Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld 165
Ybo Buruma
5.1 Beleid, informatie en technologie: veranderingen 167
5.1.1 Strafrecht in de risicosamenleving 167
5.1.2 Inlichtingenwerk 170
5.1.3 Technologische ontwikkeling 172
5.2 Het geheugen in het digitale tijdvak 174
5.2.1 Biologisch en digitaal vergeten 174
5.2.2 IJkpunten: accuratesse, betrouwbaarheid en controle 177
5.2.3 Specifieke betrouwbaarheidsproblemen: fout positief en fout negatief 178
5.3 Opslag en gebruik van gegevens in de strafrechtsketen 180
5.3.1 Opslag en verwerking van politie- en justitiegegevens: wetgeving 181

5.3.2 Kennisneming, verbetering en verwijdering van politie- en justitiegegevens 183
5.3.3 Het gebruik van politiële en justitiële gegevens 187
5.3.4 Bestandsvergelijking en datamining 190
5.4 Waarom zou vergetelheid wenselijk zijn? 194
5.4.1 Een fundamenteel andere herinnering: overheid en samenleving 194
5.4.2 Privacy: een mensenrecht en een maatschappelijk begrip 197
5.4.3 Privacy en opgeslagen gegevens in het recht 199
5.5 Bezwaren tegen een recht op vergetelheid 202
5.5.1 Bezwaren tegen verwijdering door de overheid als systeemverantwoordelijke 203
5.5.2 Bezwaren tegen verwijdering door de overheid als gebruiker 205
5.6 Conclusie 208

6 Klachten over toepassingen van informatietechnologie: Analyse van een aantal overheidsbestanden 223
Sunil Choenni, Erik Leertouwer en Tony Busker
6.1 Inleiding 223
6.2 Onderzoeksvragen en aanpak 225
6.3 Analyse van geregistreerde klachten 226
6.3.1 CMI 226
6.3.2 CBP 228
6.3.3 Een reflectie op de bestanden 235
6.4 Een eerste stap naar meer inzicht in potentiële klachten 237
6.5 Conclusies 240

DEEL II

7 Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa 249
Dennis Broeders
7.1 Inleiding 249
7.2 Staten, standaarden en industrie 252
7.3 De institutionele setting: van Maastricht naar Lissabon 255
7.3.1 De JBZ-agenda: van Tampere naar Stockholm 257
7.4 Eerste generatie databanken: moeilijke migranten in beeld 259
7.4.1 Schengen Informatie Systeem I en II 260
7.4.2 Eurodac 263
7.4.3 Visum Informatie Systeem 265
7.4.4 Tussenconclusie 267
7.5 Tweede generatie databanken: iedereen in beeld 268
7.5.1 Passenger Name Records (PNR-data) 268

7.5.2 Entry/Exit-systeem 270
7.5.3 Biometrisch paspoort 274
7.5.4 Tussenconclusie 276
7.6 Rol van industrie en adviseurs 277
7.7 Rol van standaarden 279
7.8 Conclusie 282

8 Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet 293
Esther Keymolen en Corien Prins
8.1 Inleiding 293
8.2 Korte schets verwijsindex en context 294
8.2.1 Melden van risico, niet inhoud 295
8.2.2 Wanneer mag men melden? 296
8.2.3 Van proeftuin naar wet 297
8.2.4 Iedere lokale context een eigen systeem 298
8.2.5 Ambities op rijksniveau: preventief ingrijpen door gestroomlijnde informatie-uitwisseling 300
8.2.6 Een divers palet aan ambities op lokaal niveau 302
8.3 De actoren in beeld 305
8.3.1 Gemeenten 306
8.3.2 Het ministerie 309
8.3.3 Leveranciers 310
8.3.4 Instanties en hun professionals: wie mogen (maar moeten niet) melden? 310
8.3.5 Toezichthouder en helpdesk 314
8.4 Systemen en tendensen bij digitalisering in de jeugdzorg 315
8.4.1 Overige initiatieven 315
8.4.2 Verschuivingen in de jeugdzorg 319
8.5 Motieven 329
8.5.1 Transparantie 329
8.5.2 Efficiëntie en effectiviteit 331
8.5.3 Keuzevrijheid 332
8.5.4 Accountability 334
8.5.5 Privacy 335
8.6 Slot 337

9 De digitale patiënt centraal. Medische informatie in een digitale wereld 349
Anne-Greet Keizer
9.1 Inleiding 349
9.2 Medische informatie 351
9.2.1 Medische informatie over de patiënt 352

	9.2.2	Medische informatie voor de patiënt en de zorgconsument	353
	9.2.3	Informatie voor wetenschappelijk medisch onderzoek	355
	9.2.4	Informatie voor zorg- en managementprocessen	357
9.3	Het medisch dossier in ontwikkeling		358
	9.3.1	Naar een elektronisch medisch dossier	359
	9.3.2	Wat doet het elektronisch dossier met zijn context?	360
9.4	Het landelijk EPD		361
	9.4.1	Ontwikkeling en invoering	362
	9.4.2	Externe krachten	364
	9.4.3	Het EPD en de rol van de patiënt	365
	9.4.4	Verschuiving in de doelstelling van het EPD	367
9.5	eHealth		369
	9.5.1	Wat wordt er onder verstaan?	369
	9.5.2	De opkomst van eHealth in beleid	371
	9.5.3	Medische informatie op internet	372
	9.5.4	Kansen en risico's van eHealth voor verschillende actoren	374
9.6	Beginselen		376
	9.6.1	Efficiëntie en effectiviteit	376
	9.6.2	Privacy	377
	9.6.3	Transparantie	377
	9.6.4	Keuzevrijheid	379
	9.6.5	Accountability	380
9.7	Conclusies		381
	9.7.1	Vormgeving en uitvoering	381
	9.7.2	Van passieve patiënt tot regisseur	382
10	**Chief Information Officers bij de rijksoverheid**		395
	Tamara Snijders		
10.1	Inleiding		395
10.2	Een theoretische kijk op de rol van de CIO		396
	10.2.1	Onderzoek Algemene Rekenkamer	396
	10.2.2	Maatregelen van het kabinet	399
	10.2.3	Informatiemanagement en de rol van de CIO	401
	10.2.4	Een tussenstand	407
10.3	Van ontwerp naar uitvoering: CIO's bij het rijk		408
	10.3.1	Ieder departement een CIO	409
	10.3.2	Verschillende posities	409
	10.3.3	Een netwerk van CIO's	410
	10.3.4	Afstand tot beleidsdirecties	412
	10.3.5	Adviserende rol	413
	10.3.6	Risicomanagement	414
	10.3.7	Reikwijdte	415
	10.3.8	CIO office	416

10.3.9 Architectuur en portfoliomanagement 416
10.3.10 Opdrachtgeverschap 417
10.3.11 Interdepartementale samenwerking 418
10.4 Tot slot 419

Over de auteurs 429

TEN GELEIDE

De publieke sector heeft de afgelopen jaren enthousiast de vruchten van het fenomeen digitalisering geplukt. Nu digitale toepassingen ook bij de overheid een vaste plaats in beleid en bij beleidsuitvoering hebben veroverd en hun alomtegenwoordigheid verder groeit, tekenen zich de fundamentele veranderingen en consequenties voor de burger, samenleving en overheidsinstituties af. Zo blijken de rollen en posities van overheden en burgers te veranderen en te verschuiven en wordt bovendien duidelijk dat deze veranderingen van betekenis zijn – of: zouden moeten zijn – voor zowel de bestuurlijke inrichting als ook de verantwoordelijkheidsverdeling tussen overheid en burgers.

De essays in deze verkenning handelen over bredere ontwikkelingen en thema's die met deze veranderingen en verschuivingen samenhangen en vormen daarmee onderdeel van een project dat de WRR medio 2008 is gestart en dat onder leiding stond van het Raadslid prof.mr. Corien Prins. Centraal in dit project stond de vraag naar de betekenis van digitalisering voor de relatie tussen overheid en burgers. De kennis in deze bundel legt mede de basis voor het rapport dat de WRR hierover begin 2011 heeft uitgebracht. Een ander deel van het ondersteunende materiaal is vanaf het najaar van 2010 verschenen als webpublicatie en kan via www.wrr.nl worden gedownload. Op basis van zowel de bijdragen in deze verkenning, de webpublicaties als uitgebreid empirisch en door de wetenschappelijke literatuur ondersteund onderzoek constateert de WRR dat de overheid als gevolg van de inzet van ICT de facto is veranderd in een informatie-Overheid (iOverheid). De hiermee gepaard gaande kansen, maar ook kwetsbaarheden nopen naar de mening van de raad tot een heroriëntatie. Voor de verdere digitalisering is het, zoals de raad in het rapport *iOverheid* betoogt, van groot belang dat de overheid beseft 'een iOverheid te zijn' en haar bestuurlijke kaders en organisatie daarop aanpast.

Onze grote dank gaat uit naar alle auteurs die hebben meegewerkt aan deze verkenning. Hun bijdrage strekte veel verder dan het leveren van hoofdstukken en daarmee inbreng voor het WRR-rapport *iOverheid*. Ook hun enthousiaste deelname aan de begin 2010 georganiseerde auteursbijeenkomst en de kennis en suggesties die ze daarbij inbrachten, zijn van grote waarde geweest om zowel deze verkenning als het rapport tot stand te doen komen.

1 INLEIDING

Dennis Broeders, Colette (M.K.C.) Cuijpers en Corien (J.E.J.) Prins

Op verschillende terreinen waar de overheid een verantwoordelijkheid voor beleid en uitvoering draagt – denk bijvoorbeeld aan zorg, veiligheid en sociale zekerheid – worden steeds vaker ICT-applicaties ingezet. De laatste jaren is binnen het brede domein van de overheid dan ook een indrukwekkend arsenaal aan ICT-initiatieven ontplooid. Als voorbeelden kunnen het Elektronisch Patiëntendossier (EPD), het biometrische paspoort en de Verwijsindex Risicojongeren (VIR) genoemd worden. De ontplooiing van ICT-initiatieven binnen de overheid richt zich daarbij zowel op een verbetering van de dienstverlening aan de burger als op het optimaliseren van de (samen)werking tussen ambtenaren en diensten in de backoffice van de overheid. Uiteindelijk heeft deze inzet van informatietechnologie ook gevolgen voor de relatie en verhouding tussen de overheid en haar burgers, waarbij deze gevolgen zowel beoogd als onbedoeld kunnen zijn. In het WRR-project *Beleid, Informatie en Technologie* (BIT) staan deze gevolgen centraal. In het verlengde van de observaties hierover komt de vraag aan de orde of bestaande institutionele arrangementen voldoende zijn toegesneden op deze veranderingen en zo niet, welke inhoudelijke, procedurele en institutionele aanpassingen noodzakelijk zijn om de uitdagingen van een steeds verder digitaliserende overheid te adresseren. Met andere woorden, het project beoogt een werkbaar perspectief te ontwikkelen op de rol en verantwoordelijkheid van de digitale overheid, in het bijzonder waar deze, direct dan wel indirect, raakt aan de verhouding overheid-burger.

1.1 iOVERHEID

De resultaten van het BIT-onderzoek vinden hun weerslag in het WRR-rapport *iOverheid*. Bij de zoektocht naar de fundamentele veranderingen voor en binnen een digitaliserende overheid, zoomt het rapport specifiek in op informatieprocessen die onder invloed van moderne technologie sterk van aard, reikwijdte en impact wijzigen, zijn gewijzigd of mogelijk zullen wijzigen. Behalve de focus op de relatie burger-overheid, zijn een aantal andere keuzes van belang geweest voor het onderzoek. Binnen het begrippenpaar informatie en technologie vormt *informatie* het vertrekpunt van de analyse. Dat betekent dat de technologie niet a priori en op zichzelf van belang is voor de analyse, maar wel in relatie tot de veranderingen die een technologische innovatie met zich meebrengt in termen van informatie en informatiestromen. Biometrie is hoofdzakelijk een belangrijke technologie, omdat het als sleutel fungeert voor het koppelen van persoonsinformatie, niet vanwege de technische ins en outs. Als leidraad voor de verschillende deelstudies is gekozen voor de dynamiek tussen zowel een aantal beginselen (zoals veiligheid,

privacy en transparantie, zie verder par. 1.3) die in de discussie over techniek en informatie een prominente rol spelen, als voor de dynamiek tussen de actoren (rijksoverheid, uitvoerende instanties, gemeenten, internationale organisaties, bedrijfsleven en burgers) die de discussie over en de ontwikkeling van de digitaliseringsinitiatieven sturen. Uiteindelijk leidt de analyse in het rapport *iOverheid* tot een serie aanbevelingen over de rol en verantwoordelijkheid van de overheid in digitaliseringsprocessen.

Met deze afbakeningen komen ook de hoofdvragen van het rapport in beeld. Hoe ontwikkelt de digitale overheid zich in de praktijk van alledag? Wie spelen hier een leidende rol en hoe staat het daarbij met de interactie tussen beleid en uitvoering? Welke kwesties treden naar voren als het om goed opdrachtgeverschap van de overheid gaat? Welke informatiestromen resulteren uit de inzet van moderne ICT door de overheid en wat zijn de bedoelde en onbedoelde gevolgen daarvan, niet alleen voor burgers, maar ook voor de overheid zelf? Valt de discussie over de uiteenlopende beginselen die in het geding zijn bij een digitaliseringsinitiatief – variërend van veiligheid, privacy, efficiëntie en transparantie – op een vruchtbare wijze te voeren? En, ten slotte, welke inhoudelijke, procedurele en institutionele aanpak is aan de orde wil de overheid op een zorgvuldige en innovatieve wijze het toekomstig pad van digitalisering vervolgen?

Het rapport *iOverheid* laat zien dat de term eOverheid – met zijn focus op de techniek, individuele applicaties en dienstverlening – niet langer strookt met de dagelijkse realiteit van een digitaliserende overheid. De digitale overheid heeft zich de facto en bijna ongemerkt ontwikkeld tot een iOverheid. Dit is echter geen bewuste 'strategie' van de overheid geweest. Het rapport laat zien dat in de dagelijkse praktijk van politiek en bestuur allesbehalve vanuit het samenhangende idee van de iOverheid wordt gedacht en gewerkt: het overgrote deel van de overheidsinitiatieven voor digitalisering en de informatiestromen die daaruit volgen, worden geïsoleerd bepleit, beoordeeld en ingevoerd. De centrale aanbeveling van het rapport *iOverheid* is dan ook dat het 'besef een iOverheid' te zijn, in het doen en denken van de overheid verankerd dient te worden. Het paradigma van de eOverheid moet worden ingewisseld voor dat van de iOverheid. Om dat te bereiken is die centrale aanbeveling verder uitgewerkt in een aantal strategische en institutionele aanbevelingen die de overheid in staat moeten stellen om de eigen beleidskaders en instituties in de pas te brengen met de praktijk van de iOverheid. Hoewel de genetwerkte iOverheid niet centraal en hiërarchisch aangestuurd kan worden, ligt in het besef wel de mogelijkheid de verdere ontwikkeling ervan in goede banen te leiden.

1.2 DE STAAT VAN INFORMATIE

Het onderzoek dat ten grondslag ligt aan het rapport *iOverheid* is langs drie lijnen opgezet. Naast de eerste lijn, die gevormd wordt door bestaande Nederlandse en

internationale wetenschappelijke literatuur, heeft de WRR ook twee lijnen van eigen onderzoek uitgezet. De eerste daarvan betreft vele gesprekken met wetenschappers, deskundigen, beleidsmakers en uitvoerders, die in het kader van dit project gevoerd zijn en welke een schat aan informatie hebben opgeleverd. De tweede lijn is het onderzoek dat de WRR ten behoeve van dit rapport zelf heeft uitgevoerd en door externe auteurs heeft laten uitvoeren. De resultaten hiervan zijn neergelegd in essays en empirische studies. De empirische studies zijn weer onderverdeeld in domeinstudies en blackbox-studies. De domeinstudies schetsen ontwikkelingen van digitalisering en informatisering op een breder (beleids-) terrein, zoals gezondheidszorg of het immigratiebeleid, terwijl de blackbox-studies zich richten op een veel specifieker gebied of een concrete toepassing, zoals het EPD, het biometrisch paspoort of het Europese eCall-initiatief. Hiernaast belichten enkele essays de bredere en conceptuelere thema's die het onderzoeksdomein betreffen. Overheidsverantwoordelijkheid en kwesties en afwegingen rondom risico's van informatietechnologie spelen hierin een centrale rol, zij het vanuit verschillende perspectieven zoals het strafrecht en de fundamentele mensenrechten. Dit onderzoek heeft geleid tot een veelheid aan bronnen die samen de bouwstenen voor het rapport *iOverheid* vormen. Allereerst zijn dat de domeinverkenningen, achtergrondstudies en de essays die als hoofdstuk in deze verkenning zijn opgenomen. Hiernaast is het empirisch materiaal gestoeld op en getoetst in een groot aantal interviews en discussiebijeenkomsten. Deze laatste hebben plaatsgevonden met de Raad van State, de Eerste Kamer en diverse burgerrechtenbewegingen. Tevens is met internationale wetenschappers van gedachten gewisseld tijdens een door de WRR en het Oxford Internet Institute (Oxford, VK) in mei 2010 georganiseerd expertseminar. Een belangrijke bouwsteen van het rapport wordt verder gevormd door de blackbox-studies. Deze zijn uitgegeven als webpublicatie en te raadplegen op www.wrr.nl. Het betreft de volgende studies: Bettine Pluut (2010) *Het landelijk EPD als black box: besluitvorming en opinies in kaart*; Vincent Böhre (2010) *Happy Landings? Het biometrische paspoort als zwarte doos*; Jelle Attema en David de Nood (2010) *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit*; Paul Potters en Marije de Vreeze (2010) *eCall Blackbox*; Marie-José Bonthuis en Jan Holvast (2010) *Blackbox-onderzoek veiligheidshuizen*; Mark van Loon (2010) *Goed opdrachtgeverschap jegens ICTU*; Max Snijder (2010) *Het biometrische paspoort in Nederland: crash of zachte landing?*; en Henk Griffioen (2011) *'Location based privacy' in constellaties van publiek-private verantwoordelijkheid.* De studie van Attema en De Nood is het resultaat van een survey-onderzoek waarin de rol en verantwoordelijkheid van de overheid bij de inzet van ICT centraal staan en dat is uitgevoerd door ECP-EPN in samenwerking met Centerdata en de WRR.

1.3 BEGINSELEN

Wie de beleidsvoorstellen voor digitalisering en het debat daarover van de afgelopen jaren overziet, stelt vast dat in de argumentatie en retoriek van betrokken actoren een aantal beginselen dominant is. Zo figureren veiligheid en privacy prominent in de discussies. Maar tot terugkerende beginselen behoren ook transparantie, *accountability*, keuzevrijheid, efficiëntie en effectiviteit. De invulling van deze beginselen is niet alleen van situatie tot situatie verschillend, maar verandert door de tijd heen ook onder invloed van de technologische en maatschappelijke ontwikkelingen. Voor een beter begrip en om een uiteindelijke weging tussen deze beginselen mogelijk te maken is door de WRR-projectgroep Beleid, Informatie en Technologie voor elk van de beginselen een conceptuele verkenning ondernomen. Deze zijn weergegeven in korte interne notities die ter voeding en inspiratie zijn meegegeven aan de externe en interne auteurs voor hun werk aan de verschillende essays, domeinverkenningen en blackboxes. Om de lezer van deze verkenning een handvat te bieden met betrekking tot de beginselen en de daaraan toegekende betekenis, volgt hieronder een korte duiding van elk beginsel.

Identiteit en identificatie

Identificatie is voor de overheid het vertrekpunt voor een steeds uitgebreidere verzameling van informatie over burgers. Daarbij gaat het niet langer alleen om het vaststellen 'wie iemand is', maar om zowel in de breedte (met zoveel mogelijk gegevens) als in de diepte (met zo specifiek mogelijke gegevens) een beeld te vormen van burgers ('burgerbeelden'). Deze burgerbeelden worden onder andere gevormd door het koppelen van bestanden rondom een persoon. Deelidentiteiten (belastingbetaler, autobezitter, uitkeringsgerechtigde) die voorheen van elkaar gescheiden waren, worden samengebracht (samengestelde identiteit). De idee hierbij is dat hoe meer men weet over de burger (holistisch burgerbeeld), hoe efficiënter en effectiever doelstellingen als dienstverlening en handhaving kunnen worden gerealiseerd. Deze burgerbeelden hebben de schijn volledig te zijn. Het dynamische karakter van de persoonlijke identiteit van individuele burgers toont echter dat dergelijke abstracte burgerbeelden niet stroken met de realiteit waarin een identiteit tot uitdrukking komt. Burgerbeelden (profielen) blijven kortom te allen tijde een abstractie van een persoonlijke identiteit. Dit roept op zijn beurt vragen op in de sfeer van andere beginselen zoals privacy en verantwoordelijkheid.

Identificatie gebeurt vaak via zogenaamde *identifiers*. Dit kan iemands naam zijn, maar ook een identiteitskaart of een burgerservicenummer (BSN). Met de toenemende populariteit van online interactie is ook de vraag naar digitale identifiers gegroeid. Het kan ook zijn dat klassieke identificatiemiddelen een technologische *make-over* krijgen; denk bijvoorbeeld aan de toevoeging van biometrie aan het paspoort. Het betreft hier veelal geen 'neutrale' digitaliseringsslag, omdat naast de 'oude' identificatiefunctie ook nieuwe functies mogelijk worden gemaakt. Ook

kan eenzelfde identificatiemiddel binnen verschillende – digitale – contexten gebruikt worden; denk bijvoorbeeld aan het BSN, ontworpen voor het domein van de overheid, maar steeds vaker ook gebruikt ter identificatie in de private sector. Om de explosieve groei van allerlei deelidentiteiten en online *identifiers* te beheersen, groeit de belangstelling, ook binnen de overheid, voor identiteitsmanagement. Het gebruik van een unieke identifier heeft voor de burger als voordeel dat hij of zij geen tientallen verschillende paswoorden en codes meer hoeft te onthouden. Het gebruik van unieke identifiers brengt echter ook risico's met zich mee. Zo maakt het burgers kwetsbaar voor het opkomende fenomeen van identiteitsdiefstal. Immers, één gekraakte identifier geeft toegang tot vele deelidentiteiten. Soms heeft het gebruik van verschillende identifiers ook de voorkeur, bijvoorbeeld wanneer het niet wenselijk is dat bepaalde gegevens in verschillende domeinen bekend worden.

Keuzevrijheid

Het vergroten van keuzevrijheid wordt vrijwel altijd gelijkgesteld aan het verschaffen van zoveel mogelijk informatie, ervan uitgaande dat meer informatie ook altijd leidt tot meer keuzes en ook betere keuzes (Tiemeijer & Thomas 2009: 11). ICT wordt niet alleen ingezet om informatie te ontsluiten, maar ook om informatie te filteren en doorzoeken. Online zijn er tal van websites, fora en vergelijkingssites die het individu helpen zich een weg te banen door vele informatiestromen en, door middel van slimme algoritmes (mensen die boek x kochten, schaften ook boek y aan), bij te staan in het maken van keuzes. Critici stellen daarentegen dat de technologische keuzehulpmiddelen juist afbreuk doen aan de optimalisering van keuzevrijheid. Zij vrezen dat de diversiteit en variëteit die de (digitale) wereld heeft te bieden, door deze technologische filteringen juist verloren gaat. In de relatie burger-overheid gaat keuzevrijheid ook over de wijze waarop de overheid bereikbaar is en of hier voor de burger een keuze bestaat tussen het digitale en het niet-digitale kanaal. Hierbij speelt ook het fenomeen van het verlies van functionaliteiten een rol, waarbij een functionaliteit die onder de oude dienst beschikbaar was, onder de nieuwe dienst niet meer benut kan worden. Illustratief is hier de OV-chipkaart, waar 'het retourtje' niet meer bestaat en DigiD waarmee het in eerste instantie niet mogelijk was om als vertegenwoordiger namens de houder van de handtekening een handeling te verrichten. Een derde tendens die van invloed kan zijn op keuzevrijheid betreft slimme of niet-zichtbare applicaties, zoals bepaalde webapplicaties, die (verhuld) mogelijk (ongewenste) keuzes gaan maken voor gebruikers door hun zoekgedrag te sturen.

Transparantie

Transparantie wordt heden ten dage sterk gekoppeld aan 'het recht op informatie' (Singh 2007; Horsley 2007). Iets wordt pas transparant wanneer er gegevens beschikbaar zijn. In de literatuur worden dikwijls drie technologische ontwikkelingen onderscheiden die transparantie vergroten. Ten eerste zijn door de inzet

van technologie de mogelijkheden voor het verzamelen van steeds meer verschillende soorten van informatie toegenomen. Ten tweede is de opslagcapaciteit enorm vergroot waardoor heel veel gegevens op eenvoudige wijze een zeer lange tijd (en soms in de praktijk zelfs onbeperkt) te bewaren zijn. Ten derde worden er steeds meer geavanceerde technieken ontwikkeld, zoals datamining en *profiling*, waarmee grote massa's data uit verschillende contexten aan elkaar worden gekoppeld om hier vervolgens (voor beleid en beleidsuitvoering) relevante informatie en nieuwe kennis uit te destilleren.

In de relatie burger-overheid is er een duidelijke trend waarneembaar waarbij de burger, vaak zonder dat hij hiervan zelf op de hoogte is, steeds zichtbaarder en transparanter wordt voor verschillende overheidsinstanties die door middel van het koppelen van bestanden en uitvoerige dataverzameling tot een zo volledig mogelijk burgerbeeld proberen te komen. Een transparante burger is voor de overheid belangrijk, omdat zij zo proactiever kan optreden en de dienstverlening beter kan afstemmen op de behoefte van de burgers (Van der Hof et al. 2009). Tegelijk biedt een transparante burger de overheid ook de mogelijkheid deze burger beter te controleren en in zijn gedrag te sturen. Deze ontwikkeling maakt het echter voor de burger steeds minder duidelijk wie bij de overheid welke informatie over hem bezit en op basis van welke informatie iemand tot een besluit komt. Daarnaast kan gewezen worden op de opkomst van allerhande initiatieven om de overheid transparanter te maken. Een transparante overheid, mede mogelijk gemaakt door de inzet van ICT, faciliteert accountability (Meijer 2003).

Effectiviteit en efficiëntie

Bij effectiviteit en efficiëntie gaat het niet enkel om het versoepelen van de relatie burger-overheid bijvoorbeeld door het verlagen van administratieve lasten en het opzetten van een centraal aanspreekpunt voor burgers, maar ook om het verbeteren van de interne bedrijfsvoering. Het politieke en bestuurlijke geloof in ICT voor het verbeteren van de efficiëntie van de overheid is de afgelopen jaren groot gebleken. Niet alleen gaat men ervan uit dat technologie in hoge mate stuurbaar en dus ook dienstbaar is aan de vooropgestelde doelstellingen, men gaat er ook van uit dat zowel interne als externe werkprocessen gebaat zijn bij digitalisering. Het is alleen de vraag of ICT deze verwachtingen ook waarmaakt. Hier betreden we het terrein van effectiviteit, een term die vaak in samenhang met efficiëntie wordt gebruikt. Iets is immers pas efficiënt als het ook effectief ofwel doeltreffend is. Duidelijkheid over wat ICT in bijvoorbeeld de dienstverlening of handhaving precies oplevert, is er echter niet of nauwelijks. Zo zijn er wel ramingen wat de veranderingsprocessen via e-dienstverlening moeten opleveren, maar zijn er (nog) geen harde cijfers die dit bevestigen (Kearns 2004). Deels komt dit door een gebrek aan evaluatie waardoor cijfers simpelweg niet voorhanden zijn. Deels weet men soms ook niet wat precies gemeten dient te worden of in welke grootheden zaken uit te drukken. De opbrengst van efficiëntie wordt bovendien niet altijd gewogen ten opzichte

van andere belangrijke beginselen die in het gedrang komen in digitaliseringsprocessen. Efficiëntie kan bijgevolg niet ten volle beoordeeld worden zonder de effectiviteit te toetsen en de invloed op of verhouding tot andere beginselen te wegen.

Privacy

Privacy, ofwel het recht op persoonlijke levenssfeer, is een fundamenteel recht van de mens ter bescherming van persoonlijke vrijheid. Het wordt gezien als een recht dat onlosmakelijk met de persoonlijkheid van het individu is verbonden. Privacy vormt een overkoepelend begrip waaronder verschillende dimensies vallen, zoals het recht op lichamelijke integriteit, relationele privacy, ruimtelijke privacy, en het recht op gegevensbescherming (informationele privacy). Door de enorme toename in gegevensverwerking ten gevolge van de ontwikkeling van technologie, die steeds eenvoudiger en steeds dieper in de persoonlijke levenssfeer kan binnendringen, is de aandacht voor het recht op gegevensbescherming de laatste decennia enorm toegenomen. Met de inwerkingtreding van het Verdrag van Lissabon en de daarmee gepaard gaande erkenning van rechtskracht van het Handvest van de Grondrechten van de EU, heeft dit recht uitdrukkelijk de status van fundamenteel recht in Europa gekregen (Art. 8 Handvest). Op papier heeft het recht op informationele privacy dus een sterkere positie verworven, in de praktijk lijkt het echter steeds meer aan zeggingskracht te verliezen. Niet alleen lijkt het door de technologische ontwikkelingen steeds moeilijker om het individu te beschermen tegen de ongewenste blikken van anderen (overheid of medeburger), door de genetwerkte samenleving blijkt het achterhalen van verantwoordelijkheid voor inbreuken op de privacy ook steeds moeilijker. De blik van anderen en de overheid is in het digitale tijdperk steeds pervasiever en duurzamer en bovendien niet altijd zichtbaar voor betrokkenen. Hoe onze gegevens achter de (computer)schermen van zowel de private als de publieke sector verwerkt worden, is voor de burger vaak erg onduidelijk. Zonder wetenschap van verwerking is het echter voor burgers ondoenlijk en onmogelijk na te gaan of een verwerking volgens de regels gebeurt, laat staan om hiertegen te ageren. Zelfs indien een burger op de hoogte is van onrechtmatige verwerking van zijn gegevens, is het nog maar de vraag of hij kan achterhalen wie hiervoor verantwoordelijk is. Bij keteninformatisering, maar bijvoorbeeld ook bij *cloud computing*, waarbij diensten niet langer zelf via eigen servers worden aangeboden, maar worden afgenomen van derden die mogelijk gebruikmaken van servers en *storage* verspreid over de gehele wereld, is de vraag wie, wat en waar verkeerd heeft gedaan, niet meer eenvoudig te beantwoorden. Niet voor niets werkt Europa momenteel aan een herziening van Richtlijn 95/46/EG. Praktisch gezien blijkt het wettelijk regime, en de beginselen waarop dit gestoeld is zoals *data qualitiy* en *purpose limitation*, in de huidige samenleving waarin de techniek (mede) bepalend is voor de verwerking van persoonsgegevens, moeilijk toepasbaar. Naast privacy als fundamenteel recht is privacy tegelijkertijd essentieel betrokken op sociale percepties ten aanzien van wat privaat *behoort* te zijn, oftewel op sociale normativiteit. Voor de overheid behelst privacy daarom een veel bredere opdracht dan het opzetten van juridische arrangementen

alleen. Er lijken belangrijke taken te liggen op het gebied van educatie en informatievoorziening, maar ook omgekeerd in responsiviteit ten aanzien van maatschappelijke verwachtingen en tendensen.

Accountability

Accountability draait om het geven en afnemen van verantwoording, en de repercussies waartoe deze verantwoording leidt (Bovens et al. 2008). In de context van de ICT-applicaties van de overheid is accountability een centraal, maar vaak ook problematisch beginsel, zoals hierboven reeds aangegeven met het voorbeeld van keteninformatisering en cloud computing. Hoe deze verantwoordelijkheid belegd is, bepaalt welke aanknopingspunten de burger heeft om te kunnen ageren tegen de praktische uitkomsten van de vele applicaties en informatiestromen die op hem betrekking hebben. De meest vertrouwde betekenislaag van de term accountability ziet op politieke verantwoording – en zijn noodzakelijke complement politieke afrekening. Het gaat hier om herleidbaarheid tot de wensen van de principaal, in de democratische natiestaat opgevat als het parlement. Met name met internet hebben burgers een ongemeen sterk instrument van "vigilance, denunciation and evaluation" (Rosanvallon 2008: 70) in handen waardoor accountability ook buiten de gevestigde structuren treedt. Een tweede betekenislaag van accountability betreft herleidbaarheid tot de geldende juridische regels en uitgangspunten. In andere termen: de Code wordt allesbepalend, terwijl deze aan het zicht onttrokken is (vgl. Teubner 2003). Door de digitalisering van de overheid worden veel regels en uitgangspunten verplaatst naar de systemen en koppelingen die zich achter de schermen, in de backoffice van de overheid, bevinden. Sommige beslissingen worden zelfs verplaatst naar de software en algoritmen die de applicaties van de backoffice sturen. Deze verschuiving naar de backoffice (*and beyond*) betekent dat het moeilijker wordt voor burgers om aanknopingspunten te vinden en/of om de uitkomsten van een applicatie die hun onwelgevallig zijn te corrigeren of aan te vechten. De vraag is of het menselijke oordeel de concurrentie met de ongeëvenaarde voorspelbaarheid van de (goed functionerende) computer wel aankan. De computer is, zo zou men kunnen zeggen, accountable in optima forma.

1.4 OPBOUW

Deze verkenning bevat een belangrijk deel van het ondersteunende materiaal ten behoeve van het WRR-rapport *iOverheid*. De inhoudelijke thema's van dit materiaal hangen nauw samen met de belangrijkste doelstellingen van het rapport. Zoals hiervoor al is opgemerkt, beoogt het rapport de verantwoordelijkheid van de overheid voor de omgang met ICT te duiden. Geredeneerd vanuit de centrale relatie overheid-burger zijn daarbij twee typen van verantwoordelijkheid in het geding. In de eerste plaats verantwoordelijkheid vanuit de rol van de overheid als gebruiker van ICT, met name voor de uitvoering van beleid dat de burger (direct) raakt. In de tweede plaats vanuit de rol van de overheid als 'systeembeheerder' of

regulator voor kwesties met betrekking tot technologie, informatie en informatieprocessen in de samenleving, in het bijzonder die 'private' ontwikkelingen die de positie van de burger raken. Het WRR-rapport richt zich primair op de eerste rol, maar de empirische analyse laat zien dat het belang van systeemverantwoordelijkheid groeiende is. In de epiloog van *iOverheid* formuleert de WRR dan ook een opdracht voor de overheid ten aanzien van systeemverantwoordelijkheid. In nauwe relatie tot het concept verantwoordelijkheid, staat het concept risicobeheersing. De verdeling van verantwoordelijkheid hangt immers samen met het dragen van het risico als schade voortvloeit uit het gebruik van ICT. Vanuit dit perspectief is een nadere duiding van de begrippen verantwoordelijkheid en risico in relatie tot digitalisering van belang. De eerste drie essays van deze verkenning dragen bij aan de duiding van deze voor het rapport leidende concepten. Het vierde essay bevat vervolgens een wetenschappelijke analyse van een van de grote uitdagingen die digitalisering met zich meebrengt, maar waar relatief weinig aandacht voor is: de verhouding tussen enerzijds de creatie en het belang van een duurzaam digitaal geheugen en anderzijds de roep om, en onder omstandigheden ook het belang van, een recht op vergetelheid. Concepten als verantwoordelijkheid, risico en vergetelheid houden mede verband met problemen waarvoor burgers komen te staan wanneer hun gegevens ten onrechte of onjuist in de systemen van de overheid verwerkt worden. De verkenning bevat daarom als laatste hoofdstuk van het eerste deel van deze verkenning ook een analyse van het aantal en soort klachten van burgers die voortkomen uit, of samenhangen met, het gebruik van ICT. Deze vijf externe studies vormen samen het eerste deel van deze verkenning.

DEEL I

Hoofdstuk 2
Paul de Hert, Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting

In dit essay wordt nagedacht over de systeemverantwoordelijkheid van de overheid in de Informatiesamenleving. De Hert constateert dat op basis van de argumenten dat 'privacy minder belangrijk wordt' en dat 'regulering innovatie niet in gevaar mag brengen', ICT-bedrijven niet aangesproken worden op de mensenrechtelijke aspecten van hun producten en diensten. In een mensenrechtelijke perspectief is de overheid steeds de eindverantwoordelijke voor elke schending van mensenrechten. Deze systeemverantwoordelijkheid wordt gecompenseerd door het mechanisme van verantwoordelijkheidsdistributie: via wetgeving en beleid dwingt de overheid andere actoren in de samenleving om eigen verantwoordelijkheden op te nemen en grondrechtenbeleving door andere burgers te respecteren, behoudens proportionele beperkingen. Op basis van deze mensenrechtelijke argumentatie maakt De Hert duidelijk dat het antwoord op de vraag wie welke verantwoordelijkheden draagt voor veilige en betrouwbare informa-

tiestromen in onze samenleving steeds minder speculatief wordt. Uit de leer van de positieve plichten blijkt dat in Europa een actieve, beschermende taak mag verwacht worden van bedrijven en dat de overheid hierop moet toezien. Wie macht heeft moet verantwoording afleggen. De burger kan niet verantwoordelijk gehouden worden voor een systeem waarin de overheid zijn rol niet speelt en vergeet of weigert om relevante actoren voor hun verantwoordelijkheden te plaatsen. Zo werkt systeemverantwoordelijkheid niet.

Hoofdstuk 3
Albert Meijer, Overheidsverantwoordelijkheid in het informatietijdperk: een pleidooi voor het creëren van genormeerde experimenteerruimte
In dit essay wordt op een systematische manier zowel voor gebruiks- als voor systeemverantwoordelijkheid de vraag geanalyseerd wat nu de belangrijkste vraagstukken zijn waar de overheid zich voor ziet geplaatst als het gaat om de invulling van haar verantwoordelijkheden op het gebied van informatie en technologie. Als een van de kernproblemen wijst dit essay op het manoeuvreren door onbekend gebied. Hoewel een start is gemaakt met de vormgeving van de digitale overheid, is het werkveld nog (gedeeltelijk) onbekend en kan de betekenis ervan op de lange termijn nog niet worden doorgrond. De vraag die dit opwerpt is hoe de overheid op een intelligente wijze kan manoeuvreren door onbekend gebied? De analyse laat zien dat zowel het gebruiken van nieuwe technologieën als het niet-gebruiken ervan leidt tot risico's, onzekerheden en problemen rondom overheidsverantwoordelijkheden. Vanuit dit perspectief pleit Meijer voor het creëren van een genormeerde experimenteerruimte waarbij overheden in bepaalde gevallen en onder bepaalde (proces)condities de mogelijkheid krijgen om te experimenteren met nieuwe technologieën. Op deze wijze wordt een tijdelijke gedoogzone gecreëerd om nieuwe technologieën te ontwikkelen zonder dat de overheid zich direct overgeeft aan deze nieuwe technologieën. Tevens wordt de mogelijkheid geschapen te experimenteren met nieuwe verdelingen van verantwoordelijkheden tussen overheden, burgers, bedrijven en maatschappelijke organisaties, voordat deze verantwoordelijkheden worden geformaliseerd.

Hoofdstuk 4
Michel van Eeten, Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie
In dit essay vertrekt Van Eeten vanuit het inzicht dat niet de grootte van het risico, maar de vraag 'Wie draagt het risico?' uitgangspunt moet zijn bij elk debat over de veiligheid van informatietechnologie. Vanuit de wetenschap dat 'elk systeem zal falen' en 'elk systeem onveilig is' dienen in het debat vragen centraal te staan als: Wat zijn de consequenties van dat falen? Hoe waardevol is het terugdringen daarvan? Hoe zorgen we voor een balans tussen de kosten en baten van onveiligheid? In het essay wordt vervolgens geanalyseerd hoe veiligheidsexternaliteiten te internaliseren zijn. Hoewel de instrumenten die hiervoor kunnen worden ingezet in

het geval van informatietechnologie omstreden zijn en de discussie hierover pas enkele jaren serieus wordt gevoerd, kunnen al enkele contouren worden geschetst. De vier dominante opties: ex ante veiligheidsregulering; ex post aansprakelijkheid; verplichte melding van incidenten en ondersteuning van gedupeerden, en de aansprakelijkheid van intermediaire actoren worden in het essay besproken. Van Eeten geeft hierbij aan dat het niet gaat om een uitputtend overzicht en dat ook de vormgeving van elk van deze opties nog veel werk vereist voordat er sprake kan zijn van daadwerkelijke beleidsvoorstellen. Vanuit dit perspectief wordt geredeneerd dat het belangrijk is om spoedig helderheid te scheppen over de rol van de overheid. Op die manier kan voorkomen worden dat de onheilsprofeten op het gebied van de risico's van informatietechnologie de politiek tot interventies gaan uitlokken die meer kwaad dan goed doen.

Hoofdstuk 5
Ybo Buruma, Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld
Als gevolg van de digitalisering van het strafrecht lijkt ieder belast met zijn verleden en gevoelig voor het virtuele beeld dat van hem bestaat. Vanuit dit perspectief stelt dit essay de vraag centraal of er een recht op vergetelheid zou moeten bestaan en of de overheid hiervoor een zekere mate van verantwoordelijkheid draagt. Buruma komt, op basis van een analyse van zowel het digitale en biologische geheugen als de rol die de overheid heeft in onze maatschappij, tot de conclusie terughoudend te willen zijn met de introductie van een recht op vergetelheid. Ook de verantwoordelijkheid van de overheid is hierbij naar zijn mening beperkt. Het is logisch dat iemand zich wil beschermen tegen vervelende echo's uit het verleden, maar het is toch de vraag in hoeverre de overheid hierbij een taak heeft. Deze taak zou er hooguit in schuilen dat zij burgers zou moeten faciliteren bij het uitoefenen van controle op wat anderen over hen hebben opgeslagen. Hierbij is de regulering betreffende opslag en verwerking van gegevens van minder groot belang dan de regulering van het handelen dat is gebaseerd op digitale gegevens. De overheid dient aangesproken te worden op de accuraatheid van gegevens die reële gevolgen hebben en er moeten nadere eisen worden gesteld aan verificatie. Hoewel Buruma de introductie van een recht op vergetelheid te ver vindt gaan, is er naar zijn mening wel reden de overheid en andere gegevensverzamelaars de gevolgen van de digitale herinneringsarbeid te doen beseffen. De burger die zich gesteld ziet ten overstaan van een overheid die beter dan hijzelf weet wie hij is, heeft geen behoefte meer zich in te spannen voor een goed imago. Die burger vergeet zichzelf, aldus Buruma.

Hoofdstuk 6
Sunil Choenni, Erik Leertouwer en Tony Busker, Klachten over toepassingen van informatietechnologie. Analyse van een aantal overheidsbestanden
Dit essay geeft inzicht in de relatie overheid-burger door het in kaart brengen van ICT-gerelateerde klachten. Hiertoe zijn de bestanden van het College bescherming

persoonsgegevens (CBP) en het Centraal Meldpunt Identiteitsfraude (CMI) geanalyseerd. Uit de analyse van het CMI-bestand blijkt dat in 2009 40 procent van de klachten te relateren is aan ICT. Voor het CBP ligt het percentage ICT-gerelateerde klachten in dat jaar op 37 procent. Van de typische overheidssectoren die zijn onderscheiden in de analyse, scoort de sector openbaar bestuur het hoogst met 36 procent ICT-gerelateerde klachten. Om inzicht te krijgen in het potentieel aan ICT-gerelateerde klachten is vervolgens gekeken naar architectuurdefinities en literatuur over de werking van een aantal politie- en justitiebestanden, met name het HerKenningsdienst Systeem (HKS) en de Onderzoeks- en Beleidsdatabase Justitiële Documentatie (OBJD). Voor het HKS- bestand van de politie is onderzocht hoeveel burgers hier ten onrechte in voorkomen. Uit de analyse blijkt dat 8.000 verdachten de status 'overleden' hebben en 2.800 personen die zijn vrijgesproken toch ten onrechte in HKS voorkomen. Alhoewel het aantal onterecht geregistreerden relatief meevalt – op ruim 1,5 miljoen verdachten in totaal gaat het om minder dan 0,7 procent – kan de foutieve registratie voor ieder van deze individuele personen een hoogst problematische situatie opleveren.

DEEL II

Het tweede deel van de verkenning wordt gevormd door een drietal domeinstudies. Het gaat hier niet om studies die overkoepelende concepten duiden, maar om illustratieve analyses van het gebruik van ICT binnen een specifiek domein waarbinnen de overheid van oudsher belangrijke taken en verantwoordelijkheden kent. De kansen, risico's en de beleidsmatige processen in relatie tot de digitalisering in de sector persoonsmigratie, jeugdzorg en gezondheidszorg zijn bij wijze van illustratie van bredere ontwikkelingen in kaart gebracht. Ook voor deze studies geldt dat de hierboven beschreven beginselen als achterliggende leidraad hebben gediend. Het laatste hoofdstuk van dit tweede deel van de verkenning is niet gericht op een specifiek domein, maar betreft een analyse van de rol van CIO's bij de overheid. De keuze voor deze studie hangt enerzijds samen met de rol die CIO's spelen bij de verbetering van de positionering en kwaliteit van het informatiemanagement, waar risico- en verantwoordelijkheidsverdeling belangrijke componenten van zijn. Anderzijds beoogt de functie van CIO een bijdrage te leveren aan 'goed opdrachtgeverschap' binnen de overheid.

Hoofdstuk 7
Dennis Broeders, Grensoverschrijdende mobiliteit van personen en de digitale grenzen van Europa

In deze studie staat de digitalisering van de (externe) Europese grenzen centraal. Broeders onderscheidt twee generaties van EU-migratiedatabanken en applicaties als het biometrisch paspoort. De eerste generatie, met de databanken SIS, Eurodac en VIS, richt zich op migranten uit groepen of landen van herkomst die door de EU als problematisch worden aangemerkt. De tweede generatie, PNR-data-uitwisse-

ling, het biometrisch paspoort en het Entry/Exit-systeem, richt zich op alle reizigers, inclusief EU-burgers. De digitale en biometrische grenzen van de EU hebben straks alle reizigers in het vizier en in de databanken van de EU. Hiermee verandert ook het karakter van grensbewaking: de systemen en de informatie die daarin is opgeslagen zullen de beslissingen aan de grens en op consulaten steeds meer gaan sturen. Drijvende krachten achter deze ontwikkeling zijn het grote vertrouwen in de technologie van de Europese ministers en de Europese Commissie en de veiligheids- en biometrische industrie die – op de golven van de roep om veiligheid na 9/11 – een indrukwekkend programma van digitalisering in het beleidsterrein van Justitie en Binnenlandse Zaken (JBZ) hebben uitgewerkt en uitgevoerd. De ontwikkeling van dat programma werd tot voor kort nauwelijks beïnvloed door overwegingen van privacy, transparantie en gegevensbescherming. De verwachting is dat met de inwerkingtreding van het Verdrag van Lissabon, en de toegenomen rol van het Europees Parlement en het Europees Hof van Justitie, er meer evenwicht in het programma van de digitalisering van de Europese grenzen gaat komen.

Hoofdstuk 8
Esther Keymolen en Corien Prins, Jeugdzorg via systemen. De Verwijsindex Risicojongeren als spin in een digitaal vangnet

Deze studie is een analyse van de belangrijkste kenmerken, factoren en omstandigheden die samenhangen met de plannen voor, het opzetten en implementeren van en de omgang met de Verwijsindex Risicojongeren. Wat opvalt zijn de sterk uiteenlopende ambities en uitwerkingen op enerzijds rijksniveau en anderzijds decentraal niveau. Hierdoor zijn als het ware twee werkelijkheden ontstaan: de wereld van de tekentafel op rijksniveau. Daar is het systeem voor de verwijsindex relatief kaal ingericht (uitsluitend uitwisselen van signalen, geen inhoudelijke gegevens) en zijn de wettelijke randvoorwaarden helder gesteld. Tegelijkertijd wordt op het lokale niveau dit relatief kale systeem van de tekentafel vanuit de behoeften in de lokale praktijk uitgebouwd tot een rijk en schimmig systeem dat veel meer faciliteert dan het informatieloos uitwisselen van signalen. Keymolen en Prins concluderen dat daar waar op rijksniveau de aandacht primair uitgaat naar ('neutrale') technologie, het lokale niveau juist prioriteit geeft aan allesbehalve neutrale informatie, de daarmee verbonden gegevensprocessen en daarmee te realiseren functionaliteiten. Het rijkgeschakeerde palet aan instanties dat gebruik mag maken van de verwijsindex toont dat de grenzen tussen zorg, dienstverlening en opsporing sterk onder druk komen staan. Keymolen en Prins typeren het debat over de digitalisering van de jeugdzorg, met de introductie van de Verwijsindex Risicojongeren als sprekend voorbeeld, als armoedig. De discussie beperkt zich tot de tekentafelontwerpen op rijksniveau, terwijl de echt prangende vragen, dilemma's maar zeker ook het uitdijende landschap van gegevensstromen en gegevensgebruik dat op lokaal niveau vorm en inhoud krijgt, verscholen blijft en toezicht ontbeert. Problematisch blijkt de uitoefening van rechten door jongeren en hun ouders, evenals de verantwoordelijkheid voor het gegevensgebruik. De vraag is

dan ook of de voordelen van de ruimte die op centraal niveau gegeven wordt aan het decentraal niveau, opwegen tegen het ontstane gebrek aan inzet, overzicht en toezicht op de processen en ontwikkelingen op de lokale werkvloer.

Hoofdstuk 9
Anne-Greet Keizer, De digitale patiënt centraal. Medische informatie in een digitale wereld
In deze studie wordt een beeld geschetst van actuele ontwikkelingen rond informatie en technologie in het domein gezondheidszorg. Centraal daarbij staat de vraag wat digitalisering van medische informatie, en de nieuwe mogelijkheden die het met zich meebrengt, betekent voor de bestaande relaties in dit domein. Een sterke focus ligt hierbij op het Elektronisch Patiëntendossier (EPD), hetgeen een ander karakter, een andere wijze van gebruik en andere functionaliteiten heeft dan zijn papieren voorloper en van invloed is op de organisatie van de medische sector en de relatie tussen arts en patiënt. De ontwikkeling en invoering van een EPD past in de bredere trend van *electronic Health* (eHealth). Medische informatie omvat in dit kader veel meer dan de gegevens over een patiënt in zijn dossier; het gaat ook om medische informatie gericht op preventie, geaggregeerde en geanonimiseerde data voor onderzoek en informatie over zorgprocessen ten behoeve van bedrijfsvoering van ziekenhuizen. Hoewel het EPD gezien kan worden als onderdeel van eHealth, schuilt er een duidelijke spanning tussen enerzijds de gedachte achter het EPD van volledige beschikbaarheid van informatie, en anderzijds de eigen regie van de patiënt hetgeen de achterliggende gedachte achter eHealth vormt. Van belang in dit verband is dat de rol van regisseur niet alleen rechten, maar ook verantwoordelijkheden met zich meebrengt. Een nieuwe verantwoordelijkheidsverdeling zou tot uiting kunnen komen in een nieuwe invulling van het begrip *informed consent*. Het is echter maar de vraag of alle burgers of (potentiële) patiënten in gelijke mate in staat en gemotiveerd zullen zijn deze nieuwe verantwoordelijkheden op zich te nemen.

Hoofdstuk 10
Tamara Snijders, Chief Information Officers bij de rijksoverheid
Deze studie brengt het werkveld van de CIO's bij de rijksoverheid in kaart, zowel aan de hand van de heersende opvattingen in de literatuur als aan de hand van de inzichten en ervaringen van verschillende CIO's bij Nederlandse ministeries die voor deze studie zijn geïnterviewd. Snijders komt tot de conclusie dat de invulling van een CIO-rol bij alle departementen van de rijksoverheid een goede stap is in de richting van professionele besturing van ICT-projecten en professioneler informatiemanagement binnen het departement. Het valt echter te betwijfelen of de CIO met zijn huidige bevoegdheden ook echt in staat zal zijn om het ICT-enthousiasme van politiek en bestuurders te temperen en in staat is hen bewust te maken van de realiteit van de uitvoering van ICT-projecten. Zolang (bureau)politieke redenen blijven prevaleren boven de urgente realiteit

van ICT-projecten en ook dringende adviezen van de CIO om die reden aan de kant kunnen worden geschoven, zal de CIO wellicht nooit in staat zijn het gewenste resultaat te bereiken. Ook het feit dat de rol van CIO slechts beperkt blijft tot één van de vele rollen van de betreffende ambtenaar doet afbreuk aan de kracht van de CIO in de organisatie. Teneinde de CIO beter in staat te stellen zijn taken waar te maken is het van belang de CIO uit te rusten met meer bevoegdheden, zoals een bindend advies. Daarnaast lijkt het, zeker in de ontwikkelingsfase, van belang dat een CIO voldoende tijd heeft om een langetermijnstrategie te bepalen, zodat al zijn inspanningen in lijn zijn met de meer strategische doelen en langetermijnvisie. Tot slot concludeert Snijders dat commitment van de bestuursraad van een departement een noodzakelijke voorwaarde is voor het succes als CIO.

LITERATUUR

Bovens, M., Th. Schillemans & P. 't Hart (2008) 'Does public accountability work? An assessment tool', *Public Administration*: 225-242.

Horsley, J. (2007) 'Towards a more open China?' in A. Florini (red.) *The right to know*, Chichester: Columbia University Press.

Kearns, I. (2004) *Public value and e-government*, Londen: Institute for Public Policy Research (IPPR).

Meijer, A.J. (2003) 'Transparent government: parliamentary and legal accountability in an information age', *Information Polity* 8: 67-78.

Rosanvallon, P. (2008) *Counter-democracy. Politics in an age of distrust*, Cambridge: Columbia University Press.

Singh, S. (2007) 'Grassroots initiatives' in A. Florini (red.) *The right to know*, Chichester: Columbia University Press.

Teubner, G. (2003) 'Globale Zivilverfassungen: Alternativen zur staatszentrierten Verfassungstheorie', *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* 1-28.

Tiemeijer, W. & C. Thomas (2009) 'Inleiding' in *De menselijke beslisser*, WRR-verkenning nr. 22, Amsterdam: Amsterdam University Press.

Van der Hof, S., R.E. Leenes & S. Fennell (2009) *Framing citizen's identities, The construction of personal identities in new modes of government in the Netherlands, research on personal identification and identity management in new modes of government*, commissioned by the Netherlands organisation for Scientific Research (NWO), Network of networks programme, TILT, Tilburg University.

DEEL I

2 SYSTEEMVERANTWOORDELIJKHEID VOOR DE INFORMATIEMAATSCHAPPIJ ALS POSITIEVE MENSENRECHTENVERPLICHTING

Paul de Hert

2.1 SAMENVATTING

Deze domeinverkenning geschreven voor de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) gaat, eerstens, in op de vraag wie welke verantwoordelijkheden draagt in de huidige informatiemaatschappij. De materie is omstreden. Gedrag van jongeren op sociale netwerksites wordt aangegrepen om te stellen dat privacy minder belangrijk wordt. Op deze grond, of op grond van het argument dat regulering innovatie niet in gevaar mag brengen, worden ICT-bedrijven niet aangesproken op de mensenrechtelijke aspecten van hun producten en diensten.

Dit rapport doorbreekt dit 'pingpongspel van verantwoordelijkheden' met een argumentatie opgebouwd vanuit het recht der mensenrechten. Dit rechtsdomein heeft zijn eigen dwingende logica en maakt dat de vraag wie welke verantwoordelijkheden draagt voor veilige en betrouwbare informatiestromen in onze samenleving steeds minder speculatief wordt.

2.2 WIE DRAAGT WELKE VERANTWOORDELIJKHEDEN IN DE INFORMATIESAMENLEVING?

Op een maatschappelijk debat Think Privacy georganiseerd in het Europees Parlement in Brussel op 28 januari 2010[1], werd naar aanleiding van de Europese Data Protection Dag de vraag gesteld aan het talrijke publiek wie de verantwoordelijkheid draagt voor zijn of haar privacy: de overheid, de ICT-bedrijven of de internetgebruiker die op sociale websites zijn meest persoonlijke gegevens weggooit. De vraag werd opgeworpen na een bespreking door Michel Walrave, professor aan de Universiteit van Antwerpen, van zijn onderzoek over *Teenagers's online self-disclosure* waaruit blijkt dat jongeren op de hoogte zijn van privacyaandachtspunten, maar ze in de praktijk niet toepassen. Aan het publiek werd gevraagd te stemmen over wie allereerst verantwoordelijk was, wie vervolgens, enzovoorts. De uitslag van de stemronde is hier niet van belang. Mij verbaasde het ter stemming leggen van een problematiek die vanuit mensenrechtelijke hoek heel eenvoudig lijkt (zie verder). Toch word ik regelmatig geconfronteerd met een dergelijke 'open vraag naar finale verantwoordelijkheid'. Ik geloof dat die vraag vooral opgeworpen wordt om bepaalde belangen te sparen en eigen verantwoordelijkheden te ontlopen.

Deze strategie van vragen oproepen om bepaalde antwoorden niet te geven – Socrates onwaardig – doet denken aan pogingen van de Verenigde Naties (VN) om internationale bedrijven ertoe te bewegen om mensenrechten te respecteren wanneer ze opereren in landen met zwakke juridische structuren.[1] Ook daar worden bepaalde antwoorden liever vermeden. We gaan even kijken naar dat debat, om vervolgens te kijken naar het verantwoordelijkheidsdebat in de informatiesamenleving.

2.2.1 VERANTWOORDELIJKHEID VOOR SCHENDINGEN MENSENRECHTEN MULTINATIONALS

De Verenigde Naties zijn, als promotor van mensenrechten, begaan met de kwestie van mensenrechten en ondernemingen. Gemakkelijk is dat niet. De afbakening van de verantwoordelijkheid van de staten, en die van ondernemingen, is conceptueel onduidelijk. In het internationale mensenrechtenrecht zijn (alleen) staten verantwoordelijk voor de naleving van de mensenrechten. Bedrijven worden (vooralsnog) niet beschouwd als dragers van rechtstreekse verplichtingen. Derhalve komt aan de nationale landen de taak om toe te zien op het gedrag van bedrijven in het eigen land. Dat gedrag is echter voor zwakke landen, geconfronteerd met sterke en rijke multinationals, om tal van redenen niet eenvoudig te controleren.
De Verenigde Naties zijn daarom gericht op het tot stand brengen van een internationaal initiatief ter ondersteuning van die zwakkere landen. Een van de eerste initiatieven binnen de Verenigde Naties om ondernemingen op één lijn te brengen met mensenrechten was de UN *Code of Conduct for Transnational Corporations* (Algemene Vergadering, 21 december 1990, http://www.un.org/documents/ga/res/45/a45r186.htm). Dit project, dat begon midden jaren zeventig, streefde een overkoepelende regulering van de bedrijfsactiviteit van transnationale ondernemingen na, met inbegrip van hun mensenrechtelijke impact. De idee achter zo een code werd echter nooit formeel aanvaard binnen de Verenigde Naties en het project werd begin jaren negentig stopgezet. In 1998 werkte een, in de schoot van de VN Subcommissie voor de Bescherming en Bevordering van Mensenrechten (de Subcommissie) opgerichte werkgroep van deskundigen, de *Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights* (de *Norms*) uit. Het document vormt een eerste poging om juridisch afdwingbare mensenrechtenplichten voor ondernemingen vast te leggen. De 'normen' vertrekken nog steeds van het traditionele standpunt dat staten de primaire verantwoordelijkheid dragen voor de bescherming en de bevordering van mensenrechten, maar voegen daaraan toe dat ondernemingen een secundaire verantwoordelijkheid hebben dienaangaande (UN Sub-Commission 2003). De Subcommissie nam op 13 augustus 2003 in haar Resolutie 2003/16 de *Norms* unaniem aan. Vervolgens werden ze in maart 2004 besproken door de VN Mensenrechtencommissie (nu vervangen door de Mensenrechtenraad), waar ze

koud werden onthaald (UN Commission on Human Rights 2004). Het grootste discussiepunt betrof het dwingende karakter van de mensenrechtenplichten die zouden worden opgelegd aan ondernemingen.[2] De meeste westerse staten én ontwikkelingslanden stonden, onder druk van de ondernemingen, afkerig om ook ondernemingen juridisch afdwingbare mensenrechtenplichten op te leggen. Een oplossing uit deze patsituatie bestond erin om nog maar eens een nieuw initiatief te starten en dat bestond erin om een *Special Representative* aan te stellen met als taak de kwestie wederom te onderzoeken (UN Commission on Human Rights 2005). Deze gemandateerde, de Amerikaan Ruggie, presenteerde in 2008 zijn rapport *Protect, Respect, Remedy* (Special representative to the Secretary-General 2008), met erin bouwstenen voor de overbrugging van de zogenaamde *governance gaps*. Ruggie onderscheidt drie verschillende, doch intrinsiek complementaire luiken in zijn aanpak. Ten eerste, de plicht van de staat om zijn individuen te beschermen tegen mensenrechtenschendingen (*Protect*). Ten tweede, de verantwoordelijkheid van ondernemingen om respect te hebben voor mensenrechten (*Respect*). En ten derde, de toegankelijkheid van remedies wanneer mensenrechtenschendingen zich voordoen (*Remedy*).

2.2.2 DE *STATE DUTY TO PROTECT*, DE *CORPORATE RESPONSIBILITY TO RESPECT* EN *ACCESS TO REMEDY*

Ruggies eerste luik ziet op de plicht van de staat zijn individuen te beschermen tegen mensenrechtenschendingen, inclusief die gepleegd door ondernemingen. Ruggie vertrekt van de klassieke opvatting over het internationaal mensenrechtenrecht waarin staten de hoeksteen van het systeem vormen. In het rapport wordt de nadruk gelegd op het belang voor staten om een ondernemingscultuur die oog heeft voor mensenrechten aan te moedigen, en te implementeren. Daarvoor is een coherenter overheidsbeleid benodigd; een grotere samenwerking met internationale instanties en initiatieven en speciale attentie voor conflictgebieden.

Ondernemingen kunnen virtueel alle mensenrechten aantasten, stelt het rapport. Het zwaartepunt van de discussie ligt eerder bij de inhoud en omvang van de 'verantwoordelijkheid' van ondernemingen inzake mensenrechten. Als vertrekpunt geldt dat op ondernemingen een basisverplichting rust om in overeenstemming met de nationale wetten te opereren, en meer algemeen geen mensenrechten te schenden (*do not harm*). Wanneer een onderneming werkzaam is in een land waarin geen of slechts minimale mensenrechtenwetgeving aanwezig is, voldoet een onderneming die met *due diligence* handelt, aan haar verantwoordelijkheid respect te hebben voor mensenrechten. Dit begrip houdt in dat diligente ondernemingen *idealiter* een mensenrechtenbeleid dienen aan te nemen en te integreren, aan mensenrechtelijk *impact assessment* moeten doen, en hun beleid en activiteiten aan externe audit en monitoring onderwerpen.

De derde steunpijler van het mensenrechtelijke programma van Ruggie gaat over de toegang tot herstelmaatregelen of remedies. Hoewel er een grote verscheidenheid aan remedies bestaat – juridisch en niet-juridisch – is de toegang tot juridische remedies vaak ontoereikend, en zijn niet-juridische remedies onderontwikkeld. Om geloofwaardig en efficiënt te zijn zouden de niet-juridische remedies aan een aantal principes moeten voldoen. Zo dienen deze remedies legitiem en toegankelijk voor eenieder te zijn; de procedure ervan moet voorspelbaar, billijk, transparant en overeenstemmend zijn met de internationaal aanvaarde mensenrechtenstandaarden. De ontoegankelijkheid van bestaande mechanismen kan te wijten zijn aan het gebrek aan bekendheid ervan. Zo weten slachtoffers van mensenrechtenschendingen vaak niet welke herstelmaatregelen bestaan, en waar ze deze kunnen vinden. Een andere oorzaak ligt bij de vaak beperkte bevoegdheden en draagwijdte van de herstelmechanismen. Om deze leemten te verhelpen gaan bijvoorbeeld stemmen op voor het oprichten van een globale ombudsman, die centraal alle klachten met betrekking tot ondernemingen en mensenrechten zou kunnen ontvangen en behandelen.

De reacties op het *Protect, Respect, Remedy*-rapport waren lovend. Niet enkel de Mensenrechtenraad gaf het een warm onthaal, ook staten, de ondernemingen zelf en de *civil society* baseren zich erop in hun beleid rond mensenrechten en ondernemingen.[3] Toch zijn niet alle reacties even lovend. Een groep NGO's verzocht de Mensenrechtenraad om in het nieuwe mandaat van de SRSG verder te gaan dan het Protect, Respect, Remedy-kader, en ook aandacht te hebben voor de aansprakelijkheid van ondernemingen inzake mensenrechtenschendingen. "In defining the scope of a follow-on mandate we therefore urge the HRC to broaden the focus beyond the elaboration of the 'protect, respect, and remedy' framework, and to include an explicit capacity to examine situations of corporate abuse. A more in-depth analysis of specific situations and cases is needed in order to give greater visibility and voice to those whose rights are negatively affected by business activity and to deepen understanding of the drivers of corporate human rights abuses. Both elements should underpin the elaboration of the framework and proposed policy responses. For example, the modalities of corporate impunity and its impact on the enjoyment and protection of human rights need greater scrutiny as an integral part of the effort to identify solutions. A cornerstone of human rights is combating impunity. *To date the mandate has placed relatively little emphasis on the means of holding companies – including those that operate trans-nationally – to account. But for victims of human rights violations, justice and accountability can be as important as remedial measures*" (mijn cursivering) (Joint NGO Statement 2008).

2.3 ZES LESSEN VOOR HET DEBAT OVER DE INFORMATIEMAATSCHAPPIJ

Het voorgaande geeft heel wat instrumenten om een debat over verantwoordelijkheid in de informatiesamenleving correct te voeren.

1. Het voorhanden zijn van 'internationale spelers' en 'zwakke landen' in het multinationale debat is gemakkelijk te herkennen in de discussie over de digitale wereld met Amerikaanse bedrijven uit het genre Facebook, Intel, Microsoft en Google. Deze opereren vanuit Sillicon Valley waar privacywetgeving naar Europese normen inferieur is en laten de ene na de andere ICT-toepassing op ons los met een ritme waartegen geen verweer mogelijk is.

2. Ook herkenbaar in de discussie over multinationals en mensenrechten is het argument over het vermeende marktverstorende gevolg van overheidsingrijpen. De voorgaande paragrafen tonen aan dat het verzet tegen dwingende aan ondernemingen op te leggen normen afkomstig is van zowel westerse staten als van de ontwikkelingslanden. Het geloof dat meer bescherming voor de burger een innovatief klimaat doodt, lijkt bijgevolg breed verspreid onder beleidsmensen. In de context van de informatiesamenleving doet ons dit denken aan de debatten rond Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (*de e-commerce-richtlijn*), vertaald in Nederland in artikel 6: 196c van het Burgerlijk Wetboek. De uiteindelijk tot stand gekomen regelgeving bevat voor *access providers* (geven informatie door) en *hosting providers* (slaan informatie ook op) een soepel aansprakelijkheidsregime, dat afwijkt van de gewone civielrechtelijke en strafrechtelijke aansprakelijkheid. De gunstige regeling kwam er precies om dit soort dienstverlening vooral niet te zwaar te belasten met te veel verantwoordelijkheden.[4]

3. In de discussie over multinationals en mensenrechten gaat het niet over de vraag *of* bedrijven zich moeten engageren tot het respect voor de mensenrechten. Daar is iedereen het over eens. Het echte debat gaat over *de wijze waarop* dat engagement moet blijken en in het bijzonder over de vraag of er behoefte is aan bindende juridische normen.
In de discussie over de informatiesamenleving draait op eenzelfde wijze het debat *niet* om mensenrechten of waarden zoals 'veilig en betrouwbaar' internet. Daar is ongeveer iedereen het wel over eens. Wel gaat de discussie over de vraag hoe je deze waarden realiseert en of er al dan niet behoefte is aan 'juridische afdwingbare' rechten of waarden, waarbij vastgesteld wordt wie er primair en secundair verantwoordelijk is voor mogelijke problemen. Zolang dat laatste niet helder is, heb je *governance gaps*.

4. Binnen het paradigma van de verantwoordelijkheden zijn er meerdere keuzen mogelijk. In de discussie over multinationals en mensenrechten lijkt Ruggies Protect, Respect, Remedy-schema aanvaardbaar voor de meeste 'stakeholders'. Toch willen sommigen vooral wat de verantwoordelijkheid van de bedrijven betreft een stap verdergaan. Zij bepleiten een 'upgrade' van de verantwoordelijk-

heid van de bedrijven en een omzetting van hun *respect*-opdracht in een *protect*-opdracht. Anders gezegd, er wordt een stap bepleit van wat ik (loutere) *compliance* zou noemen naar accountability.[5] Daarmee zijn we bij een kernthema van het WRR-onderzoek gekomen waarbinnen deze verkenning zich situeert. Ik kom erop terug.

5. In het debat over multinationals en bedrijven is er geen sprake van het culpabiliseren van de mensen in ontwikkelingslanden die ervoor 'kiezen' om voor multinationale bedrijven te werken, wat ook de arbeidsvoorwaarden zijn. Blijkbaar is in deze discussie iedereen het er wel over eens dat de machtsverhoudingen zodanig zijn dat van de burgers in die landen geen keuzevrijheid kan worden verwacht. Door de slechte levensomstandigheden kunnen arbeiders en bedienden die 'kiezen' om in bedrijven te werken die het met de mensenrechten niet ernstig nemen, toch voor deze keuze niet verantwoordelijk worden gehouden.
Vraag is of het bij gebruikers van de informatiearchitectuur van onze informatiesamenleving anders gesteld is. *Digital divide*-studies tonen onder meer aan dat elke werknemer vijf jaar na het wegvallen van een werkbetrekking als ICT-ongeletterd mag worden beschouwd. De evolutie gaat zo snel dat het wegvallen van een omgeving waarin permanent bijgeschoold wordt funest is. In die omstandigheden een verantwoordelijkheid tot zelfbescherming plaatsen bij gebruikers ligt dan ook niet voor de hand. De voorbereidende notitie *Beginsel Accountability* wijst erop dat vele internetgebruikers geen besef hebben van de 'kleine letters' en helemaal niets van de onzichtbare protocollen van internet. [6] De auteurs van de tekst maken daarbij een reflectie over accountability bij overheidsbeslissingen die mijns inziens vrij eenvoudig te transponeren valt naar beslissingen op de eMarkt.[7]

6. Wat de derde bouwsteen van Ruggies Protect, Respect, Remedy-schema goed naar boven brengt is dat naar burgers niet moet gekeken worden in termen van 'eigen verantwoordelijkheid', doch eerder in termen van *empowerment.* Als een burger al verantwoordelijkheid moet dragen in een context waarin onveiligheid blijkbaar 'mag', geef hem en haar dan toegang tot toereikende juridische en niet-juridische remedies ('access to justice') en richt de *awareness*-campagnes dan niet (uitsluitend) op de eigen verantwoordelijkheid, doch eerder op het bestaan van die remedies en herstelmaatregelen, waarbij op het niveau van ondersteuning gedacht moet worden aan faciliterende instanties in het genre van de ombudsman. In de voorbereidende notitie *Beginsel Accountability* spreekt men van 'accountability-arrangementen'.[8] Die zijn er niet in de ontwikkelingslanden en volgens de genoemde notitie zijn ze er evenmin in onze digitale samenleving waar de overheid frontoffices creëert die op vrij onzichtbare wijze voor meerdere backoffices opereren, terwijl deze frontoffices vaak juridisch onaanspreekbaar zijn, omdat de accountability structuren zich nog steeds richten op de backoffices.[9]

2.3.1 HET EUROPESE MENSENRECHTENPERSPECTIEF OP VERANTWOORDELIJKHEID IN DE INFORMATIESAMENLEVING

Een strikt Europees perspectief op mensenrechtelijke discussies zoals deze hierboven geschetst geeft nog meer stof tot nadenken. Dit Europees perspectief wordt grotendeels beheerst door het Verdrag voor de Bescherming van de Rechten van de Mens (1950) met het Europees Hof voor de Rechten van de Mens, zetelend te Straatsburg en (althans hier) in mindere mate door het gemeenschapsrecht en het Charter voor de EU Fundamentele Rechten (2001) met het Hof van Justitie te Luxemburg. We wijzen terloops op andere mensenrechtelijke teksten zoals de 1990 Conventie inzake de Rechten van het Kind en het aanvullende protocol bij deze conventie, met erin een heel mooie bepaling die stelt dat kinderen recht hebben op privacy. Hier echter houden we het even binnen Europa en meer bepaald bij het mooie werk geleverd door het Europees Hof voor de Rechten van de Mens.

Er bestaat geen twijfel over dat 'formeel' gesproken de Europese mensenrechtentekst even traditioneel is als de andere internationale teksten in de zin dat de tekst zich richt tot landen en geen rechtstreeks bindende verplichtingen oplegt aan bedrijven of particulieren. Illustratief is dat alleen landen te Straatsburg kunnen worden veroordeeld wegens een verdragsschending. Klachten tegen bedrijven en particulieren zijn gewoon niet-ontvankelijk. Daar moet je mee naar je eigen nationale rechter, maar dat veronderstelt dan weer dat er een rechter is, een gedegen rechtssysteem en een wetgeving die mensenrechtelijk conform is.

Precies op dit punt heeft het Europees Hof voor een doorbraak gezorgd met de leer van de positieve plichten. Deze in de Europese rechtspraak ontwikkelde leer is vrij uniek en was in haar soort zonder twijfel de eerste (Van Dijk 1998).[10] Het Europees Hof ontwikkelde de leer om overheidsgedragingen te toetsen, wanneer bijvoorbeeld de grondrechten van een individu niet door een overheidshandeling (of door een regelgeving die deze mogelijk maakt) worden bedreigd, maar door een stilzitten of een niet-handelen van de overheid. Tot dusver werd de leer vooral toegepast met betrekking tot de rechten beschermd door artikel 8 van het EVRM. Artikel 8 EVRM erkent grondrechten op bescherming van de persoonlijke levenssfeer, het gezin, de communicatie en de woning. Op basis van de leer wordt in deze bepaling niet alleen een verbod gelezen voor staten om zich te mengen in de grondrechten van de burgers, maar tevens een plicht voor verdragsstaten om maatregelen te nemen teneinde het effectieve genot van de rechten uit artikel 8 EVRM te verzekeren en om specifieke bepalingen in te voeren ter vermijding of bestraffing van handelingen van particulieren die deze rechten zouden miskennen of schenden (Renchon 1994: 98-102). Deze 'positieve' plicht staat niet met zoveel woorden in het Verdrag, maar ze werd er door het Hof uit afgeleid (Russo, Trichilo & Marotta 1995: 308).

De eerste toepassingen van de leer in de sfeer van artikel 8 EVRM vormen de arresten *Marckx* (1979) en *Airey* met betrekking tot het recht op familieleven en de arresten *Rees* (1986) en *Gaskin* (1989) met betrekking tot het recht op privéleven.[11] Meer recentelijk werd de leer van de positieve verplichtingen hernomen in de zaak-Stjerna (naamcorrectierecht) [12], de Guillot-zaak (naamgeving)[13], de zaak-Willsher (inzagerecht) [14], de zaken López Ostra en Guerra (leefmilieu)[15] en in de zaak-Botta (faciliteiten voor gehandicapten). [16]

In het laatstgenoemde arrest geeft het Hof aan dat van positieve plichten slechts sprake kan zijn "wanneer het van oordeel is dat de door de betrokkene gevraagde maatregelen een directe en onmiddellijke band vertonen met het privé- en familieleven van de betrokkene".[17] In laatste instantie komt het bijgevolg aan het Hof toe om uit te maken of er een positieve verplichting bestaat of niet.[18] Positieve plichten liggen bijgevolg niet bij voorbaat vast. Wat een effectieve eerbiediging van het privé- of familierecht aan initiatieven vereist van een staat valt niet op voorhand te bepalen.[19]

Decisief bij de ontwikkeling van deze theorie was de uitspraak van het Hof in de Marckx-zaak uit 1979. Uit het recht op eerbiediging van het gezinsleven vloeit niet alleen een plicht voor de overheid (voort) om zich van inmengingen in het gezinsleven te onthouden, maar ook een positieve plicht: die maatregelen nemen die inherent zijn aan een effectieve eerbiediging van het gezinsleven. Omwille van het recht op bescherming van het gezinsleven moeten de staten vooral die maatregelen nemen die nodig zijn om dit recht mogelijk te maken. Zo betekent het bestaan van positieve plichten met betrekking tot het gezinsleven dat staten bij het uitwerken van familierechtelijke regels, de normale ontplooiing van gezinsbanden niet mogen verhinderen, doch integendeel moeten mogelijk maken.

Nog datzelfde jaar deed het Hof uitspraak over de onmogelijkheid van mevrouw Airey om op grond van het Ierse recht in het echt te scheiden. Voor klaagster vormde deze wetgeving een inbreuk op meerdere grondrechten. Een ervan was het grondrecht op bescherming van het privéleven en van het gezinsleven. Van een inbreuk, aldus het Hof in deze zaak, is geen sprake. De kern van Aireys klacht is niet dat Ierland een handeling heeft gesteld, maar integendeel, dat het faalde om een handeling te stellen.[20] In identieke bewoordingen en met verwijzing naar deze uitspraak stelt het Hof in de Gaskin-zaak uit 1989 dat de weigering om Gaskin toegang te verlenen tot een dossier over zijn jeugdjaren, geen reële inbreuk op diens privé- en familieleven uitmaakt, daar de Britse overheid niet echt iets aanvangt met Gaskins gegevens (door ze bijvoorbeeld door te geven). Wel zou er sprake kunnen zijn van het niet-naleven van een positieve plicht uit hoofde van de Britse overheid om tegemoet te komen aan Gaskins verzoek.[21]

2.3.2 REGULERING VEREIST SOMS STRAFBAARSTELLINGEN

Het Hof heeft de leer van de positieve staatsplichten ook doorgetrokken naar het strafrecht. Soms kan die leer betekenen dat er extra stafrecht moet komen in een bepaalde lidstaat. Aanvangspunt voor dit aspect van ons verhaal is het arrest *X en Y t. Nederland* uit 1985.[22] In dit arrest gaat het Hof de leer van de positieve plichten toepassen op de problematiek van de bescherming van burgers tegen seksuele vergrijpen. Het 'effectieve respect' voor het privéleven brengt mee dat een staat de positieve verplichting heeft om maatregelen te treffen om het privéleven te verzekeren, zelfs in de sfeer van de onderlinge betrekkingen tussen individuen.[23] Het Hof veroordeelt Nederland, omdat in de interne wetgeving de mogelijkheid ontbreekt om strafvervolging in te stellen tegen iemand die seksueel geweld pleegde op een mentaal gehandicapt meisje dat juist zestien jaar geworden was.[24] Het recht op eerbiediging van het privéleven, aldus het Hof in deze zaak, verplicht de lidstaten maatregelen te nemen ter bescherming van de seksuele integriteit. Niettegenstaande dat het Hof de nationale *margin of appreciation* inzake de middelen ter bekrachtiging van het privéleven erkent, stelt het dat civielrechtelijke rechtsbescherming niet voldoet in het geval van een ernstige schending van de seksuele integriteit. Strafvervolging moet in dit geval mogelijk zijn.[25]

Een vergelijking van de Marckx-zaak met de zaak *X en Y t. Nederland* leert dat er in feite twee soorten van positieve plichten bestaan (Renchon 1994: 98-102). Enerzijds moet de staat maatregelen nemen die de uitoefening van grondrechten mogelijk maken.[26] Anderzijds moet de staat tevens specifieke bepalingen invoeren ter vermijding en/of bestraffing van handelingen van particulieren die grondrechten miskennen of schenden.[27] Beide plichten komen mooi samen in het arrest *M.C. t. Bulgarije* van 4 december 2003.[28] In deze zaak wordt Bulgarije veroordeeld omdat een verkrachte persoon juridisch niet beschermd werd door een bestraffing van de dader. Omdat het vermeende slachtoffer niet kon bewijzen dat het zich tegen de seksuele handelingen had verzet, volgde er geen strafrechtelijke veroordeling van de aangeklaagde mannen.[29] Voor het Europees Hof vormde deze nietvervolging een schending van de positieve verplichting van een verdragsstaat burgers te beschermen tegen inbreuken op hun fundamentele vrijheden en rechten. Het Hof stelde uitdrukkelijk dat er inzake verkrachting een verplichting bestaat om het onderzoek te concentreren op de toestemmingsvraag en om vanuit dat oogpunt alle feiten en de omstandigheden waarin ze plaats vonden te onderzoeken. Bovendien moet rekening worden gehouden met de bijzondere kwetsbaarheid en specifieke psychologie van jonge slachtoffers. Volgens de Straatsburgse rechters was de Bulgaarse overheid tekortgeschoten aan de overheidsverplichting een effectieve strafrechtelijke bescherming te bieden tegen verkrachting en seksueel misbruik. Dientengevolge concludeerde het Hof dat de artikelen 3 en 8 EVRM geschonden waren.[30]

Deze onderzoeksplicht naar mensenrechtenschendingen moet samen gelezen worden met de plicht tot het waarborgen van een effectieve remedie voor mensenrechtenschendingen vervat in artikel 13 EVRM. Dit recht geldt als een sluitstuk in het EVRM voor de bescherming van de rechten vervat in de overige bepalingen. Burgers 'hebben' niet alleen die rechten, doch ze 'hebben' ook recht er op dat schendingen van die rechten effectief geremedieerd worden.

Naast deze 'onderzoeksplicht' en deze 'remedieplicht' wordt in *M.C. t. Bulgarije* tevens een miskenning van de plicht tot behoorlijk en adequaat strafwetgeven vastgesteld. In de Bulgaarse wetgeving is er alleen sprake van strafbare verkrachting als er sprake is van aantoonbaar verzet van het slachtoffer. Eenvoudigweg *niet* toestemmen is onvoldoende. Het Europees Hof voor de Rechten van de Mens verwerpt resoluut deze 'wetgevende situatie'.[31] Het stelt dat de artikelen 3 en 8 EVRM staten ertoe verplichten om elke niet-consensuele seksuele daad strafbaar te stellen en effectief te vervolgen, ook wanneer het slachtoffer geen fysiek verzet heeft geboden. Het Hof baseerde deze interpretatie onder meer op de evolutie van het strafrecht in deze materie in de meeste Europese landen, evenals op rechtspraak van het Internationaal Strafgerechtshof voor voormalig Joegoslavië. In het bijzonder verplicht artikel 8 EVRM tot het voorzien in maatregelen om de relaties tussen individuen te regelen. Bij bijzonder ernstige aantastingen van fundamentele waarden en van het privéleven kan geen genoegen genomen worden met rechtsbescherming van niet-strafrechtelijke aard. Alleen het strafecht vormt hier het geschikte overheidsinstrument.[32] Gecombineerd met de onderzoeks- en handhavingsplichten gesteund op artikel 3 EVRM besluit het Hof dat: "States have a positive obligation inherent in Articles 3 and 8 of the Convention to enact criminal-law provisions effectively punishing rape and to apply them in practice through effective investigation and prosecution."[33]

2.3.3 EINDVERANTWOORDELIJKHEID EN DE IDEE VAN VERANTWOORDELIJKHEIDSDISTRIBUTIE

Het voorgaande samenvattend kunnen we stellen dat vanuit mensenrechtelijk perspectief de eindverantwoordelijkheid voor mensenrechtenschendingen steeds bij de overheid ligt. Daar moet voortaan op congressen over privacy niet meer over gestemd worden. Toch is daarmee niet gezegd dat de overheid altijd verantwoordelijkheid draagt of dat een overheid altijd moet ingrijpen. Komt het in een land over een mensenrechtenaandachtspunt nooit tot conflicten, dan is de overheid niet gehouden tot ingrijpen en kan ze rustig populaire mantra's over bijvoorbeeld zelfregulering door de bedrijfswereld laten klinken. Komt het wel tot conflicten, doch zorgt de overheid voor een strikt kader waarin adequaat gereageerd wordt op schendingen van mensenrechten, door bijvoorbeeld bedrijven administratiefrechtelijk of mensenrechtelijk onder druk te zetten ('aanscherpen van accountability', of verhogen van 'enforcement' op 'compliance'), dan is de overheid te Straatsburg gevrijwaard van aansprakelijkheid.

Een vertaling naar de respectievelijke rolverdeling in de informatiesamenleving is niet moeilijk. Het excuus dat de technologie snel evolueert en niet uit Eindhoven doch uit *Silicon Valley* komt, overtuigt niet langer. De overheid is verantwoordelijk voor de drie bouwstenen (Protect, Respect & Remedy).

De overheid moet met andere woorden:
– burgers beschermen tegen mensenrechtenschendingen door bedrijven en tegen misbruiken door andere gebruikers op internet (taak/bouwsteen 1);
– ervoor zorgen dat ondernemingen hun mensenrechtenplichten respecteren (taak/bouwsteen 2);
– zorgen voor vlot toegankelijke herstelmaatregelen of remedies (taak/bouwsteen 3).

Met betrekking tot de tweede taak kan de overheid ervoor kiezen (bewust of door niet op te treden) om het *accountability*-probleem *niet* door te schuiven naar de ICT-bedrijven en dienstenleveranciers, maar dan is ze te Straatsburg zelf verantwoordelijk voor mogelijke mensenrechtenschendingen door ondernemingen. Zij kan integendeel ervoor kiezen ICT-bedrijven en dienstenleveranciers wel verantwoordelijk te stellen en te binden aan bindende normen en dan doet de Straatsburgse test minder pijn.

Deze mensenrechtelijke analyse geeft mijns inziens wat meer lichaam en kleur aan de ideeën over verantwoordelijkheid uiteengezet in de al genoemde voorbereidende notitie *Beginsel Accountability*. Deze tekst geeft mooi aan hoe de roep naar accountability goed past in een postmoderne en digitale tijd waarin traditionele gezagsstructuren zoals toezicht door het parlement aan belang verliezen en waar complexe en snel evoluerende globaliserende en technologische processen succesvol anticiperende regulering via wetgeving en regeringsbeleid in de weg staan.[34] De tekst wijst op het onderscheid tussen verantwoording (beperkt, speelt alleen bij geschillen) en verantwoordelijkheid (ruimer) en op het onderscheid tussen gebruikersverantwoordelijkheid van de overheid (verantwoordelijkheid van de overheid voor problemen met eigen ICT-systemen) én op een systeemverantwoordelijkheid voor diezelfde overheid. Met dit begrip wordt gedoeld op de verantwoordelijkheid van de overheid voor het maatschappelijke gebruik van ICT: "Ten aanzien van de verantwoordelijkheid van de overheid voor de eigen applicaties heeft accountability een vrij natuurlijke plek – waarmee niet is gezegd dat hierin altijd wordt voorzien. Door accountability-arrangementen kunnen de onvermijdelijke onzekerheden die met de introductie van nieuwe systemen gepaard gaan enigszins worden opgevangen, door de problemen en geschillen die zullen rijzen alvast institutioneel een plek te geven. Voor de systeemverantwoordelijkheid van de overheid voor informatietechnologische ontwikkelingen buiten haar eigen organisatie heeft accountability een wat andere positie. De overheid staat als het ware aan de zijde van de individuele burger in het eisen van accountability van

dienstverleners op de ICT-markt. Dit is, bezien vanuit de overheid, een moeilijkere rol dan het inrichten van verantwoording in de eigen processen."[35] Als voorbeelden van deze verantwoordelijkheid geven de auteurs het inrichten van adequate fora om conflicten te beslechten en de introductie van beschermende randvoorwaarden voor de regulering van bepaalde subpolitieke niches op internet met veel, te veel sociale macht.[36]

In mensenrechtelijke zienswijze van Straatsburg is de overheid niet rechtstreeks verantwoordelijk voor alle mensenrechtenschendingen in Europa, maar wordt ze verantwoordelijk gemaakt voor het niet adequaat reageren op mensenrechtenschendingen onder haar jurisdictie. Straatsburg zorgt derhalve voor de juridische sprong van verantwoording voor de eigen geschillen naar systeemverantwoordelijkheid, een begrip dat naar mijn smaak in de voorbereidende notitie *Beginsel Accountability* iets te veel in de lucht hangt. Wanneer er mensenrechten op het spel staan, en dat is het geval, is systeemverantwoordelijkheid niet vrijblijvend maar een juridische opdracht. Overheden moeten aan de zijde van de burgers gaan staan in het eisen van accountability. Een deel van de systeemverantwoordelijkheid bestaat er bijgevolg in om actoren zoals internetbedrijven te responsabiliseren. Overheden zijn niet rechtstreeks verantwoordelijk voor elke mensenrechtenschending, maar dienen ervoor te zorgen dat via een efficiënte verantwoordelijkheidsdistributie verantwoordelijkheden belegd worden.

Dat brengt me bij een tweede bedenking. In de genoemde voorbereidende notitie *Beginsel Accountability*, en de erin aangehaalde literatuur, wordt te snel het einde van het traditioneel rechtstatelijk denken aangekondigd. Bijna elke *governance*-tekst wijst op de gebreken van het traditionele *government*. Ontwikkelingen op het vlak van technologie en globaliseren halen de pijlers van die traditionele gezagsvormen onderuit, heet het dan. Ik heb me, als jurist, nooit helemaal in die analyses kunnen vinden. Een recht is wat mij betreft altijd meer proces dan structuur geweest, een systeem van bewegwijzering waarbij feiten en gebeurtenissen toegedicht (geattribueerd) worden aan personen en waarbij rechters door het spreken van recht en juridische beginselen van attributie zorgen voor een systeem van verantwoordelijkheden (Gutwirth, De Hert & De Sutter 2008; De Sutter & Gutwirth 2004). Los van traditionele en strakke aansprakelijkheidsmechanismen uit het privaatrecht en *tort law* ontwikkelt Straatsburg een aansprakelijkheidssysteem dat in meer dan één opzicht modern is: wordt er geklaagd over een mensenrechtenschending, dan is de overheid verantwoordelijk te Straatsburg wanneer onzorgvuldigheden of fouten blijken in de eigen accountability-arrangementen of wanneer onzorgvuldig of geen verantwoordelijkheidsdistributie heeft plaatsgevonden. Dat is een meer dan machtig antwoord op in de literatuur aangevoerde tekortkomingen van het klassieke rechtssysteem.

Hernemen we de opmerking uit de voorbereidende notitie *Beginsel Accountability* dat internetgebruikers helemaal niets begrijpen van de onzichtbare protocollen van internet[37], en dat door het gebruik van informatietechnologie de anatomie van beslissingen aan het oog wordt onttrokken waardoor bepaalde handelingen minder goed toetsbaar zijn.[38] Straatsburg haalt eenvoudig de schouders op en maakt de overheid verantwoordelijk voor schendingen van het recht op privacy wanneer geen wetgevende en regulatieve initiatieven zijn genomen om deze te beschermen en voor schendingen van het recht op een effectief rechtsmiddel (artikel 13 EVRM) wanneer er onvoldoende accountability-arrangementen zijn gecreëerd. Hoezo postmoderne vaagheid?

Vanuit Nederlands perspectief en vanuit een beleidsperspectief is het voorgaande geen bron van vreugde. Het verhaal van globalisering en van complexe technologische ontwikkelingen is er een dat door politici vaak strategisch uitgespeeld wordt om verantwoordelijkheden weg te schuiven[39], maar hier wordt nu een wat klemmender verhaal verteld over positieve plichten om wel verantwoordelijkheid te nemen. Hoe ver strekken die positieve verplichtingen tot systeemverantwoordelijkheid dan wel? Er zijn meerdere analyses geschreven over de bescherming geboden door Europese rechters aan kwetsbare groepen. Onder meer Olivier De Schutter heeft in een essay gewezen op de gemiste kansen in de rechtspraak van het Europees Hof én op de structurele of institutionele beperkingen van het rechtersrecht voor de ontwikkeling van het mensenrechtenrecht (De Schutter 2005). Er wordt te veel gewerkt met open begrippen en de uitslag van de concrete zaken is te zeer gebonden aan de onmiddellijke context van de eiser. Het 'binaire' karakter (alles of niets) van de rechtsprekende functie leidt bij rechters vaak tot een *hands-off approach* eerder dan tot een geleidelijke ontwikkeling van het recht. Ook het schaarsteprobleem leidt tot rechterlijke terughoudendheid: als een rechter een claim inwilligt, zal dit ten koste gaan van andere noodzakelijke overheidstaken (De Schutter 2005: 42-43; Fuller 1972).[40]

Het antwoord op de vraag 'wat nu precies Straatsburg allemaal aan positieve plichten meebrengt voor een privacybeleid' is bijgevolg niet eenvoudig. Waarschijnlijk is de vraag ook niet op zijn plaats. Het doordenken van mensenrechten is niet uitsluitend de taak van het Europees Hof. Mensenrechten zijn in de eerste plaats een verantwoordelijkheid van de lidstaten die ze erkennen. Dit sluit aan bij de zienswijze dat het Europees mensenrechtensysteem stoelt op het zogenaamde subsidiariteitsbeginsel. Dit beginsel dat niet expliciet terug te vinden is in het EVRM, doch wel inherent aanwezig is (Vande Lanotte & Haeck 2005), luidt dat de bescherming van de in het Verdrag neergelegde mensenrechten in eerste instantie een zaak is van de lidstaten zelf. Zij dienen zorg te dragen voor een effectieve bescherming en voor een redresmogelijkheid in geval de bescherming onverhoopt toch op de één of andere manier tekortschiet. Het Europese stelsel speelt slechts een aanvullende rol en komt pas in beeld wanneer de nationale autoriteiten

zich niet of onvoldoende aan hun taak hebben gewijd. Het is bijgevolg aan Nederland zelf om de idee van negatieve en positieve plichten door te denken in de context van de informatiemaatschappij.[41] Het Hof gaat zich daarbij terughoudend opstellen, onder meer om niet in de plaats te gaan staan van de overheden die keuzen moeten maken in functie van factoren zoals budgettaire beperkingen, maar gaat wel kijken naar het eindresultaat en dat moet erin bestaan dat de verdragsrechten praktisch en effectief blijven en niet tot dode letter verworden.[42]

Aan Den Haag om de uitdaging verder op te nemen, aldus de Europese rechters. Toch is er een dialoog. Uit Straatsburg komen steeds meer arresten met grote relevantie voor de regulering van de informatiesamenleving en hieruit kunnen veel waardevolle elementen afgeleid worden voor een verantwoordelijk systeembeleid. We bekijken enkele van de belangrijke arresten.

2.4 SYSTEEMVERANTWOORDELIJKHEID INZAKE TOEGANG EN PUBLIEKE PRIVACY: GASKIN EN PECK

Eerder stonden we stil bij het arrest *Gaskin* uit 1989. Het arrest toont mooi aan dat de leer van de positieve plichten perfect toe te passen is op problemen in verband met privacy: het niet toegang verlenen tot je eigen persoonsgegevens schendt het Verdrag. Het toegangsrecht is bijgevolg een mensenrechtelijke positieve plicht. Van personen die persoonsgegevens onder zich hebben wordt een inspanning gevraagd en geen stilzitten.

Op dit punt moeten nationale overheden echter beleid vooraf maken. Het systeem van Straatsburg is immers geen opvangsysteem dat *altijd* werkt: het Hof is geen grondwettelijk Hof en werkt slechts subsidiair. Een burger of groepering kan bijvoorbeeld niet naar Straatsburg wegens het ontbreken van een wettelijke regeling voor technologie als er *geen* aanwijsbaar, concreet mensenrechtelijk probleem is. Dat ondervond de Belgische Liga voor de Mensenrechten die te Straatsburg opkwam tegen het ontbreken in de Belgische wetgeving van een wettelijke regeling op camerabewaking. De klacht werd niet ontvankelijk verklaard.[43] Het was dus wachten op een echt cameraprobleem. Dat kwam er pas vele jaren later in de zaak Peck.[44] In deze zaak was een beeldverslag gemaakt van een zelfmoordpoging op een publieke plaats. De op de Britse televisie vertoonde beelden waren afkomstig van CCTV-bewakingscamera's die ter beschikking gesteld waren aan journalisten. Het Hof veroordeelt deze praktijk: bekendmaking via de media van privacygevoelige gegevens is in casu een inbreuk op artikel 8 EVRM. Het herkenbaar tonen van verzoeker op televisie en het publiceren van zijn foto in de pers vormt een inbreuk op zijn recht op privacy. Dit recht was geschonden, omdat de betrokkene daarvoor geen toestemming had gegeven. Bovendien was de persoon ook niet onherkenbaar gemaakt.[45] We vermelden de zaak terloops, omdat de feiten ook duidelijk aangeven dat de visie dat alles wat we in het openbaar doen ipso facto

onbeschermd is onjuist is. Het Hof erkent ook privacy voor handelingen buiten de strikte privésfeer en betrekt daarbij onder meer het criterium van de redelijke privacyverwachting. Vertaald naar sociale netwerken betekent dit dat we ons recht op privacy niet voor altijd kwijt zijn, omdat we gegevens uitwisselen naar anderen, zeker niet als we de verwachting hebben dat de verantwoordelijke van de netwerksite zorgvuldig met onze gegevens omspringt.

2.4.1 SYSTEEMVERANTWOORDELIJKHEID BETREFFENDE BEVEILIGING: I. T. FINLAND

In 2008 werd aan deze leer van de positieve plichten in de sfeer van het gebruik van persoonsgegevens een nieuwe dimensie toegevoegd in het arrest *I. tegen Finland (I. t.)* gewezen op 17 juli 2008.[46] In het kort besliste het Hof in dit arrest dat beveiligingsmaatregelen genomen door een Fins ziekenhuis en bedoeld om het recht op respect voor het privéleven te garanderen van een hiv-patiënte die in datzelfde ziekenhuis werkte, inadequaat waren en een schending van artikel 8 van het EVRM uitmaakten. In wat volgt spitten we deze belangrijke zaak wat verder uit, omdat ze aantoont hoe heerlijk concreet Straatsburg doorwerkt.

De verzoekster werkte tussen 1989 en 1994 als verpleegster op de afdeling voor oogziekten in een publiek ziekenhuis in Finland. Sinds 1987 bezocht ze regelmatig de afdeling 'besmettelijke ziekten' in datzelfde hospitaal, omdat hiv bij haar vastgesteld werd. Na drie jaar gewerkt te hebben in het ziekenhuis rees bij haar het vermoeden dat haar collega's wisten van haar ziekte. Medewerkers van het ziekenhuis hadden in die tijd vrije toegang tot informatie over de patiënten en hun gezondheid. Op haar vraag werd deze situatie rechtgezet. Voortaan kreeg enkel het behandelende personeel toegang tot de patiëntendossiers. Bovendien werd klaagster onder een valse naam en onder een nieuw uniek nummer ingeschreven. In 1995 werd haar arbeidsovereenkomst niet verlengd. In november 1996 diende de verzoekster een klacht in bij de County Administrative Board, omdat haar persoonlijke gegevens misbruikt zouden zijn. Ze vroeg om te mogen nagaan wie allemaal toegang had gehad tot haar gegevens. De directeur van het archief beweerde echter dat dit onmogelijk was, aangezien het systeem enkel de vijf meest recente raadplegers weergeeft. Bovendien geeft het systeem slechts de raadplegende afdeling weer, niet de persoon die het dossier geraadpleegd heeft. Deze informatie wordt ook nog eens allemaal verwijderd, zodra het dossier terug in het archief zit. De klacht van de verzoekster werd dus verworpen. Nadien werd het archiefsysteem van het ziekenhuis zo aangepast dat het mogelijk werd om te kunnen bepalen wie de patiëntengegevens geraadpleegd had.

Een serie van burgerlijke procedures die door de verzoekster voor de District Court en het Court of Appeal gebracht werden tegen de autoriteit die toezicht moest houden op het ziekenhuis, werden allemaal afgewezen, omdat de verzoek-

ster niet kon bewijzen dat haar gegevens onwettelijk geconsulteerd werden. Een beroep voor het Finse hooggerechtshof werd ook afgewezen, waarop de verzoekster naar het Europese Hof voor de Rechten van de Mens stapte. Te Straatsburg roept de verzoekster in dat de Finse toezichthoudende autoriteit gefaald had in haar verplichting om een systeem op poten te zetten waarin patiëntengegevens niet onwettig gebruikt konden worden, wat volgens haar strijdig is met artikel 8 van het EVRM. Het vereiste van retrospectieve controle is volgens haar essentieel voor het respecteren van dit recht. De Finse overheid antwoordde hierop dat de nationale wetgeving patiëntengegevens adequaat beschermt en dat "systemen ontwikkeld worden in de ziekenhuizen die het bijhouden van dossiers over patiënten mogelijk maken, maar dat deze systemen alleen correct kunnen werken als er gedetailleerde instructies aan het personeel gegeven worden, als zij hoge morele standaarden respecteren, er toezicht uitgeoefend wordt en het personeel het beroepsgeheim naleeft." In casu was het aldus de Finse overheid niet mogelijk geweest voor het ziekenhuis om een systeem te creëren waarbij vooraf de authenticiteit van elk verzoek gecontroleerd kan worden, aangezien toegang tot de gegevens vaak onmiddellijk en dringend vereist is.

In het beschikkende gedeelte van het arrest gaat het Hof allereerst een aantal algemene beginselen inzake persoonsgegevens identificeren. Het Europese Hof bevestigt dat medische gegevens binnen de draagwijdte van artikel 8 EVRM vallen en dat "de bescherming van persoonlijke gegevens, en specifiek medische gegevens, van fundamenteel belang zijn voor het recht van een persoon op respect voor zijn/haar privé- en familieleven". Het Hof erkent ook dat de belangrijkste – negatieve – doelstelling van artikel 8 bestaat uit "het beschermen van individuen tegen arbitraire inmengingen door publieke autoriteiten", maar het benadrukt tezelfdertijd dat er ook positieve verplichtingen kunnen voortvloeien uit het recht op respect voor iemands privéleven. Deze verplichtingen omvatten onder meer het aannemen van maatregelen die het recht op respect voor het privéleven kunnen verzekeren, zelfs wanneer deze regels betrekking hebben op relaties tussen individuen onderling.[47] Het Hof merkt op dat de bescherming van persoonsgegevens, in het bijzonder deze van gezondheidsgegevens, van fundamenteel belang is voor het recht op bescherming van het privéleven én van het gezinsleven van de patiënt.[48] Die bescherming is cruciaal voor het respect van het gevoel en de verwachting van privacy van de patiënt ("the sense of privacy of a patient"), maar ook cruciaal voor het vertrouwen van de patiënt in de medische beroepen en de gezondheidsdiensten in het algemeen.[49] Positieve plichten betreffende de zorg voor persoonsgegevens dienen derhalve niet een louter individueel belang en kunnen ook van particulieren geëist worden.

Na deze opsomming van beginselen kijkt het Hof naar het Finse recht en de gebeurtenissen in deze zaak. Het Hof staat stil bij de Finse Wbp, de *Personal Files Act* van 1987. Artikel 26 van deze wet verplicht de verwerker om beveiligingsmaat-

regelen te nemen en ervoor te zorgen dat alleen het behandelende personeel toegang krijgt tot het dossier. Strikte toepassing van deze bepaling zou een effectieve bescherming in de zin van artikel 8 EVRM zijn geweest en zou het ziekenhuis hebben toegelaten om toegang te controleren ("to police strictly access to a disclosure of health records"). [50] Het Hof stelt vast dat er in casu geen adequate beveiliging was en besluit dat er sprake was van een miskenning van de Finse wetgeving en (daarom) tot een schending van het EVRM: het nemen van beveiligingsmaatregelen door bedrijven en instellingen zoals neergelegd in de wetgeving op de bescherming van de persoonsgegevens vormt niet louter een morele of wettelijke plicht, doch een positieve mensenrechtenplicht. Niet naleven van die plicht is op zich een inbreuk op het mensenrechtenverdrag.

Bovendien is ook de controle op wat er fout loopt bij het gebruik van persoonsgegevens een positieve mensenrechtelijke plicht. Wat nodig is, aldus het Hof, is een praktische en effectieve bescherming om elke mogelijkheid tot ongeautoriseerde toegang uit te kunnen sluiten. Deze bescherming werd hier echter niet gegeven.[51]

Laten we een tussenstand maken en ons even richten tot de Nederlandse beleidsmensen die Straatsburg en de leer van de verdragsverplichtingen te vaag vinden (zo die er al zijn). In voorliggend arrest is geen sprake van vaagheid.

- Zoals steeds meer het geval is in de rechtspraak van het Hof, vangt het beschikkend gedeelte aan met een opsomming van algemene beginselen die het Hof als uitgangspunt neemt (Lawson & Verheij 2002: 514). Het Hof komt zo los van de traditionele casuïstische benadering van rechtspreken en tracht wat meer houvast te bieden in de uitspraken voor staten met het oog op het aanpassen aan de normen van het verdrag zoals die door het Hof ontwikkeld worden.
- Bovendien gaat het Hof de concrete zaak ook aan de hand van deze canon van algemene beginselen inzake persoonsgegevens beoordelen, wat nog meer concrete richtlijnen oplevert.
- Duidelijk blijkt dat het omgaan met persoonsgegevens door individuen en instellingen adequate beveiligingsmaatregelen verlangt, bedoeld om het recht op respect voor het privéleven te garanderen.
- Algemener kan gesteld worden dat door het naleven van de in lidstaten bestaande wetgeving betreffende de bescherming van persoonsgegevens, tegemoet wordt gekomen aan de positieve verplichtingen afgeleid uit het EVRM.

2.5 SCHADEVERGOEDING MAG NOOIT DE ENIGE OPLOSSING ZIJN; DE IDEE VAN BESCHERMING VOORAF

Er vallen nog meer richtlijnen in *I. t. Finland* te ontwaren. Verzoekster beklaagt zich immers tevens over de wijze waarop met schadevergoeding wordt omgesprongen in het Finse recht. In dat verband klaagt ze niet alleen over een schending van artikel 8 EVRM, maar ook van artikel 6 en 13 EVRM.

Het Hof stelt vast dat de verzoekster haar burgerlijke procedures in Finland wegens de schending van de regels op het gebied van bescherming van de persoonsgegevens verloren had, omdat ze er niet in slaagde een causaal verband aan te tonen tussen de tekortkomingen in de toegangsregels en de onterechte verspreiding van informatie over haar medische toestand. Het Europees Hof is duidelijk niet gecharmeerd door deze klassieke, ook in Nederland bekende, civielrechtelijke benadering van aquiliaanse[52] schadegevallen. Het plaatsen van een dergelijke bewijslast op de schouders van de verzoeker is unfair, aldus het Hof: "to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital's record keeping at the material time".[53] Als het ziekenhuis een grotere controle op de toegang tot de gezondheidsgegevens had uitgevoerd, bijvoorbeeld door alleen de personen die direct betrokken zijn bij de behandeling, toegang tot de gegevens te verschaffen of door een logboek bij te houden van alle personen die toegang hebben gehad tot de gegevens, dan had de verzoekster in een minder slechte bewijspositie gestaan voor de nationale rechtbanken. Die strenge lijn wordt doorgetrokken naar de vraag hoe de schadevergoeding voor verzoekster berekend moet worden. In de praktijk blijkt dit een heikel punt voor toezichthouders. Wat is de schade als er onzorgvuldig met persoonsgegevens wordt omgesprongen? We hebben net gezien dat het Hof op dit punt geen al te grote bewijslast uit hoofde van de geregistreerde burger verlangt. Aan dit uitgangspunt voegt het Hof toe dat verzoekster eveneens in aanmerking komt voor vergoeding van niet-geldelijke schade. Verzoekster heeft niet-geldelijke schade geleden en komt daarom in aanmerking voor geldelijke schadevergoeding. "Het niet naleven van een beveiligingsplicht wordt niet gecompenseerd door eenvoudige aanpassing van de beveiligingsmaatregelen, doch vereist een geldelijke schadevergoeding."[54]

Het belang van het arrest *I. t. Finland* van 17 juli 2008 voor de discussie over de inrichting van de informatiemaatschappij is nog veel te weinig aan de orde gesteld. Het Hof stelt met zoveel woorden dat het loutere feit dat de nationale wetgeving de mogelijkheid geeft om een vergoeding te vragen na geleden privacyschade, onvoldoende is. De overheid moet zorgen voor een praktische en effectieve bescherming van dit rechtsgoed. Voorzien in een systeem van schadevergoeding (Ruggies derde bouwsteen) is dus niet genoeg. Een samenleving moet zich inzetten om mensenrechtelijke standaarden te realiseren en ook het recht kan daarbij een rol spelen. De overheid is verantwoordelijk voor het eindresultaat. In de terminologie van de voorbereidende notitie *Beginsel Accountability* kunnen we zeggen dat er niet alleen juridisch afrekenen achteraf, maar ook sturing vooraf door wetgeving en toezicht moet zijn.[55] Daarmee is niet gezegd dat Ruggies derde bouwsteen niet belangrijk is. Integendeel. Een systeem van schadevergoeding voor opgetreden schade moet bestaan en moet zijn gebaseerd op eerlijke en toegankelijke procedures. Er mag geen onredelijke bewijslast worden gelegd op de schouders van het rechtssubject en er moet worden voorzien in een geldelijke schadevergoeding.

2.5.1 ALS ER SCHADEVERGOEDING WORDT TOEGEKEND MOET DEZE REDELIJK DOCH SUBSTANTIEEL ZIJN

We horen de bedenking al komen: waar gaat dat naar toe als we voor schendingen van regels over gebruik persoonsgegevens ook schade moeten uitbetalen voor geleden niet-geldelijke schade? Wat zijn de grenzen van een dergelijke verplichting? Voor het Europees Hof moet dergelijke schadevergoeding redelijk zijn. Deze eis dat schadevergoeding bij misbruiken én ongelukjes met persoonsgegevens redelijk moet zijn blijkt uit het arrest *Armonas t. Litouwen* uit 2008.[56] Ik ga wat nader in op de feiten in deze zaak. Ze geven de dagelijkse berichten in onze kranten over 'ongelukjes' met persoonsgegevens (verlies, uitlekken in de pers, enz.) een bijzondere dimensie.

Armonas, woonachtig in het Litouwse district Pasvalys, is de vrouw van een zekere L. A., die gestorven is op 15 april 2002. Op 31 januari 2001 bericht *Lietuvos Rytas*, de grootste Litouwse krant, over een zogenaamde aidsdreiging die zou heersen in de dorpen van Pasvalys. Het voorpagina-artikel vermeldt L. A. bij naam en toenaam en identificeert hem als een aidspatiënt. Het artikel meldt ook dat hij twee buitenechtelijke kinderen zou hebben bij een vrouw, G. B., die eveneens aidspatiënt was. L. A. vangt een procedure aan tegen de krant en krijgt een schadevergoeding toegekend wegens schending van zijn privacy. Er zouden onvoldoende bewijzen zijn voor de buitenechtelijke relatie. De rechtbank oordeelt echter dat de informatie betreffende de buitenechtelijke relatie en de gezondheidstoestand niet opzettelijk zou zijn kenbaar gemaakt. De schadevergoeding kan daarom wettelijk niet hoger zijn dan 10.000 LTL (ongeveer € 2.896). Armonas richt zich vervolgens tot het Europees Hof met de interessante klacht dat er een schending is van haar recht op privéleven wegens de bespottelijk lage schadevergoeding die aan haar man werd toegekend, ondanks de erkenning door de rechter dat er een schending van het privéleven had plaatsgevonden. Een dergelijk lage schadevergoeding zou ook niet voldoen aan de vereisten, conform artikel 8 en 13 EVRM, om te beschikken over een effectief rechtsmiddel.

Technisch was het niet een-twee-drie zeker dat een dergelijke klacht een kans zou maken, doch het Europees Hof verklaart de klacht ontvankelijk[57], wat meestal al een signaal is voor de bereidheid van het Hof om de zaak ook ten gronde ernstig te nemen. Opnieuw vertrekt het Hof vanuit de idee dat er negatieve en positieve plichten rusten op lidstaten. Deze laatste plichten kunnen onder meer betekenen dat de overheid maatregelen moet nemen om het privéleven te beschermen in relaties tussen individuen.[58] Evenredigheid is een centrale notie bij de beoordeling van de reikwijdte van die plichten en in casu moet een faire balans gevonden worden tussen de persvrijheid en het recht op privéleven.[59]

Bij die beoordeling ten gronde maakt het Hof een onderscheid tussen het verspreiden van feitelijke informatie als onderdeel van een maatschappelijk debat enerzijds en smakeloze beschuldigingen betreffende het privéleven van een persoon anderzijds.[60] De bescherming van het privéleven is er om de personen te stimuleren in hun ontwikkeling, waarbij de geboden bescherming verdergaat dan de familiekring en tevens een bepaalde sociale dimensie van het individu beschermt.[61] Het privacygrondrecht is daarom zonder twijfel van toepassing op deze zaak. De publicatie van informatie over de gezondheidstoestand van Armonas' man draagt niet bij tot een maatschappelijk debat en diende enkel om de nieuwsgierigheid van een bepaald lezerspubliek te dienen. De balans weegt daarom in casu in het voordeel van het individuele recht op privacy. De overheid had de plicht om ervoor te zorgen dat dit recht kon worden afgedwongen ten opzichte van de pers. Het Hof tilt overigens zwaar aan de bewering in het artikel dat de informatie over de gezondheidstoestand was bevestigd door de werknemers van het aidscentrum. Dit zou, volgens het Hof, ontmoedigend kunnen werken op anderen om vrijwillig aidstesten te laten afnemen. De bescherming van de persoonsgegevens in deze context is van bijzonder belang.

Het Litouwse recht beschikt, aldus het Hof, over beschikkingen ter bescherming van vertrouwelijke informatie en een schadevergoeding werd toegekend. Echter, de vraag is of de hoogte van de schadevergoeding evenredig is tot de schade en in welke mate de wettelijke beperkingen op de berekening ervan conform artikel 8 EVRM zijn. Ook al laat het Hof een zekere beoordelingsmarge aan staten betreffende het regelen van financiële vergoedingen, en moet rekening gehouden worden met de socio-economische toestand van een land, de beperkingen mogen er niet toe leiden dat het recht op zich wordt uitgehold. Het Hof erkent dat het opleggen van al te zware sancties op de pers een *chilling effect* kan hebben op de persvrijheid.[62] Echter, in geval van een manifest misbruik van die vrijheid zoals in casu het geval is, meent het Hof dat de zware wettelijke beperkingen op de compensatie van de slachtoffers niet in lijn ligt met de verwachtingen die men op dat gebied conform artikel 8 EVRM heeft. Er is daarom een schending van artikel 8 EVRM en Litouwen wordt dan ook veroordeeld.[63]

2.5.2 HET ARREST ARMONAS T. LITOUWEN UIT 2008: SAMENVATTENDE BESCHOUWING

Het arrest *Armonas t. Litouwen* uit 2008 geeft aan dat niet zomaar alles in de krant mag geschreven worden. De lering kan doorgetrokken worden naar andere media zoals internet. Ook hier geldt het onderscheid tussen het verspreiden van feitelijke informatie als onderdeel van een maatschappelijk debat enerzijds en smakeloze beschuldigingen betreffende het privéleven van een persoon anderzijds. De overheid moet de burger tegen dit laatste beschermen en burgers en kranten moeten ervan afzien dergelijke informatie te plaatsen. In feite wisten we dit al door een

ander beroemd arrest, ditmaal van het Hof van Justitie te Luxemburg, het arrest *Bodil Lindqvist* van 6 november 2003.[64] Door het arrest *Armonas* van Straatsburg krijgen we echter meer inzicht in het evenwicht dat tussen bescherming van privéleven en bescherming van de persvrijheid en meningsvrijheid moet gevonden worden, vooral door het belangrijke onderscheid tussen het verspreiden van feitelijke informatie als onderdeel van een maatschappelijk debat enerzijds en smakeloze beschuldigingen betreffende het privéleven van een persoon anderzijds.
Op deze criteria oordeelde de kortgedingrechter in Amsterdam eind 2009 dat een filmpje van een dronken studente ("Jullie moeten mij majesteit noemen, ik ben de praeses") op de 'shockblog' GeenStijl niet alleen het portretrecht van studente schendt, doch ook haar privéleven. De rechter weegt dit belang af tegen het nieuwsbelang dat GeenStijl claimde, en komt tot de conclusie dat het laatste het moet afleggen wegens te weinig nieuwswaarde.[65] Zonder te verwijzen naar het brede privacybegrip gehanteerd door het Europees Hof, onder meer in *Armonas*, verwerpt de kortgedingrechter het argument van GeenStijl dat er geen privacybescherming zou gelden voor de studente, omdat ze "midden in de nacht op straat gefilmd zou zijn" (overweging 4.7). Er is duidelijk schade aan het privéleven van de studente, onder meer door wat met de beelden vervolgens werd aangevangen, maar reeds op het ogenblik van het filmen van de beelden geldt de bescherming van het recht op privéleven ook onder meer omdat "zij geen bekende persoonlijkheid is en geen publieke functies vervult" (overweging 4.7. en 4.9).[66]

Het arrest *Armonas t. Litouwen* uit 2008 leert tevens dat door de leer van de positieve verplichtingen van artikel 8 EVRM overheden het recht op bescherming van persoonsgegevens op alerte en passende wijze moeten beschermen, desnoods via het opleggen van voldoende hoge schadevergoedingen in geval van inbreuken door uitgevers, mediabedrijven of adverteerders (Voorhoof 2009: 155).[67] Ook leert het arrest *Armonas* dat schadevergoeding qua omvang een verband dient te tonen met de geleden schade waarbij te lage forfaits niet kunnen. Staten moeten bijgevolg hun schadevergoedingssysteem (Ruggies derde bouwsteen) uitbouwen, zodat remediëring van schade mogelijk wordt zonder een excessieve bewijslast en zonder schijnjustitie in de vorm van bespottelijk lage schadevergoedingen. Een effectieve remedie en een effectief rechtsmiddel in de zin van het EVRM moet voorhanden zijn, ook wanneer er uitsluitend sprake is van morele schade als gevolg van een schending van het zelfbeschikkingsrecht.[68]

Vraag is of deze op dit ogenblik in Nederland voorhanden is. Het staartje van het hiervoor besproken kort geding plus vonnis van GeenStijl is niet onschuldig. Weliswaar moet GeenStijl de beelden van zijn website halen, doch de kortgedingrechter weigert in te gaan op de eis van de studente dat GeenStijl Google zou benaderen om verdere verspreiding op andere sites tegen te gaan (overweging 4.12.) en weigert tevens zich uit te spreken over de vordering tot het verwijderen

van kopieën (overweging 4.13). Heel de kwestie van de schadevergoeding wordt naar de bodemrechter doorverwezen. Met dit laatste valt te leven, maar of het beperken van de gevolgen van het vonnis tot het ene filmpje in handen van Geen-Stijl effectief is, terwijl de beelden circuleren op internet, is twijfelachtig.[69]
In wat volgt wil ik ingaan op de taken van de wetgever. Uit het voorgaande blijkt dat deze een systeem van rechtsbescherming én toezicht vooraf moet instellen.
In mijn recente werk heb ik veel aandacht besteed aan recente Europese mensenrechtspraak (De Hert 2009). De Europese rechters hebben zich met veel vertraging de idee eigen gemaakt dat er ook zoiets bestaat als privacy buiten de slaapkamer. Dit inzicht bestond al veel langer in het gegevensbeschermingsrecht (*law of data protection*) dat consequent elk persoonsgegeven beschermwaardig acht. Rechters hebben het er echter om allerlei redenen moeilijk mee gehad om zich dit uitgangspunt eigen te maken (De Hert & Gutwirth 2001). Codificatie van nieuwe inzichten in mensenrechtenteksten en grondwetten kan dan helpen als steun in de rug voor rechters. Het kan echter ook een steun in de rug zijn voor de nationale wetgever.

2.6 HET EU HANDVEST ALS OPSTAP NAAR SYSTEEMVERANTWOORDELIJKHEID VAN DE WETGEVER

De grote meerwaarde van het op 7 december 2000[70] en op 14 december 2007 afgekondigde[71] en via het Verdrag van Lissabon[72] bindend verklaarde EU Handvest voor de Fundamentele Rechten schuilt in het gegeven dat deze tekst niet alleen de inhoud van het EVRM herneemt, doch tevens nieuwe mensenrechtenontwikkelingen codificeert. Artikel 7 van het Handvest bevat het ons uit het EVRM vertrouwde privacyrecht. Artikel 8 van het Handvest gaat echter een stap verder dan het EVRM en erkent een zelfstandig recht op bescherming van persoonsgegevens. In de bepaling wordt min of meer in detail een aantal beginselen van het gegevensbeschermingsrecht mensenrechtelijk verankerd. De bepaling zegt namelijk niet alleen dat persoonsgegevens moeten worden beschermd, doch ook dat:

- persoonsgegevens moeten worden verwerkt op eerlijke wijze,
- persoonsgegevens moeten worden verwerkt voor bepaalde doeleinden (doelbinding),
- persoonsgegevens moeten worden verwerkt met toestemming van de betrokkene of(,)
- persoonsgegevens moeten worden verwerkt op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet,
- eenieder recht heeft op toegang tot de over hem verzamelde gegevens,
- eenieder recht heeft op correctie daarvan,
- eenieder recht heeft op een onafhankelijke toezichthouder die toeziet op de naleving van de wet.

Al deze beginselen, die we kennen uit de Wbp en enkele internationale teksten (*infra*) staan voortaan fijntjes in een tekst met groot gezag. In het bijzonder de opname van het doelbindingprincipe verdient waardering, omdat dit principe erg grote implicaties heeft op het werk van bijvoorbeeld justitie en politie en op de handelswijze van controlerende werkgevers (De Hert & Gutwirth 2001: 315-317). Ook is dit principe zwak verankerd in de Aziatische en Amerikaanse wetgeving, zodat het geen kwaad kan om in een tekst te benadrukken dat Europa er belang aan hecht.[73] Hetzelfde geldt voor dat andere pijnpunt in de transatlantische relaties, de vraag of er verplicht een toezichthouder moet geïnstalleerd worden in een rechtssysteem dat gebruik van persoonsgegevens toelaat. De opname van deze nieuwe rechten in de hoogste fundamentele rechten is niet zonder betekenis, zoals de VS recent mocht ondervinden toen het Europees Parlement zich kantte tegen inzage van Swift-bankgegevens wegens te weinig begeleidende waarborgen (Pop 2010).

2.6.1 'WAAROM SPECIFIEKE BIOMETRIEWETGEVING? DE WBP IS TOCH VAN TOEPASSING!'

Die volwassen houding van Europa zit niet alleen op het niveau van de affirmatie van nieuwe fundamentele rechten, maar ook in het vertalen van die basiswaarden en uitgangspunten in nieuw beleid toegepast op nieuwe ontwikkelingen. Er zijn nog steeds stemmen die zich kanten tegen regulering van specifieke technologieën op detailniveau. In deze visie zou het beschermen van onze persoonsgegevens het beste lukken op grond van algemene beginselen die van toepassing zijn op *elke* technologie die persoonsgegevens verwerkt. Die beginselen zijn vervat in de OESO-Richtlijnen[74] en het Data Protection Verdrag van Straatsburg[75], de Europese Richtlijn 95/46/EG[76] en recent is daar nog een 'kaderbesluit' bijgekomen dat doorgifte van gegevens tussen justitie- en politiediensten regelt.[77] Over die beginselen van *data protection* wordt tamelijk ernstig gedaan. Amendering ervan zou dan in genoemde visie deze beginselen alleen maar verzwakken. Deze visie is tamelijk sterk ingeburgerd en verklaart onder meer waarom op Europees vlak en in vele landen geen wetgeving tot stand is gekomen over het gebruik van camera's. Steunend op mijn literatuur van Orwell ben ik van oordeel dat dit toch een erg dringend privacyprobleem is dat nadere regulering behoeft. Echter bots ik vaak op de zienswijze 'Waarom specifieke biometriewetgeving? De Wet bescherming persoonsgegevens is toch van toepassing!'

Mij heeft deze zienswijze nooit overtuigd. Het is juist dat bijna elke technologie ingrijpt op persoonsgegevens, maar de wijze waarop dit gebeurt, is telkens anders. Artikel 5 van Richtlijn 95/46/EG stelt als algemene regel dat lidstaten concreet moeten aangeven wat de voorwaarden zijn waaronder de verwerking van persoonsgegevens rechtmatig is. Bij gebrek aan specifieke wetgeving voor nieuwe technologische ontwikkelingen met duidelijke voorwaarden en begrenzingen

blijft het basisprincipe van de eerlijke en rechtmatige verwerking vaag en in onze ogen moeilijk te handhaven. Denk daarbij maar aan biometrische toepassingen die bestaan in een grote verscheidenheid en worden toegepast door uiteenlopende actoren. Hoe concretiseer je in dit licht algemene principes van gegevensbescherming?[78]

Het Europese gegevensbeschermingsrecht is het bijgevolg aan zichzelf verplicht om actief op te treden om de Europese mensenrechten te beschermen. Roepen dat internet onveilig is en dat iedereen er zich op eigen risico op beweegt, is geen optie. Het biometrieverhaal, en ook het al wat oudere cameraverhaal, zijn voorbeelden van technologie-ontwikkelingen voorbij de ontgroeningfase, waarin quasi alle landen doch ook de EU een steek hebben laten vallen.

Vooral de EU doet het echter op andere terreinen wél goed en leeft daarbij op naar de mensenrechtelijke verwachtingen. Meer en meer wordt voor internet de vergelijking gemaakt met de verkeerswetgeving.[79] Overheden reguleren actief vele aspecten van het verkeer: de wagens, de bestuurders, de bewegwijzering en afspraken, het wegdek en de verlichting. Eindbetrachting is een veilig verkeer en rechtbanken spreken overheden civielrechtelijk aan wanneer blijkt dat bijvoorbeeld bewegwijzering onvoldoende is of het wegdek erbarmelijk zodat ongelukken gebeuren. De keuze voor die vergelijking is volgens mij de juiste en geeft goed aan waar we naartoe moeten. Een veilige en betrouwbare, mensenrechtelijk vriendelijke informatiesamenleving met de overheid als eindverantwoordelijke die actief reguleert en verantwoordelijk maakt.

Een goed voorbeeld hiervan vormt het beleid dat Europa voert op het gebied van de bescherming van persoonsgegevens in de telecommunicatiesector. Het voorbeeld geeft ook aan dat Europa nooit geaarzeld heeft om de 'heilige beginselen van dataprotectie' te concretiseren en risico's en oplossingen bij naam te noemen.

2.6.2 TECHNOLOGIE ACTIEF TEGEMOET TREDEN: HET VOORBEELD VAN DE ePRIVACYRICHTLIJNEN

Nog geen twee jaar na de algemene richtlijn over de bescherming van persoonsgegevens werd deze aangevuld door de Europese richtlijn van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector.[80] Deze richtlijn ziet toe op de bescherming van de vertrouwelijkheid van persoonsgegevens die telecommunicatiediensten en telecommunicatienetwerken verwerken. De richtlijn was gericht op ISDN, omdat het ontbreken van harmonisatie op dit terrein de creatie van een interne markt op het terrein van de telecommunicatie zou verstoren.[81] Precies ISDN werd als een belangrijke voorwaarde voor de verdere ontwikkeling van de interne markt gezien. De richtlijn gaf aan de burger belangrijke waarborgen

(in de vorm van nieuwe expliciete subjectieve rechten) betreffende onder meer de aanleg van abonneelijsten, de opstelling van de gedetailleerde factuur en het doorschakelen van oproepen. De richtlijn bevatte talrijke andere nieuwe 'telecommunicatiewaarborgen'.

Primo werden de lidstaten door de richtlijn verplicht ervoor te zorgen dat het vertrouwelijke karakter van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten wordt gegarandeerd.[82] *Secundo* kwamen er de nieuwe rechten inzake nummeridentificatie en regels rond hijgtelefoons.[83] *Tertio* kwam er een verbod voor aanbieders van telecommunicatiediensten om abonneegegevens door te gegeven.[84] *Quarto* kwam er een verbod voor ongevraagde spam: automatische oproepsystemen met het oog op direct marketing mogen alleen gebruikt worden bij abonnees die daarmee vooraf hebben ingestemd.

De eerste *ePrivacy*-richtlijn was te zeer toegespitst op openbare telecommunicatienetwerken (ISDN ondersteund) en openbare digitale mobiele netwerken.[85] Internet werd niet bij name genoemd in de richtlijn, ook niet in de preambule. De richtlijn werd daarom in 2002 vervangen door een meer geactualiseerde versie[86], waarin internet centraal wordt gesteld en onder meer een regeling voor cookies, spyware, malware en virussen wordt uitgewerkt, zijnde allerlei vormen van technologieën waarmee derden informatie op de apparatuur van een gebruiker willen opslaan of toegang willen krijgen tot al opgeslagen informatie.

Opvallend aan het EU-verhaal is de continuïteit van dit proces van wetgevende actualisatie in functie van nieuwe ontwikkelingen. De ePrivacyrichtlijn uit 2002 werd immers in 2009 opnieuw geactualiseerd waarbij wederom rekening werd gehouden met de allernieuwste ontwikkelingen.[87] Deze actualisatie kadert goed in een aan de gang zijnde beweging van *compliance* naar *accountability* bij telecommunicatiebedrijven.[88] Allereerst legt de nieuwe ePrivacyrichtlijn een verplichting op aan telecombedrijven om inbreuken op de beveiliging van persoonsgegevens te melden (*data security breach notification*).[89] Het gaat in feite om een dubbele verplichting. Ten eerste is er de meldingsplicht aan de bevoegde overheid: bij *elke* beveiligingsinbreuk moeten de bevoegde instanties van nationale controle in kennis gesteld worden, ongeacht of er al dan niet een risico is voor de betrokken individuele gebruikers. De kennisgeving moet een omschrijving bevatten van de gevolgen van de inbreuk en van voorgestelde of getroffen maatregelen om de inbreuk aan te pakken. Ten tweede is er een meldingsplicht richting de individuele gebruikers en dit bij inbreuken met 'waarschijnlijk ongunstige gevolgen' voor hun persoonsgegevens en persoonlijke levenssfeer. Daarbij kan gedacht worden aan identiteitsdiefstal of -fraude, lichamelijke schade, ernstige vernedering en aantasting van de reputatie.[90] De telecommunicatiebedrijven zijn verplicht om een inventaris bij te houden van de inbreuken, waarin onder andere de feiten,

gevolgen en getroffen herstelmaatregelen bijgehouden worden. Ten tweede zijn er nieuwe verfijningen in de regels over cookies, spyware, malware en virussen. Een aantal onvolmaaktheden in de regeling hierover in de ePrivacyrichtlijn van 2002 zijn in de nieuwe regeling weggewerkt.[91] Een derde maatregel heeft betrekking op het verbod op spam dat teruggaat tot de eerste versie van de richtlijn uit 1997.

Omdat individuele personen meestal niet optreden tegen spammers (hetzij omdat ze de middelen niet hebben om een rechtszaak te beginnen, hetzij omdat de schade die ze lijden te gering is om een procedure op te starten), wordt het voortaan mogelijk voor natuurlijke personen en rechtspersonen die een rechtmatig belang hebben bij de bestrijding van spam, om zelf gerechtelijke stappen te nemen tegen spammers. Aanbieders van elektronische communicatiediensten die hun rechtmatige ondernemingsbelangen of de belangen van hun klanten willen beschermen, en consumentenverenigingen en vakbonden die de belangen van gespamde personen vertegenwoordigen, kunnen voortaan bijdragen aan veiliger internet! Daarnaast maakt de nieuwe richtlijn het ook mogelijk voor lidstaten om specifieke sancties uit te vaardigen voor aanbieders van elektronische communicatiediensten die door nalatigheid bijdragen tot spamming. Ten slotte (en ten vierde) bevat de nieuwe richtlijn ook aandacht voor sterkere handhavingsmechanismen. Zo moeten controleautoriteiten een bevoegdheid krijgen tot het bevelen van een staking van ePrivacy-inbreuken op een omzettingsbepaling van richtlijn 2002/58.

Al Ruggies bouwstenen komen mooi samen in dit hervormingspakket. De weg naar justitie wordt vereenvoudigd door betere kennisgeving van *security breaches* en door collectieve belangengroeperingen in te schakelen en wordt tevens aantrekkelijker gemaakt voor het slachtoffer door de extra mogelijkheid van het stakingsbevel. Naar de betrokken bedrijven toe is er sprake van aanscherping. Loutere compliance wordt aangescherpt en omgezet in heuse accountability. Voortaan moet er een actief beleid komen richting overheid en burger (notificaties), moet een veiliger eindproduct worden gegarandeerd (vrij van cookies, spyware, malware, virussen en spam) en is sanctionering mogelijk bij 'nalatig bijdragen'.

2.6.3 TECHNOLOGIE ACTIEF TEGEMOET TREDEN: HET VOORBEELD VAN RFID

Een tweede voorbeeld geven de op 12 mei 2009 verspreide aanbevelingen inzake *Rfid chips* (intelligente chips of radiotags) door de Europese Commissie (Europese Commissie 2009; De Boel 2009: 5). In het door de Commissie verspreide persbericht luidt het trots dat de Europese Commissie met de aanbeveling wil garanderen dat alle ontwerpers of exploitanten van Rfid-technologie *het individuele recht op privacy en gegevensbescherming zoals neergelegd in het op 14 december 2007 afgekondigde Handvest van de grondrechten van de Europese Unie* respecteren (Europese Commissie 2009a) (mijn cursivering).

De aanbevelingen moeten er onder meer voor zorgen dat:
- consumenten weten of bepaalde producten in winkels al dan niet met intelligente chips zijn uitgerust. Wanneer consumenten producten met intelligente chips kopen, moeten deze automatisch, onmiddellijk en kosteloos worden gedeactiveerd op het verkooppunt, tenzij de consument uitdrukkelijk verzoekt de chip operationeel te laten. Uitzonderingen kunnen worden toegestaan, bijvoorbeeld om kleinhandelaren niet nodeloos te belasten, op voorwaarde echter dat de gevolgen van de chip voor de privacy zijn nagegaan;
- bedrijven of overheidsdiensten die gebruikmaken van intelligente chips, consumenten duidelijke en eenvoudige informatie verschaffen, zodat deze kunnen inschatten of hun persoonlijke gegevens zullen worden gebruikt, alsook welke gegevens zullen worden gebruikt (bijv. naam, adres of geboortedatum) en waarvoor. Zij moeten ook zorgen voor een duidelijke etikettering ter identificatie van de elementen die de in intelligente chips opgeslagen informatie 'lezen', en een contactpunt instellen waar burgers terecht kunnen voor meer informatie;
- verenigingen en organisaties van kleinhandelaren de consument beter bewust maken van met intelligente chips uitgeruste producten via een gemeenschappelijk Europees merkteken waarmee de aanwezigheid van een intelligente chip wordt aangegeven;
- bedrijven en overheidsdiensten effectbeoordelingen inzake de bescherming van privacy en gegevens moeten uitvoeren alvorens gebruik te maken van intelligente chips. Ter waarborging van de veiligheid en de bescherming van persoonlijke gegevens moeten deze beoordelingen worden gecontroleerd door de nationale autoriteiten voor gegevensbescherming.

Ik wil hier minder de nadruk leggen op de wijze waarop Ruggies bouwstenen via de aanbevelingen gestapeld worden, maar meer op twee andere puntjes. Primo, verantwoordelijkheid nemen als overheid behoeft niet steeds op wetten te steunen. Zeker in een aanvangsfase kan een beroep op *soft law and governance* aangewezen zijn. Een proces van trial and error wordt aldus mogelijk. Secundo, en dit ligt in het verlengde van het voorgaande, is er het belang van de procesmatige aanpak van de Commissie. De Commissie vertrekt van het standpunt dat het recht op bescherming van persoonsgegevens en de betrokken richtlijnen van toepassing zijn en formuleert een aantal nieuwe ontbrekende rechten, zoals het recht op *chip-kill*. Het zwaartepunt van de regeling is echter procedureel; transparantie geven door een merkteken en effectenbeoordelingen uitvoeren (*privacy impact assessments*) die door de nationale gegevensautoriteiten moeten worden gecontroleerd. De hele totstandkoming van de aanbevelingen getuigt van procedurele zorg. In 2006 lanceerde de Commissie een publieke raadpleging over het onderwerp, op basis waarvan zij in maart 2007 bekendmaakte dat er bij de burgers een verwachting leeft van verdere actie op het gebied van de bescherming van privacy en gegevens. Dan volgde een reeks raadplegingen van belanghebbenden (leveranciers en

verwerkende bedrijven, normalisatie-instellingen, consumentenorganisaties, maatschappelijke organisaties en vakbonden) die uiteindelijk leidde tot de aanbevelingen van 2009. Dit proces creëert een breed draagvlak en geeft tevens een tijdig signaal aan de Europese industrie. Het proces stopt ook niet bij de aanbevelingen. De lidstaten krijgen twee jaar de tijd om de Commissie mee te delen welke stappen zij zullen nemen ter verwezenlijking van de doelstellingen van de aanbeveling. De Commissie zal binnen een termijn van drie jaar een verslag opstellen over de tenuitvoerlegging van de aanbeveling, met een analyse van de gevolgen voor bedrijven en overheidsdiensten die gebruikmaken van intelligente chips, alsook voor de burger.

2.6.4 SPELVERDELING VAN VERANTWOORDELIJKHEDEN: HET SPEL KEURIG AFGEHASPELD

Wat ons bezighoudt in dit rapport is hoe je de nieuwe situatie doorvertaalt naar het niveau van de lidstaten. Het EU-Handvest is alleen bindend voor de EU-instellingen en de handelingen gesteld door de lidstaten in uitvoering van EU-recht. Van mensenrechtenrechtspraak kan je steeds beweren dat het zaakgebonden is. Zo zijn er nog meer non-argumenten voor lidstaten om vooral geen eigen verantwoordelijkheid te nemen. Een veelgehoorde is dat *data protection* een door Brussel gedicteerde zaak is én dat je niet mag reguleren rond concrete technologieën, want dan zou je afbreuk doen aan de algemene beginselen van het gegevensbeschermingsrecht. Dat laatste is inderdaad een non-argument. Hiervoor beschreef ik dat Europees gewerkt wordt aan bijstelling van wetgeving betreffende het gebruik van persoonsgegevens. Richtlijn 97/66/EG werd vervangen door Richtlijn 2002/58/EG (richtlijn privacy en elektronische communicatie) en deze wordt op haar beurt opnieuw geactualiseerd door Richtlijn 2009/136/EG. Ook in het Rfid-dossier wordt geïnnoveerd door nieuwe rechten en nieuwe procedures. Het bestaan van algemene richtlijnen betreffende gegevensbeschermingsrecht vormt bijgevolg geen reden tot stilstand. Integendeel. Toch is dat nu net wat gebeurt in Nederland en andere landen. Zo hebben zowat alle landen hun gegevensbeschermingsautoriteiten rustig laten aanmodderen met biometrie, hoewel er grote onduidelijkheid bestaat over bepaalde biometrieaanwendingen, onder meer over de betekenis voor deze technologie van sturende beginselen zoals proportionaliteit en doelbinding (Kindt 2007: 166-170; Liu 2009; De Hert & Sprokkereef 2009).

Een ander mooi voorbeeld geeft de problematiek van *ambient intelligence.* In de Nederlandse Kamer legt een regeringslid een brief voor over de gevolgen voor persoonsgegevens van ontwikkelingen betreffende ambient intelligence.[92] Het regeringslid stelt in zijn verklaring een expertrapport voor dat door hem is uitgelokt. De experts hebben hun werk op geloofwaardige wijze gedaan (en een boek geraadpleegd waaraan ik meegewerkt heb). Breeduit wordt de conclusie omarmd die luidt dat er voorlopig niets moet veranderen aan de bestaande wetten. De

kleine reserve van de experts "dat de technologieën en de toepassing nog volop in ontwikkeling zijn" en dat "in de toekomst aanvullende technologische, juridische en organisatorische mechanismen nodig kunnen zijn" wordt daarbij meegenomen. Dan volgt een overzicht van wat beleid dat deze regering desondanks heeft ontwikkeld. Hoewel "het bedrijfsleven in eerste instantie verantwoordelijk voor een adequate bescherming van de persoonsgegevens is", wordt de nood onderstreept om de consument goed voor te lichten. In een duidelijk voor juristen bedoeld paragraafje 'Regelgeving' krijgt de expertgroep twee zachte tikken op de vingers. De expertgroep had namelijk toch iets te expliciet gesteld dat de Wbp en de Telecommunicatiewet mede door hun technologieneutrale vormgeving in de toekomst mogelijk onvoldoende zijn toegerust om het hoofd te bieden aan een groot aantal zeer uiteenlopende ontwikkelingen. Het regeringslid is ferm op dit punt: "Deze ontwikkelingen zijn op dit ogenblik nog zodanig onzeker dat een uitspraak over de noodzaak tot wijziging van de regelgeving nog niet aan de orde is." Bovendien zijn genoemde wetten gevolg van EU-richtlijnen en het is op dat niveau dat de eerste stappen moeten worden genomen. In dat standpunt speelt een achtergrondstudie van het CBP van oktober 2006 over Rfid mee.[93] In die studie concludeerde het CBP dat ten aanzien van Rfid de Wbp in algemene zin voldoet voor de beheersing van de risico's die met deze technologie samenhangen. "Het kabinet ziet de achtergrondstudie van het CBP als een bevestiging van de hierboven weergegeven conclusie." Alle trefwoorden voor keurig beleid zijn er: 'de burger moet geïnstrueerd worden', 'de expert', 'de rol van Europa', 'de taak van de ondernemingen als eerste verantwoordelijke' en 'het CBP' komen aan bod.

Een eerder 'driepuntenplan' van OPTA voor veiliger internet werd niet zo lang geleden met dezelfde trefwoorden afgeschoten: we gaan vooral niet meer doen dan te rekenen op wat geldelijk ondersteunde zelfregulering (Heemskerk 2008).[94] OPTA had zich voor dit plan (te komen tot veiliger internet) gesteund op artikel 11.3 van de Telecommunicatiewet. Deze bepaling verplicht internet service providers en andere aanbieders van openbare telecommunicatienetwerken om maatregelen te treffen voor een veilige internetinfrastructuur en om internetgebruikers voor te lichten over internetrisico's. Begin 2008 greep OPTA deze wat vaag gehouden zorgplichten[95] aan om een driepuntenplan voor te stellen op weg naar veiliger internet: ten eerste de plicht voor ISP's om hun abonnees te informeren over veiligheidsrisico's (informatieplicht), ten tweede het ontwikkelen van een keurmerk door ISP's voor hun eigen branche en ten derde de aanpak van het probleem van zombiecomputers.[96] Zoals gezegd werd het plan politiek afgeschoten. Eerder was het al 'weggeduwd' door de telecommunicatieaanbieders die ondanks protesten van de Consumentenbond de eindverantwoordelijkheid voor veilig internet bij de eindgebruiker (blijven) leggen (Doorenbosch 2007: 3).

Hiervoor werd in dit essay reeds kort gesteld dat het verhaal van de globalisering en van complexe technologische ontwikkelingen vaak door beleidsmensen strate-

gisch wordt uitgespeeld om verantwoordelijkheden weg te schuiven. Zo wordt een situatie bereikt die in de voorbereidende notitie *Beginsel Accountability* 'accountability zonder de sanctie van verantwoordelijkheid' wordt genoemd.[97] In voorliggend mensenrechtelijk essay wordt een ander verhaal naar voren geschoven, met andere trefwoorden. Het is geen verhaal geworden over zelfregulering, expertstudies, te helpen burgers en de rol van Brussel. Integendeel, het werd een verhaal over 'verantwoordelijkheden van overheden voor veilig internet', 'verantwoordelijkheden van overheden voor effectief toezicht op de handhaving van de beginselen van de Wbp' en 'bedrijven met aansprakelijkheidsplichten'.

Een echte politiek rond technologie wordt tenslotte pas mogelijk wanneer het drogverhaal Europa tot een einde wordt gebracht. Moderne Europese politici hebben een gave ontwikkeld om in eigen land te zeggen dat ze niets mogen van Brussel, terwijl ze in Brussel net het omgekeerde doen, hoewel ze daar, zeker op het terrein van de veiligheid, door een zwakke positie van het Europees Hof en het Europees Parlement, alles te zeggen hebben.[98] Vergelijkt men het Europese beleid inzake Rfid met het Nederlandse beleid, dan valt op hoe onbetekenend dit laatste is geweest: geen publiek debat, geen consultatie, geen agendapunt (Knapen 2007). Alsof de Nederlandse burger en de Nederlandse politieke agenda ongeschikt zijn voor een debat. Wordt er nog aan politiek gedaan in dit land? Die politiek is perfect mogelijk. Rfid creëert eigen specifieke privacybedreigingen en er zijn veel beleidskeuzen die sommige producenten en bedrijven vrezen, maar die in het belang van die burger (met zijn mensenrechten) een politiek debat behoeven (Lockton & Rosenberg 2006).

Het voorgaande mensenrechtelijk perspectief op verantwoordelijkheden in de informatiemaatschappij wordt in de nu volgende korte delen verder uitgewerkt. De overheid is bijgevolg eindverantwoordelijk en kan bij het dragen van die verantwoordelijkheid een keuze maken hetzij voor een jungle model voor burgers dan wel voor een compliance model of een accountability model voor bedrijven. Het feit dat er keuzevrijheid is, draagt bij tot de idee van verantwoordelijkheidsdistributie. Het overzicht van positieve plichten voortvloeiend uit het EVRM heeft aangetoond dat een accountabilitymodel het meest voor de hand ligt in een mensenrechtenperspectief. Eveneens toont de gemaakte analyse aan dat er een actief wetgevend en toezichtbeleid vooraf nodig is. De idee van positieve plichten verzet zich tegen een informatiemaatschappij waarbij aan het concreet omgaan met persoonsgegevens geen beschermende regels verbonden zijn.

Tot dusver hebben we veel aandacht besteed aan rechten en beginselen betreffende de bescherming van de persoonlijke levenssfeer. De leer van de positieve plichten is echter ruimer en wordt gekoppeld aan alle rechten uit het EVRM. De systeemverantwoordelijkheid van de overheid en de behoefte aan efficiënte distributie van verantwoordelijkheden is derhalve ruimer. In wat volgt, kijken we naar de taken van de overheid op het vlak van identiteitsfraude en media pluralisme.

2.7 VERANTWOORDELIJKHEDEN BETREFFENDE IDENTITEITSFRAUDE

2.7.1 EEN NIET ONDERGEBRACHT VERANTWOORDELIJKHEIDSPROBLEEM

Identiteitsfraude is het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee (willen) begaan van een wederrechtelijke gedraging (De Vries et al. 2007: 12). Geslaagde identiteitsfraude op een zwakke plek ergens in een bepaalde keten, aldus Grijpink in 2006, verspreidt zich ongemerkt naar andere ketens en processen. "Als men op iemands rijbewijs kan meeliften bij het aangaan van een nieuwe arbeidsverhouding, vindt belastingheffing bij het slachtoffer plaats; bij het te naam stellen van een kenteken kan men heffingen, boetes en incasso's ontlopen" (Grijpink 2006: 40).

In de voorbereidende notitie *Beginsel Accountability* wordt even stilgestaan bij het fenomeen van de identiteitsfraude en dit naar aanleiding van het streven van het openbaar bestuur naar keteninformatisering (coördinatie van digitale informatiestromen en uitwisseling van gegevens tussen overheidsinformatiediensten). Het is een ontwikkeling die het interne beheer van de overheid overzichtelijker maakt en grote efficiencyvoordelen tot gevolg heeft die ook het gemak van de burger kunnen dienen. Nadeel is dat de burger die slachtoffer is van identiteitsfraude extra kwetsbaar is en het 'uitermate moeilijk' heeft 'om de ketens weer recht te zetten'. Kort gezegd weet de burger eenvoudig niet waar hij moet aankloppen om de fraude aan te klagen en recht te zetten en weten de in één frontoffice gegroepeerde overheden het vaak ook niet (Koedooder 2009).[99] Het probleem van de verantwoordelijkheid is door de netwerkende overheden nergens ondergebracht.

Het probleem zit breder aldus Corien Prins in het *Nederlands Juristenblad*. Zeker op het vlak van financiële identiteitsfraude is er geen sprake van een strategisch beleid van de overheid en lijkt ook de Nederlandse Vereniging van Banken niet bijzonder actief (Prins 2010: 537). De opmerking geldt ook meer algemeen. Er is, aldus Prins, een Meldpunt Identiteitsfraude, doch dit is nooit expliciet onder de aandacht van burgers gebracht en in tegenstelling tot de VS heeft de overheid tot op heden niets gedaan aan publiekscampagnes rondom dit fenomeen. Het politieregistratiesysteem voor aangiftes van identiteitsfraude bestaat niet of nauwelijks en verantwoordelijkheden worden doorgeschoven van de politie naar de banken.[100] Prins eindigt haar betoog met de vaststelling dat er beleid nodig is, minstens om te kijken hoe groot het probleem is.[101] Dan kan de vraag worden beantwoord in hoeverre en op welke wijze de overheid de verantwoordelijkheid naar zich toe moet trekken voor het reduceren van de onzekerheid over aard en omvang van identiteitsfraude. Op die vragen kom ik terug in een volgende para-

graaf. Interessant is dat Prins er geen twijfel over laat bestaan dat er een grote rol bestaat voor de overheid, minstens als regisseur der verantwoordelijkheden, en een heleboel praktische beleidsstappen suggereert om de strijd aan te binden tegen identiteitsfraude.[102] Een maatregel bestaat in een zelfstandige strafbaarstelling van identiteitsdiefstal los van bestaande delicten zoals deze vervat in artikel 321 Sr (fraude met reisdocumenten), 326 Sr (oplichting) en de artikelen 139c en 139e Sr (kopiëren van computergegevens).

Ook Michel van Eeten, nochtans geen voorstander van overdreven overheidsinterventie, laat goed zien dat er zeker op het vlak van wetgeving actie mogelijk is. Er is tot nader order geen extern toezicht op de claim van banken dat ze schade van financiële identiteitsfraude en fraude met online betalingsverkeer vergoeden. De regelgeving dwingt dit niet af en gebruikers hebben niet of nauwelijks mogelijkheden om banken aan die toezegging te houden (Van Eeten 2011).[103] In de praktijk besluit de bank zelf of ze het redelijk vindt om schade te vergoeden. Juridisch verweer tegen een dergelijke beslissing is lastig, aldus Van Eeten, en kosten van de rechtsgang zijn hoog: "men kan opdraaien voor de proceskosten en de rechters hebben zich vaak onkritisch opgesteld tegenover de technische beweringen van de banken."

2.7.2 IDENTITEIT WORDT BESCHERMD VIA ARTIKEL 8 EVRM

Komen we terug op de vraag in hoeverre zorg voor bescherming van onze identiteit een overheidstaak is. In het belangrijke arrest *Reklos & Davourlis t. Griekenland* van 2009 vat het Hof haar recente rechtspraak op dit punt samen. Ik citeer de overweging in het Engels: "In general terms, the Court observes that according to its case-law 'private life' is a broad concept not susceptible to exhaustive definition. The notion encompasses the right to identity (…) and the right to personal development, whether in terms of personality (…) or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees (…)."[104]
Het Hof gaat er bijgevolg van uit dat er een recht bestaat op eigen identiteit, net zoals er een recht bestaat op zelfontplooiing, als deelaspecten van het recht op privacy, en dat beide deelrechten kunnen begrepen worden in termen van persoonlijkheid of in termen van persoonlijke autonomie. Aan deze rechten komt bescherming toe via de leer van de negatieve en positieve plichten.

2.7.3 DE LEER VAN DE POSITIEVE PLICHTEN TOEGEPAST OP IDENTITEITSFRAUDE: K.U. TEGEN FINLAND (2008)

Hiervoor hebben we gezien dat de leer van de positieve plichten met zich meebrengt dat het omgaan met persoonsgegevens op een beveiligde wijze moet gebeuren. In het reeds besproken arrest *I. t. Finland* gewezen op 17 juli 2008

maakte het Europees Hof schoon schip met gepruttel van de Finse overheid dat het betrokken ziekenhuis gedaan had wat het kon op het vlak van beveiliging (*supra*). Wanneer banken diensten aanbieden maar niet zorgen voor adequate beveiliging en de overheid laat betijen, dan lijkt het er sterk op dat de norm van Straatsburg niet gehaald wordt. Respect voor positieve plichten kan met zich meebrengen dat staten nieuwe strafbaarstellingen invoeren of bestaande strafbaarstellingen verduidelijken. Het pleidooi van Corien Prins tot een specifieke strafbaarstelling kan in dit licht worden begrepen.

Michel van Eeten toont in zijn essay aan dat veiligheid in feite een resultante is van allerlei gemaakte keuzen. Het is zeker geen goed dat ten koste van alles wordt nagestreefd. Een van de belangen die haaks kan staan op veiligheid is de keuze voor gebruiksvriendelijkheid. Een ander belang dat zou kunnen spelen is het belang van burgers, zijnde andere burgers dan het slachtoffer bij anonimiteit en bescherming van het privéleven. Het is hier de plaats in te gaan op het Europese arrest *K.U. tegen Finland* van 2 december 2008.[105] Het arrest toont aan dat als gevolg van een mensenrechtelijke systeemverantwoordelijkheid soms maatregelen nodig zijn die inperkingen op vrijheden verlangen.

Op 15 maart 1999 plaatst een onbekende een advertentie op een Finse *dating site* op internet, in naam van K.U. en zonder zijn medeweten hiervan. K.U. is op het ogenblik van deze feiten twaalf jaar oud. De advertentie vermeldt leeftijd en lichaamskarakteristieken, alsook een foto van K.U. via een link naar zijn webpagina. Bovendien maakt de advertentie ook melding van het telefoonnummer van K.U., dat correct wordt weergegeven op één cijfer na. Volgens de advertentie zou K.U. op zoek zijn naar een jongen van dezelfde leeftijd of ouder "om hem de weg te wijzen". K.U. komt op de hoogte van deze advertentie wanneer hij, als reactie op deze advertentie, een e-mail ontvangt met een voorstel van een man om hem te ontmoeten. De vader van K.U. vraagt aan de internet service provider (ISP) de identiteit te achterhalen van de persoon die de advertentie heeft geplaatst. De service provider weigert echter de identiteit van de houder van het IP-adres te onthullen en beroept zich op de geldende privacywetgeving. De politie vraagt vervolgens aan de rechter om aan het bedrijf een bevel op te leggen de identiteit mede te delen van degene die de informatie op de dating site had geplaatst, maar de rechtbank weigerde op dit verzoek in te gaan, omdat de wetgeving niet toelaat voor laster een dergelijk bevel uit te schrijven.[106] Een vervolging van de ISP voor de feiten was in beginsel ook mogelijk wegens inbreuk op de Finse Wet bescherming persoonsgegevens. Deze verplicht aan internet service providers om bij het publiceren via internet van gevoelige informatie de identiteit na te trekken van de afzender en om te verifiëren of de betrokkene wel instemde met de openbaarmaking van de privacygevoelige informatie. Echter, de feiten waren op dit punt verjaard.

De zaak komt voor het Europees Hof. K.U. meent dat er een schending heeft plaatsgevonden van de artikelen 8 en 13 EVRM in zoverre hij niet beschikte over de mogelijkheid om een genoegdoening te krijgen wegens een schending van zijn privéleven. Immers, het was onmogelijk om de identiteit te achterhalen van de persoon die de advertentie had geplaatst. De uitbetaling van een civiele schadevergoeding gebeurde niet door de persoon die de inbreuk heeft gepleegd en is daarom een ineffectieve remedie.

Het Hof begint zijn analyse met een bespreking van een aantal relevante internationale instrumenten, zowel bindend als niet-bindend, betreffende computergerelateerde misdrijven.[107] Vervolgens verklaart het Artikel 8 EVRM van toepassing. Ook al geldt op nationaal vlak eerder de kwalificatie laster, het Hof onderzoekt de inbreuk liever vanuit de noties van een mogelijke bedreiging voor het fysisch en psychisch welzijn van K.U., gelet op zijn jonge leeftijd en kwetsbare situatie. Deze zaak valt onder de noemer van de positieve verplichtingen van de staat. Zware schendingen van het privéleven vereisen strafrechtelijk efficiënte voorzieningen. Het Hof wijst erop dat we hier te maken hebben met het kwetsbaar opstellen van een minderjarige voor toenaderingen door pedofielen. Het strafbaar stellen van een misdrijf volstaat echter niet. In casu bestond de mogelijkheid om een procedure aan te spannen wegens laster, maar zolang de dader niet kan worden geïdentificeerd, heeft de strafbaarstelling slechts een beperkt afschrikkend effect. Waar het fysisch en psychisch welzijn van een kind in gevaar komt, is dit des te erger. Het feit dat K.U. genoegdoening kon krijgen vanwege een derde partij, namelijk de service provider, volstaat niet.[108] Gegeven de omstandigheden vereisen de openbare belangen en de bescherming van het kind dat van de eigenlijke dader een financiële schadevergoeding kan worden verkregen. Het Hof herhaalt hier echter dat dit geen afbreuk doet aan het feit dat positieve verplichtingen geen onevenredige last mogen leggen op de overheid en dat steeds moet worden toegezien op het respect van het recht op een eerlijk proces. De artikelen 8 en 10 EVRM bevatten ook deze waarborgen, en kunnen door de overtreders zelf aangehaald worden in hun verdediging. Het Hof is ook niet ongevoelig voor de sociale omstandigheden die aan de basis kunnen liggen van een tekortkomende wetgeving.

In casu meent het Hof echter dat, net omwille van het anonieme karakter van internet, de overheid zelfs al in 1999 had moeten voorzien dat internet voor misdrijfdoeleinden zou kunnen worden gebruikt. Ook seksueel misbruik van kinderen was al een welgekend probleem.[109] Er kan daarom niet gezegd worden dat de overheid zich niet bewust was van de noodzaak van een systeem ter bescherming tegen kindermisbruik via internet. Praktische en efficiënte beschermingsmaatregelen dienden er daarom toe om de identiteit van de betrokkene te achterhalen. Een efficiënt onderzoek was niet mogelijk omwille van de overmacht van de vertrouwelijkheid[110], terwijl die niet absoluut is en naargelang de omstandigheden zelfs moet buigen voor de behoefte aan ordehandhaving. Met een beroep op de

expressievrijheid en het daaraan gerelateerde recht op anonimiteit kan men zich immers niet onttrekken aan bepaalde verantwoordelijkheden: "Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others."[111] Er is daarom een schending van het Verdrag, in het bijzonder van artikel 8 EVRM.[112]

2.7.4 GEVOLGTREKKINGEN VOOR DE VERANTWOORDELIJKHEID BIJ IDENTITEITSFRAUDE

Het arrest *K.U. t. Finland* is meer dan alleen een arrest over identiteitsfraude. De klemtoon ligt op de bescherming van kinderen tegen pedofielen. Toch is de zaak gestart met een vorm van identiteitsfraude: iemand gaat aan de haal met K.U.'s gegevens en laat de digitale identiteit van K.U. een rol spelen die hij nooit heeft willen spelen. Het Europees Hof erkent een recht op bescherming van identiteit (*supra*) en laat er geen twijfel over bestaan dat een rechtssysteem effectief moet optreden tegen ernstige vormen van identiteitsfraude. Of daar in zijn algemeenheid strafrecht bij gebruikt moet worden kan niet worden gesteld (*infra*).

In naam van de strijd tegen de identiteitsfraude besliste toenmalig minister Hirsch Ballin (Ministerie van Justitie) om meer vingerafdrukken en foto's te laten nemen van verdachten en veroordeelden. De beslissing volgde op onderzoeken waaruit gebleken is dat politie en justitie niet zelden bewust worden misleid door mensen die zich uitgeven voor een ander.[113] Met de nieuwe wet worden personen voortaan direct na hun aanhouding verplicht om vingerafdrukken af te staan en worden er foto's van deze verdachten gemaakt als er twijfels zijn over hun identiteit. Verder worden van alle gedetineerden pal vóór de opsluiting in een inrichting foto's en vingerafdrukken genomen en vastgelegd. Tot slot komt er een zogeheten strafrechtsketennummer (SKN) als persoonsnummer voor de gehele strafrechtsketen.

Nog in 2009 bood de minister excuses én compensatie aan een zakenman aan die als gevolg van identiteitsfraude jarenlang ten onrechte als drugscrimineel in systemen van de overheid geregistreerd stond. Uit de voorgaande paragrafen blijkt echter dat de Nederlandse overheid meer zal moeten doen op het vlak van de bestrijding van identiteitsfraude, zowel in de gevallen waarin het zelf betrokken partij is, als in gevallen waarin burgers tegenover burgers en bedrijven staan.

Uit de leer van de positieve plichten kon vroeger al worden afgeleid dat op staten een positieve plicht rust tot effectieve gebruikmaking van strafrecht. Dit ter bescherming van kinderen en kwetsbare groepen tegen zware misdrijven, onder

meer in de sfeer van de seksuele delicten. Uit het arrest *K.U. t. Finland* kan ook worden afgeleid dat er (ook) een positieve verplichting bestaat tot gebruikmaking van het strafrecht bij de bescherming van kinderen tegen het zonder hun toestemming op internet plaatsen van seksueel getinte contactadvertenties over hen. Opvallend is de nadruk op het gegeven dat K.U. een kind is (Groothuis 2009: 288). Het is bijgevolg oppassen met het veralgemenen van de boodschap (en eveneens met het radicaal ondergraven van het privacyrecht van kinderen) (Dowty 2008).

Wel kan worden afgeleid dat het Hof aan staten de duidelijke boodschap geeft dat staten een positieve verplichting hebben om kinderen te beschermen tegen misbruik door pedofielen op internet. Het argument dat internet nog maar enkele jaren oud is, vormt geen geldig excuus voor het niet ter hand nemen van de systeemverantwoordelijkheid. Opnieuw kan nauwelijks gesproken worden van vaagheid in hoofde van de Europese rechters. De zorgplicht voor staten wordt vrij precies gekaderd:

– er moet bij het creëren van maatregelen ter bescherming van kinderen naar een evenwicht gezocht worden met het belang van de vrije meningsuiting en het privacyrecht van internetgebruikers;
– een louter systeem van schadevergoeding bij derden, in casu de providers, is onvoldoende; de persoon die de gegevens heeft geplaatst, moet kunnen worden vervolgd.

Het wordt mijns inziens tijd om de fundamentele keuzen gemaakt in Richtlijn 2000/31/EG (de e-commercerichtlijn) betreffende de immuniteiten voor *access* en *hosting providers* (*supra*) opnieuw te bekijken. Het verstoort een verantwoordelijkheidsdistributie die alle op het spel staande belangen verzoent en alle betrokken actoren, inclusief de ISP's, hun deel van de positieve mensenrechtenverplichtingen toewijst. In de richtlijn staan geen aanvaardbare invullingen van de *state duty to protect*, de *corporate responsibility to respect* en de idee van *access to remedy*, met als gevolg dat burgers geen verweer hebben tegen bepaalde misbruiken. Bij die broodnodige reflectie, die ervoor kan zorgen dat we niet in het andere uiterste vervallen waar geen privacy voor internetgebruikers en kinderen wordt erkend, moet het systeem herdacht worden vanuit de mensenrechtelijke positie van de burger in zijn vele verschijningsvormen en identiteiten. Storende details die een burger ontmoedigen om op te komen voor zijn geschonden belangen moeten weggenomen worden. Ik denk daarbij aan de bevinding van het Europees Hof van Justitie dat artikel 5 van de e-commercerichtlijn (service providers zijn verplicht contactgegevens te verschaffen aan consumenten met het oog op directe en effectieve communicatie) *niet* verplicht om telefoonnummers op sites te plaatsen waardoor telefonisch contact tussen provider en consument mogelijk wordt.[114] Deze lectuur naar de letter van de wet kan mijns inziens vanuit consumentenperspectief niet overtuigen, een visie die ook gedragen wordt door de Nederlandse Consumentenautoriteit (De Jong & Erents 2009: 170 en 173). De

letter van de wet zal dan ook verscherpt moeten worden om de idee van vlotte access to remedy optimaal te realiseren.

2.8 VERANTWOORDELIJKHEDEN OP HET GEBIED VAN INFORMATIE OVER MAATSCHAPPELIJKE AANGELEGENHEDEN

2.8.1 KEUZEVRIJHEID ALS SLEUTEL TOT VERGETEN

In zijn boek *Republic 2.0* (uitgegeven in 2000, heruitgegeven in 2007) kijkt Cass Sunstein naar de gevaren voor de democratie in het digitale tijdperk (Sunstein 2001). In de inleiding tot dat boek geeft deze eminente jurist en huidig topadviseur van Obama aan dat niet privacy, doch wel mediapluralisme en toegang tot relevante informatie dé uitdaging vormt van de toekomst (Sunstein 2001: 16-17). Het punt van Sunstein over privacy is goed geplaatst. Op een belangrijke conferentie gehouden te Brussel op 20 mei 2009 (die trouwens helemaal op internet te zien is)[115] kwam een topman van Google het verblufte publiek via een knappe beeldshow tonen dat de moderne gebruiker bij Google alles naar de eigen hand kan zetten. Het bedrijf maakt namelijk alles openbaar en de gebruiker kan zelfs kijken welk profiel Google op de gebruiker kleeft en desnoods het profiel aanpassen ('intellectueel' in plaats van 'sportliefhebber', enz.). De markt is klaar voor de kiezende burger. Als privacy samenvalt met keuze, dan zal de teloorgang ervan niet te wijten zijn aan moderne innovatieve bedrijven.

Deze voor mij zeer gemengde ervaring met Google deed me terugdenken aan een mooi essay van Finkielkraut 'Bestaat er herinneringsplicht?' uit een van zijn soms wat slordig gecomponeerde boekjes (Finkielkraut 2001: 1-25). Het antwoord op de vraag of er een herinneringsplicht is, luidt 'zeker'. Moderne democratieën hebben de boodschap goed begrepen. Toch ontwaart de denker vele mechanismen om het juiste herinneren te perverteren of uit te schakelen. Cultuur en technologie zijn twee van die mechanismen. Finkielkraut ontwaart in onze digitale samenleving een grote behoefte aan affirmatie van het ik en de eigen identiteit (keuzen!). Er is geen streven naar de opbouw van een cultuur gewijd aan de verheldering van het zijn; er is alleen een cultuur die (slechts) gewijd is aan de ontplooiing en affirmatie van het ik. Internet, aldus Finkielkraut zonder te veel bewijsmateriaal, is een vergeetmachine. Vergeten is gehoorzamen en slaafs meedoen met de algemene trend.

In het tweede hoofdstuk 'Het oproepen van schimmen: Kosovo' gaat Finkielkraut uitdrukkelijk in op de rol van technologie in dit vergeten en niet actief herinneren. De moderne beeld- en informatiemedia met hun privilegiëring van het beeld zijn slechte media om het vergeten tegen te gaan, omdat ze geen context scheppen. Context heeft te maken met het verleden, en televisie of internetbeelden tonen bijna uitsluitend het hier en nu. Het beeld haalt zijn materiaal uit het zichtbare en gaat voorbij aan het onzichtbare. "Het hoeft niet te worden vervalst om tenden-

tieus te zijn. Niet alleen tilt het beeld slechts fragmenten uit de toonbare werkelijkheid, het schuift ook het niet-toonbare deel van de werkelijkheid terzijde. Van het heden, dat het niet in zijn totaliteit kan vatten, doet het bovendien de historische diepte verdwijnen. Op de vragen 'waarom' en 'sinds wanneer' bestaat geen voor het blote oog toegankelijk antwoord. De menselijke ervaring wordt, onder het bewind van het visuele, als het ware beroofd van haar narratieve samenhang. De feiten worden losgekoppeld van de herinnering eraan. "De vreemde indruk die de eentonigheid van het nieuwe maakt, dooft in ons de liefde voor en zelfs de behoefte aan de betekenis," zoals Valéry in zijn tijd al voorvoelde. "We zijn zo in de ban van wat we voor ons zien, zo gefascineerd door wat live wordt uitgezonden, dat we vergeten dat de werkelijkheid niet alleen uit tastbare en rechtstreeks waarneembare dingen bestaat. De actualiteit wordt haar eigen context, het medium is de omgeving en wat continuïteit zou moeten zijn is een ononderbroken stroom waarin niets duurzaam en blijvend is" (Finkielkraut 2001: 28-29).[116]

2.8.2 DE ONGELOVIGE REIZIGER DOOR CYBERSPACE

Op het einde van dit tweede essay gaat Finkielkraut in op de koppeling tussen nieuwe beeldmedia en de keuzevrijheid van de internetgebruiker en een hedendaagse scepsis ten aanzien van autoriteit en waarheid (mediakritiek).[117] De relatie tot de wereld wordt geprivatiseerd door naar eigen keuze het informatiemenu op het net samen te stellen. Elke gebeurtenis wordt onder verdenking gesteld, zelfs beelden van het nu. "De ongelovige reiziger door cyberspace, te mediadeskundig om zich in de boot te laten nemen, te helderziend om zijn ogen te geloven, zal alleen die feiten erkennen die bij zijn geloof passen" (Finkielkraut 2001: 39). Hij vervolgt: "De werkelijkheidsgegevens zullen niet meer doordringen tot het denken, en wanneer in het ongrijpbare universum van beeld en elektronische tekst alle wegen mogelijk zullen zijn en alle meningen toegestaan, zullen alle ideeën voortvloeien uit onweerlegbare premissen. Eenieder zal zijn gril of zijn hobby hebben, de individuen zullen groepen berijders van stokpaardjes gaan vormen, en, schitterende mediasociologische paradox, in het tijdperk van de wereldwijde communicatie zal het vlechtwerk van hermetisch gesloten logica's in de plaats komen van de dialoog tussen mensen" (Finkielkraut 2001: 39).

Ook bij Sunstein in zijn genoemd werk *Republic 2.0* gaat de zorg uit naar mediapluralisme en het behoud van het democratisch debat. Ons ongebreideld vermogen tot het maken van keuzen (*click and browse*) en het filteren van informatie brengen ons veraf van de ideale democratische gespreksruimte.

In de literatuur wordt de boodschap van Finkielkraut, Sunstein en anderen[118] onder de noemer gebracht van de homofiliethesis ('internet zorgt dat we alleen zoeken naar het eigen gelijk door de keuzeopties'). Naar de gefundeerdheid van die these verloopt op meerdere plaatsen empirisch onderzoek en de focus is daar-

bij niet zelden op het gebruik van internet door religieuze en politieke fundamentalisten. Sunstein zelf gaf het startschot voor dat soort mediaonderzoek door in zijn boek resultaten te verwerken van een zelf verricht onderzoek naar 'overgepolariseerde' blogs. Onder meer blijkt daaruit dat uiterst rechts alleen maar naar zichzelf verwijst in discussies. Als er al een verwijzing is naar de tegenstander, dan is dit steeds smalend zonder een eerlijke discussie van de argumenten (Sunstein: 46-96). Dit soort groepsdiscussies, aldus Sunstein, leidt tot groepspolarisatie (Sunstein 2001: 80).

Leen d'Haenens komt in haar onderzoek naar internetgebruik door jonge migranten tot gemengde conclusies, maar eindigt haar analyse met een pleidooi gericht aan de overheid om het te vaak op oude media gerichte mediabeleid om te buigen tot een beleid naar deze nieuwe media en er bijvoorbeeld voor te zorgen dat 'nieuwe Nederlanders' niet steeds naar informatiekanalen uit het land van herkomst moeten gaan (D'Haenens 2003).

Sunstein bepleit een radicale politiek om mensen te confronteren met materiaal dat ze zelf niet zouden hebben geselecteerd en een politiek om mensen bepaalde gezamenlijke ervaringen te laten doorlopen (Sunstein 2001: 190-211). Enclavediscussies en consumentensoevereiniteit op het vlak van nieuwsgaring moeten doorbroken worden (Sunstein 2001: 80) via een serie van democratische instrumenten steunend enerzijds op een systeem van zelfregulering door content providers en anderzijds op overheidssystemen van *must carry* en subsidies. Opvallend is dat Sunstein geen betoog houdt gericht op het promoten van participatie aan de democratie via nieuwe media.[119] Al zijn aandacht is erop gericht ons te confronteren met het onverwachte en om te verhinderen datgene te doen wat we allen zo automatisch doen, filteren en wegklikken. Hij schuwt daarbij geen enkel taboe en toont onder meer aan dat het Amerikaanse grondwettelijk recht wel degelijk positieve rechten kent om mensenrechten te realiseren, wat ook het dominante Amerikaanse geloof in (uitsluitend) negatieve mensenrechtenverplichtingen mag zijn.[120] Ook breekt hij een lans voor de *fairness doctrine*, een door de *Supreme Court* afgewezen theorie die stelt dat media in hun verslaggeving een stem moeten geven aan de tegenpartij. Een variant hierop is een *disclosure*-plicht, een plicht om informatie te geven aan het publiek ('roken schaadt de gezondheid') toegepast op de media ('dit programma bericht over zaken van maatschappelijk belang'). Als alle zenders hun programmatie via dit perspectief moeten doorlichten krijg je hefbomen om verbeteringen te eisen (Sunstein 2001: 195-198).

Sunstein gaat in zijn werk vaak op zoek naar ervaringen en mechanismen die een digitale variant vormen op wat vroeger bestond: tijdens onze fysieke verplaatsingen worden we geconfronteerd met spandoeken, reclame en aanplakborden én met andere mensen die op straat op een of andere wijze een boodschap brengen; tijdens onze krantenlectuur en het televisiekijken (vroeger toen het zappen nog

niet bestond) kwamen we in contact met opvattingen van anderen.[121] Dit soort ervaringen is waardevol en moet worden gereconstrueerd aldus Sunstein, die met zijn voorstellen felle kritieken van zowel progressieven als conservatieven uitlokte met vragen over de beperking van de vrijheid van meningsuiting.[122]

2.8.3 POSITIEVE PLICHTEN TOT MEDIAPLURALISME OP GROND VAN ARTIKEL 10 EVRM EN ARTIKEL 11 HANDVEST

De aandacht voor de homofiliethesis kan gekaderd worden in een bredere zorg voor mediapluralisme. Het inzicht dat eenzijdige nieuwsgaring het democratische debat ondermijnt en staten berooft van vitaliteit is zonder meer aanwezig op internationaal vlak en vertaalt zich in juridische aanbevelingen en verdragen. Zo werd in oktober 2005 het Unesco Verdrag over culturele diversiteit goedgekeurd, en ondanks verzet van de Verenigde Staten (en zijn filmindustrie) is dit Verdrag al in meer dan tachtig landen geratificeerd (Tongue 2009).

Met meer gemak dan in de Verenigde Staten kan in Europa het mediapluralisme juridisch hard gemaakt worden, dit op grond van de leer van de positieve plichten, ditmaal afgeleid uit artikel 10 EVRM. Deze bepaling voorziet de vrijheid van meningsuiting voor eenieder. "Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen." De bepaling wordt herhaald in het EU Handvest (artikel 11) waarin echter een belangrijke toevoeging wordt ingelast. Volgens artikel 11 van het Handvest heeft eenieder het recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën, zonder inmenging van enig openbaar gezag en ongeacht grenzen (artikel 11, lid 1 Handvest). Tevens wordt het volgende bepaald: "De vrijheid en de pluriformiteit van de media worden geëerbiedigd" (artikel 12).

Binnen het wat oudere EVRM ontbreekt deze toevoeging, maar op basis van de Europese rechtspraak van het Europees Hof voor de Rechten van de Mens kan gesteld worden dat de eis als deel van het mensenrechtelijk *acquis* moet worden beschouwd. Hins heeft treffend aangetoond dat het belang van pluralisme al in een vroeg stadium werd onderkend en dat het Hof niet alleen de vrijheid van de media beschermt, maar ook het recht van het publiek om goed geïnformeerd te worden (Hins 2010: 98-100).[123] Daarbij wordt op beleidsniveau in Europa algemeen een grote rol weggelegd voor publieke mediadiensten. Denkbaar is, schrijft Hins, dat in de toekomst de vraag zal worden gesteld hoe een uitbreiding van de taken van de publieke omroep naar internet moet worden beoordeeld in het licht van artikel 10 EVRM. Is het subsidiëren van nieuwe diensten geoorloofd? Bestaat er zelfs een positieve verplichting om dit te doen? (Hins 2010: 99)

Er is voorlopig nog geen rechtspraak ter beantwoording van deze vragen, maar er zijn natuurlijk wel massa's indicaties over de mogelijke antwoorden. In een zaak die leidde tot het arrest TV *Vest As & Rogaland Pensjonistparti t. Noorwegen* uit 2008 werd het Hof geconfronteerd met een klacht van een kleine politieke partij over een algemeen verbod op tv-reclame voor politieke partijen. Het Hof keek naar dit verbod in het licht van artikel 10 EVRM en zag een gerechtvaardigd doel, namelijk het bestrijden van te simpele beeldvorming en voorkomen van benadeling van minder draagkrachtige partijen. Echter, merkte het Hof op dat een verbod ook contraproductief kan werken voor partijen die weinig bekend zijn. Tv-reclame kan voor hen juist een machtig middel zijn om de aandacht op zich te vestigen. Op basis van deze overweging was het Hof van oordeel dat een absoluut en permanent verbod disproportioneel was en onverenigbaar was met artikel 10 EVRM.[124] Het arrest geeft goed aan dat overheden een beleid kunnen uitstippelen tegen eenvoudige beeldvorming en voor pluriformiteit binnen de grenzen van de redelijkheid. Dat kan betekenen dingen uitsluiten *of* dingen toelaten. De Noorse bejaardenpartij moet een kans krijgen om zich zichtbaar te maken, ook al is het 'maar' via tv-reclame. De uitkomst van het arrest lijkt ons in de lijn te liggen van Sunsteins wens om een ontmoeting met onverwachte én bepaalde niet gewenste informatie blijvend mogelijk te maken. Een vrije samenleving, aldus Sunstein, respecteert keuzevrijheid, doch draagt ook zorg voor de opbouw van wensen, overtuigingen en denkbeelden: "When people are deprived of opportunities, they are likely to adapt and to develop preferences and tastes for what little they have" (Sunstein 2001: 122).

Een andere zaak die onze aandacht trekt, is deze die aanleiding gaf tot het arrest *Appleby e.a. t. Verenigd Koninkrijk* uit 2003.[125] Centraal stond een geprivatiseerd winkelcentrum The Galleries in Washington in het noordoosten van Engeland, nabij Newcastle, dat tevens de functie van nieuw stadscentrum vervult. Het management liet er bepaalde dorpsbewoners, onder wie Mary Eileen Appleby, niet toe om campagne te voeren tegen lokale bouwplannen. Doel van de actie was een informatiestandje op te zetten en een handtekeningenactie te organiseren in het publieke gedeelte van het winkelcomplex. De eigenaar van The Galleries gaf zoals gezegd geen toestemming. Hij wenste neutraal te blijven in politieke en religieuze zaken en gaf om deze reden nooit toestemming voor dit soort acties. Te Straatsburg klagen deze burgers over een schending van hun vrijheid van meningsuiting en vergadering. De zaak wordt bekeken in het licht van de positieve plichten die rusten op overheden. In het kort stelt het Hof dat de autoriteiten geen positieve verplichtingen hebben geschonden. Er bestonden immers voldoende alternatieve mogelijkheden voor de campagnevoerders om het publiek te bereiken en het Hof ziet dan ook geen schending van het Verdrag.

Voorhoof benadrukt terecht dat in de zaak Appleby de beperking op de grondrechten niet uitgaat van de overheid zelf, maar van een private organisatie, name-

lijk de eigenaar van het winkelcomplex. Van een directe verantwoordelijkheid van de overheid voor de beperking van de expressievrijheid van klagers is geen sprake. Toch wordt de zaak tegen het Verenigd Koninkrijk te Straatsburg ontvankelijk verklaard. Technisch juridisch erkent het Hof hier een vorm van 'indirecte horizontale werking'.[126] Ook private partijen moeten in beginsel rechten en vrijheden respecteren en op de overheid rust de verantwoordelijkheid om dit te bewerkstelligen. Op de staat rust dus een positieve verplichting om te komen tot een mensenrechtelijk eindresultaat en dit op grond van een eerlijke afweging van de op het spel staande belangen (Voorhoof 2003). In dit essay spreken we van systeemverantwoordelijkheid. De overheid moet maatregelen nemen om niet gewenste beperkingen van de expressievrijheid door de eigenaar van het winkelcomplex tegen te gaan.

Concreet geeft de uitkomst van de zaak geen hoop aan voorstanders van een democratische confrontatiepolitiek genre Sunstein. Het Hof betrekt in de balans niet alleen de expressievrijheid van eisers, maar ook het eigendomsrecht van het winkelcentrum in toepassing van artikel 1 van het Eerste Protocol bij het EVRM.[127] Eisers hadden in hun betoog verwezen naar een ontwikkeling in de Amerikaanse rechtspraak over soortgelijke disputen waaruit blijkt dat de rechters oog hebben voor de groeiende publieke functie als *public forum* van private winkelcentra die meer en meer functies aannemen van semi-publieke ruimtes. Toch is de rechtspraak onder invloed van de Supreme Court in meerderheid tegen het doortrekken van mensenrechteneisen naar deze juridisch private complexen. Met verwijzing naar deze 'ouderwetse' Amerikaanse rechtspraak komt het Europees Hof tot de conclusie dat de Britse autoriteiten niet tekort zijn geschoten en dat er geen schending is van artikel 10 EVRM, temeer daar de actiegroep over alternatieve kanalen beschikte om hun informatie te verspreiden en handtekeningen te verzamelen (andere winkels, de ingang van het winkelcomplex, het stadscentrum, lokale pers en deur-aan-deuracties). Het eigendomsrecht van de eigenaar van The Galleries krijgt daarom de voorrang in de belangenafweging en het Verenigd Koninkrijk wordt niet verantwoordelijk gesteld voor een falen van het systeem: "Balancing therefore the rights at issue and having regard to the nature and scope of the restriction in this case, the Court does not find that the Government failed in any positive obligation to protect the applicants' freedom of expression."[128]

2.8.4 GEVOLGTREKKINGEN: SYSTEEMVERANTWOORDELIJKHEID VOOR MEDIAPLURALISME

Vanuit mensenrechtelijk standpunt is het arrest *Appleby e.a. t. Verenigd Koninkrijk* uit 2003 geen stap vooruit. Het Hof erkent de ontwikkeling van nieuwe informatiekanalen die mogelijk negatieve effecten kunnen hebben op het recht op informatie te ontvangen en te verstrekken, maar schijnt niet te bewegen tot een tussenkomst dan in uiterste gevallen.[129]

Concreet 'wint' de Britse overheid de zaak en kan de eigenaar van The Galleries verdergaan met zijn absoluut verbod op expressie van meningen. Dat zet geen goede gedragslijn uit. De meerwaarde van de horizontale werking van mensenrechten bestaat erin dat de mensenrechten als uiterst fundamentele rechten, principes aanreiken die zo fundamenteel zijn dat ze in beginsel gerespecteerd moeten worden. Als een persoon een grondrecht van een andere persoon beperkt, weet of behoort hij te weten dat hij dit grondrecht slechts mag beperken als de beperking proportioneel beoordeeld kan worden ten aanzien van het doel dat hij nastreeft (Van Leuven 2009: 13).

Van belang is echter dat in het arrest principieel een systeemverantwoordelijkheid in hoofde van de overheid op het vlak van expressievrijheid erkend wordt, die dienstbaar is aan de idee van mediapluralisme. Het recht van de burger op vrije media en op degelijke informatie moet effectief gerealiseerd worden. Rechten zoals het eigendomsrecht moeten wijken wanneer deze rechten niet meer effectief kunnen worden uitgeoefend. We herinneren tevens aan het in het arrest *Armonas t. Litouwen* uit 2008 gemaakte onderscheid tussen het verspreiden van feitelijke informatie als onderdeel van een maatschappelijk debat enerzijds en smakeloze beschuldigingen betreffende het privéleven van een persoon anderzijds. In dit laatste geval moet de overheid beschermende maatregelen nemen.

Derhalve is het aan de overheid om op basis van de leer der positieve plichten een permanente bezinning te organiseren waarbij ook de nieuwe media worden betrokken (D'Haenens 2003: 91-122) , inclusief het gegeven dat in die nieuwe media 'content' geleverd kan worden door amateurs en het gegeven dat door te klikken op het reeds bekende groepspolarisatie kan ontstaan. Een deel van de verantwoordelijkheid is erkend met de herziene Mediawet[130] die de taakopdracht van de publieke omroep wijzigt in het licht van ontwikkelingen in technologie, media-aanbod, mediaproductie, distributie en mediagebruik en moet zorgen voor de aanwezigheid van een publieke sector in de sfeer van digitale televisie, IPTV, mobiele televisie en video on demand (Hins 2010: 93-108). Het andere luik van de systeemverantwoordelijkheid, zorg voor het publieke debat en tegengaan van groepspolarisatie door klikgedrag, staat nog nergens. In vergelijking met de uitgangspunten en invulling van de systeemverantwoordelijkheid voor de bescherming van persoonsgegevens (deel 1) en identiteitsfraude (deel 2) zijn onze juridische handen op dit punt het minst gevuld. Hoe zinvol te reageren op het internet- en kijkgedrag van burgers die omwille van de individuele autonomie geen inmenging dulden in hun consumptie van de beschikbare informatie op internet en op de andere moderne media? Kunnen we volstaan met het uitzetten van gedragslijnen gericht aan de personen die informatie verschaffen of moeten er ook gedragslijnen komen voor de personen die informatie tot zich nemen? Kinderen kunnen via onderwijs bereikt worden met goede cursussen mediakritiek die wijzen op de gevaren van te veel eigenzinnige deskundigheid bij blootstelling aan

informatie. Hoe bereiken we volwassenen? De overheid zal op een slimme wijze haar verantwoordelijkheid moeten nemen en een evenwicht moeten zoeken tussen betrokkenheid en onverschilligheid, tussen verpletteren en onbeschermd laten. Het zijn klassieke vragen rond de bescherming van de democratische rechtsstaat tegen zichzelf, vertaald naar problemen van vandaag. Nooit definitief te beantwoorden, maar altijd op te nemen.

2.9 ALGEMEEN BESLUIT

In dit essay wordt nagedacht over de systeemverantwoordelijkheid van de overheid in de informatiesamenleving. Deze verantwoordelijkheid 'voor het geheel' bestaat zowel op het vlak van bescherming van persoonsgegevens (deel 1), bestrijding van identiteitsfraude (deel 2) en de bescherming van het mediapluralisme (deel 3). De verantwoordelijkheid is moreel doch ook juridisch afdwingbaar op grond van de mensenrechten.
Aan de grondrechten van het EVRM kleven positieve verplichtingen. Deze brengen met zich mee dat de staat actief moet optreden tegen inbreuken door overheidsambtenaren én particulieren en positieve stappen moet ondernemen om het genot van grondrechten mogelijk te maken. Dit optreden vergt toezicht vooraf én achteraf, via wetgeving en beleid. Dat beleid moet op het strafrecht steunen wanneer zware vergrijpen voorliggen. Aanscherping van onduidelijke strafbepalingen, invoering van nieuwe strafbepalingen en gebruik van politie en justitie zijn daarbij niet uit te sluiten. De systeemverantwoordelijkheid van de overheid veronderstelt verantwoordelijkheidsdistributie. Andere actoren in de samenleving moeten gedwongen worden om hun verantwoordelijkheid te nemen en grondrechtenbeleving door andere burgers te respecteren, behoudens proportionele beperkingen. Gebeurt deze distributie niet of slecht, dan is de overheid terechte eindverantwoordelijke te Straatsburg voor het Europees Hof.

De aanname dat de Europese rechtspraak te weinig concrete handvatten geeft voor overheden is onterecht. Op het gebied van de bescherming van persoonsgegevens heeft het Hof algemene beginselen ontwikkeld, die in steeds meer zaken toegepast worden. Hetzelfde is in iets mindere mate waar voor de strijd tegen identiteitsfraude en de bescherming van het mediapluralisme. Nederland kan met die beginselen aan de slag en in dit essay is onder meer de suggestie gedaan om de geschiktheid van bestaande remedies en schadevergoedingssystemen te toetsen aan wat gebeurt met het plaatsen van materiaal over mensen op internet.
Het belang van het arrest *I. t. Finland* van 17 juli 2008 voor de discussie over de inrichting van de informatiemaatschappij is nog veel te weinig aan de orde gesteld. Het Hof stelt met zoveel woorden dat het loutere feit dat de nationale wetgeving de mogelijkheid geeft om een vergoeding te vragen, onvoldoende is en dat gezorgd moet worden voor een praktische en effectieve bescherming van dit rechtsgoed. Voorzien in een systeem van schadevergoeding, gebaseerd op eerlijke en toegan-

kelijke procedures is belangrijk, maar onvoldoende. Een volledige mensenrechtenstructuur die zowel beschermt als ontwikkelt (beter: ontwikkeling aanmoedigt) is nodig en uit het arrest *K.U. tegen Finland* van 2 december 2008 blijkt dat voor het Hof de gewenningsfase voorbij is: de informatiemaatschappij is er en overheden hebben sinds de jaren negentig tijd gehad om adequaat op te treden.

Dit essay begon met een vergelijking tussen het debat over de informatiemaatschappij en over het respect voor de mensenrechten door multinationals in 'zwakke' landen. In beide debatten is er een sterke onderstroom tegen regulering en overheidsinterventie en worden governance gaps met de mantel der liefde toegedekt dan wel gecreëerd of gesteund, weze het in naam van de nieuwheid van de technologie die alle ontwikkelingskansen moet krijgen of in naam van de economische ontwikkeling in arme landen.[131]

Binnen het paradigma van de verantwoordelijkheden zijn er meerdere keuzen mogelijk, waarbij Ruggies Protect, Respect, Remedy-schema goed het basisschema voor de bouwstenen aangeeft, maar waarbij sommigen vooral wat de bedrijven beteft een stap verder willen gaan en hun *respect*-opdracht omzetten in een *protect*-opdracht. Uit de leer van de positieve plichten blijkt dat in Europa een actieve, beschermende taak mag verwacht worden van bedrijven. Wie macht heeft moet verantwoording afleggen. Een informatiemaatschappij die werkt met providers die geen problemen zien in onveilige diensten en ongecontroleerde informatieverstrekking, ook over derden, is steeds minder verdedigbaar. De burger kan niet verantwoordelijk gehouden worden voor een systeem waarin de overheid haar rol niet speelt en vergeet of weigert om relevante actoren voor hun verantwoordelijkheden te plaatsen. Zo werkt systeemverantwoordelijkheid niet.

NOTEN

1 Cf. www.dataprotectionday.eu.

2 Het is belangrijk hier stil te staan bij het verschil in de samenstelling van de Subcommissie, bestaande uit 26 onafhankelijke deskundigen, en de Mensenrechtencommissie waarin 53 regeringsvertegenwoordigers zetelen. Uit de samenstelling blijkt het doorgetrokken politieke karakter van de Mensenrechtencommissie, in tegenstelling tot de Subcommissie. Deze factor kan één van de achterliggende redenen zijn voor het 'falen' van de *Norms*.

3 Zo maakte het Britse Nationaal Contactpunt van de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) gebruik van het concept *due diligence* van de SRSG in een mensenrechtenklacht tegen een onderneming. Ook aanvaarden onder meer de International Organization of Employers (IOE), de International Chambre of Commerce (ICC) en de Business and Industry Advisory Committee (BIAC) het beleidskader als leidraad. Ten slotte erkennen ook niet-gouvernementele organisaties (NGO's) zoals Amnesty International het belang van Ruggies werk.

4 Cf. art. 12 tot 15 van Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel in de interne markt, *Pb*., L 178/1 van 17 juli 2000. Deze richtlijn beoogt zonder binnengrenzen het vrije verkeer van diensten van de informatiemaatschappij tussen de lidstaten te waarborgen. Meer vrijheid en vertrouwen in de elektronische handel staan daarbij centraal. Opvallend is dat deze richtlijn tevens bepalingen bevat met een weerslag op het strafrecht. De tekst voorziet in een horizontale (voor alle rechtsgebieden gelijk geldende) aansprakelijkheidsbeperking ten behoeve van internetproviders. Het gaat om de artikelen 12 tot en met 14 die de service provider vrijwaren voor de aansprakelijkheid voor de informatie voor websites die via zijn toegangsdienst beschikbaar komen, wanneer hij alleen maar doorgeefluik is (*mere conduit*), wanneer hij die pagina's alleen maar kort opslaat als het om veelgevraagde informatie gaat (*caching*) of wanneer hij tijdelijk informatie van een ander herbergt (*hosting*). Deze regels zijn dus behoudens op het terrein van het intellectueel recht, ook van toepassing op het strafrecht. Men leze: Van Esch 2001: 379-381; Schellekens 2001; Bodard, 2001: 285-331; Van der Net 2002: 10-15. Op de regeling in de richtlijn, die zeer vriendelijk is voor de tussenpersonen, zeker ten aanzien van de bestaande regels inzake strafrechtelijke en burgerrechtelijke aansprakelijkheid in verschillende landen, is veel kritiek gerezen. Men leze voor Frankrijk en België Lucas 2001: 42-52; voor Nederland Van Esch 2001: 380.

5 Compliance betekent (niet meer) dan dat een organisatie voldoet aan de regels die van buitenaf of van binnenuit zijn opgelegd. Deze worden gezien als een last die met tegenzin wordt gedragen, maar niet als trigger om te komen tot een actief gestuurd beleid waarbij processen worden bijgestuurd. Accountability of *proven trust* staat tegenover compliance als *blind trust*. Bij accountability is het voor

betrokkene mogelijk om bewijs te leveren van goed gedrag omdat zelf actieve, aanwijsbare stappen zijn gezet om een bepaald 'goed' te bewerkstelligen of te beschermen. Zie voor een brede definitie (te breed) van compliance: De Vries H. & W. Janssen, 'Compliance als kans', *Ego. Magazine voor informatiemanagement*, 2010, vol. 9, nr. 3, blz. 11-15.

6 Voorbereidende notitie *Beginsel Accountability*, Projectgroep BIT, WRR 2010, blz. 10. De voorbereidende notitie *Beginsel Accountability* van de projectgroep BIT is niet gepubliceerd. Een exemplaar van deze notitie is op te vragen bij de WRR.

7 De auteurs van de tekst wijzen erop dat bij gebruik van informatietechnologie de anatomie van overheidsbeslissingen aan het oog wordt onttrokken "waardoor het geheel minder goed toetsbaar is. Veel van wat bij rechtsbescherming komt kijken, is immers het uiteenrafelen van besluitvormingstrajecten, mede om te bepalen of de gang van zaken in alle fasen ook procesmatig zorgvuldig is geweest. Die zorgvuldigheid is bij geautomatiseerde processen veel minder goed na te gaan omdat dan eigenlijk getoetst moet worden hoe het systeem ontworpen is, wat een tamelijk moeilijke, abstracte, en ook betekenisloze exercitie kan zijn." Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 11.

8 Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 2.

9 Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 12.

10 De leer is bijvoorbeeld onbekend in het Amerikaanse constitutioneel recht.

11 EHRM, *Paula en Alexandra Marckx t. België*, 13 juni 1979, *N.J.*, 1980, 462, noot EAA; EHRM, *Johanna Airey t. Ierland*, 9 oktober 1979, *Series A*, vol. 32, § 32; EHRM, *Mark Rees t. Verenigd Koninkrijk*, 17 oktober 1986, *Series A*, vol. 106, § 36; *N.J.*, 1987, nr. 945, noot E. Alkema; EHRM, Graham Gaskin, 7 juli 1989, *Series A*, vol. 160, § 42. Zie eveneens EHRM, *Johnston t. Ierland*, 28 december 1987, *Series A*, vol. 128. Men leze Lawson 1995: 559-567.

12 In de Stjerna-zaak verduidelijkt het Hof op een zeldzaam duidelijke wijze het verschil tussen positieve en negatieve plichten. De weigering van de Finse overheid om Stjerna toe te laten zijn naam te veranderen vormt geen inmenging met zijn grondrecht op privéleven en gezinsleven en de theorie van de positieve plichten moet dan ook toegepast worden. Van een inmenging, aldus het Hof, zou bijvoorbeeld sprake zijn wanneer de overheid Stjerna zou verplichten van naam te veranderen (EHRM, *Stjerna t. Finland*, 25 november 1994, *Series A*, vol. 299-B, § 38). Over dit aspect van het arrest: Lawson 1995: 743-746.

13 EHRM, *Marie-Patrice Lassauzet en Gérard Guillot t. Frankrijk*, 24 oktober 1996, *Reports of Judgements and Decisions*, 1996.

14 ECRM, *Willsher t. Verenigd Koninkrijk*, 9 april 1997, verzoekschrift nr. 31024/96, E.H.R.R., 1997, jan-ma, 191.

15 EHRM, *Gregoria López Ostra t. Spanje*, 9 december 1994, *Series A*, vol. 303-C, § 58; EHRM, *Guerra e.a. t. Italië*, 19 februari 1998, *J.T.D.E.*, 1998, 91-92; *Nederlands Juristenblad*, 17 april 1998, 742-743; *NJCM-Bulletin*, 1998, 5: 639-640, § 60.

16 EHRM, *Botta t. Italië*, 24 februari 1998, *Nederlands Juristenblad*, 24 april 1998: 789; *NJCM-Bulletin*, 1998, 5, 597-610, noot R. Lawson en noot A. Hendriks; *NJCM-*

Bulletin, 1998, 5: 647-648. Een overzicht van wetgeving ter bescherming van de fysiek gehandicapte persoon in België geeft: Nys 1991-1992: 350-360.

17 EHRM, *Botta t. Italië*, 24 februari 1998, *l.c.*, § 34.

18 Recapitulerend kunnen we op basis van het voorgaande besluiten dat een schending van de rechten vervat in artikel 8 EVRM mogelijk is: - wanneer de staat zich inmengt in deze grondrechten; - wanneer een onthouding of een niet optreden van de staat de rechten erkend in de bepaling miskennen; - wanneer een onthouden van de staat derden in de mogelijkheid stelt de genoemde rechten te miskennen. Cf. Cohen-Jonathan 1989: 375; Renchon 1994: 99.

19 Bovendien moet in concreto nagegaan worden of er een verband bestaat tussen een mogelijke positieve verplichting en de klacht van het subject dat de schending van zijn grondrechten inroept.

20 "The Court does not consider that Ireland can be said to have 'interfered' with Airey's private or family life: the substance of her complaint is not that the State has acted but that it has failed to act. However, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life (see the above-mentioned Marck judgement)" (EHRM, *Johanna Airey t. Ierland*, 9 oktober 1979, *Series A*, vol. 32, § 32).

21 EHRM, *Graham Gaskin t. Verenigd Koninkrijk*, 7 juli 1989, *Series A*, vol. 160, § 41.

22 EHRM, *X en Y t. Nederland*, 26 maart 1985, *Series A*, vol. 91; *R.W.*, 1985-86: 265; *NJCM-Bulletin*, 1985: 410-419, noot J. Schokkenbroek; *N.J.*, 1985, blz. 16925-194, noot E. Alkema.

23 EHRM, *X en Y t. Nederland*, § 23.

24 In casu werd Y., een dag na haar zestiende verjaardag, seksueel misbruikt door de zoon van de directrice van het verblijf voor geestelijk gehandicapten, waar ze verbleef. Na seponering door het parket start haar vader (X.) een gerechtelijke procedure wegens het opzettelijk bewegen van minderjarigen tot ontucht (art. 248ter Nl. Sw.). De procedure wordt desondanks door het Arnhemse gerechtshof niet-ontvankelijk verklaard, daar luidens het strafwetboek alleen het slachtoffer zelf een klacht had kunnen indienen (Hof Arnhem, 12 juli 1979, *N.J.* 1980, nr. 175). Alleen voor jongeren onder de zestien jaar wordt voorzien in een wettelijke vertegenwoordiging. Te Straatsburg klagen vader en dochter een schending aan van artikel 8, 3, 13 en 14 EVRM. Met betrekking tot artikel 8 EVRM wordt aangevoerd dat voor een jong meisje als Y. alleen strafrechtelijke bescherming volstaat.

25 EHRM, *X en Y t. Nederland*, § 27.

26 Cf. EHRM, *Paula en Alexandra Marckx t. België*, § 31.

27 Cf. EHRM, *X en Y t. Nederland*, 26 maart 1985, *Series A*, vol. 91, § 23.

28 EHRM, *M.C. t. Bulgarije*, 4 december 2003, rolnummer 39272/98, *EHRC*, 2004/6, noot G. Mols. Men leze tevens Brems 2004: 575-577.

29 De verzoekster stelde dat ze in de zomer van 1995, toen ze veertien jaar oud was,

door twee mannen was verkracht. Ze was vrijwillig met drie vage kennissen meegegaan met de wagen naar een disco, maar de mannen brachten haar nadien naar een waterplas, zogezegd om te zwemmen. Daar gebeurde de eerste verkrachting. Bang en gegeneerd had het meisje niet de kracht om zich te verzetten. Nadien ging ze met de mannen mee naar een woning, waar een tweede man haar verkrachtte. Naar eigen zeggen had ze gehuild en gesmeekt om te stoppen, maar geen fysiek verzet geboden. Toen haar moeder haar 's ochtends in die woning aantrof, bracht ze haar naar het ziekenhuis, waar werd vastgesteld dat ze seksuele betrekkingen had gehad. Dit ontkenden de mannen niet, maar ze beweerden dat het om vrijwillige betrekkingen ging. Uiteindelijk kwam het tot een rechtszaak, waarin de mannen werden vrijgesproken. De rechter stelde dat niet bewezen was dat het meisje met geweld gedwongen was om seks te hebben, aangezien er geen bewijs was dat ze zich verzet zou hebben.

30 Het Hof verweet de Bulgaarse rechters dat ze in de afwezigheid van rechtstreeks bewijs van verkrachting nalieten de omstandigheden van het misdrijf te reconstrueren en de geloofwaardigheid van tegenstrijdige verklaringen te evalueren waaruit mogelijk een onrechtstreeks bewijs van afwezigheid van toestemming kon worden afgeleid. Uit het rapport van de Bulgaarse onderzoekers blijkt dat ze niet uitsloten dat het meisje niet zou hebben toegestemd, maar dat ze bij gebrek aan bewijs van verzet niet konden besluiten dat de daders begrepen hadden dat ze niet toestemde.

31 Concreet vereiste het Bulgaarse strafrecht geen bewijs van fysiek verzet, maar werd het wel op die manier geïnterpreteerd.

32 Cf. paragraaf 150: "Positive obligations on the State are inherent, in the right to effective respect for private life under Article 8; these obligations may involve the adoption of measures even in the sphere of the relations of individuals between themselves. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is in principle within the State's margin of appreciation, effective deterrence against grave acts such as rape, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions. Children and other vulnerable individuals, in particular, are entitled to effective protection." (see *X and Y v. the Netherlands*, judgment of 26 March 1985, Series A no. 91, blz. 11-13, 23, 24 and 27; and *August v. the United Kingdom* (dec.), no. 36505/02, 21 January 2003).

33 EHRM, *M.C. t. Bulgarije*, 4 december 2003, rolnummer 39272/98, *EHRC*, 2004/6, noot G. Mols, § 153.

34 Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 1-2.

35 Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 2.

36 Resp. Voorbereidende notitie *Beginsel Accountability*, o.c., blz. 2 en 9. We komen later terug op het tweede voorbeeld.

37 Voorbereidende notitie *Beginsel Accountability*, blz. 10.

38 "Veel van wat bij rechtsbescherming komt kijken, is immers het uiteenrafelen van besluitvormingstrajecten, mede om te bepalen of de gang van zaken in alle fasen ook

procesmatig zorgvuldig is geweest. Die zorgvuldigheid is bij geautomatiseerde processen veel minder goed na te gaan omdat dan eigenlijk getoetst moet worden hoe het systeem ontworpen is, wat een tamelijk moeilijke, abstracte, en ook betekenisloze exercitie kan zijn." Voorbereidende notitie *Beginsel Accountability*, blz. 11.

39 Over deze 'accountability zonder de sanctie van verantwoordelijkheid', leze men Voorbereidende notitie *Beginsel Accountability*, blz. 15.

40 De Schutter verwijst in dit verband naar het werk van Lon Fuller. Deze ontwikkelde de idee van polycentraliteit: een aantal geschillen zijn inherent ongeschikt om door een rechter beoordeeld te worden omdat erachter complexe kwesties en belangen schuil gaan die onderling met elkaar verbonden zijn. Cf. Fuller 1972: 353 e.v.

41 Vgl. met EHRM, 25 november 2008 (*Armonas t. Litouwen*), verzoekschrift nr. 36919/02, *EHRC*, 2009, nr. 6, noot Gerards, § 46: "The Court agrees with the Government that a State enjoys a certain margin of appreciation in deciding what 'respect' for private life requires in particular circumstances (cf. *Stubbings and Others v. the United Kingdom*, 22 October 1996, §§ 62-63, *Reports* 1996-IV; *X and Y v. the Netherlands*, 26 March 1985, § 24, Series A no. 91). The Court also acknowledges that certain financial standards based on the economic situation of the State are to be taken into account when determining the measures required for the better implementation of the foregoing obligation."

42 EHRM, 25 november 2008 (*Armonas t. Litouwen*), verzoekschrift nr. 36919/02, EHRC, 2009, nr. 6, noot Gerards, § 38: "The Court reiterates that, as regards such positive obligations, the notion of respect is not clear-cut. In view of the diversity of the practices followed and the situations obtaining in the Contracting States, the notion's requirements will vary considerably from case to case. Accordingly, this is an area in which the Contracting Parties enjoy a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention, account being taken of the needs and resources of the community and of individuals (see *Johnston and Others v. Ireland*, judgment of 18 December 1986, Series A no. 112, § 55). The Court nonetheless recalls that Article 8, like any other provision of the Convention or its Protocols, must be interpreted in such a way as to guarantee not rights that are theoretical or illusory but rights that are practical and effective (see *Shevanova v. Latvia*, no. 58822/00, § 69, 15 June 2006)."

43 ECommissieRM, *Pierre Herbecq en Ligue des droits de l'homme t. België*, 14 januari 1998, verzoekschriften nr. 32200/96 en 32201/96, *J.T.D.E.*, 1998, 67-68; *Algemeen Juridisch Tijdschrift (AJT)*, 1998, noot P. de Hert & O. De Schutter.

44 EHRM, 28 januari 2003 (*Peck t. Verenigd Koninkrijk*), verzoek nr. 44647/98, *Nederlands Juristenblad (NJB)*, 2003, nr. 625; *Reports of Judgments and Decisions*, 2003-I.

45 De Britse overheid had tevergeefs een beroep gedaan op artikel 10 EVRM. Het verweer luidde dat een effectieve rechtsbescherming tegen de schending van het recht op privacy door de media een bedreiging zou vormen voor de persvrijheid. Daarmee is het Hof het evenwel niet eens. Het Mensenrechtenhof overweegt dat "*As noted above, the Council, and therefore the media, could have achieved their*

objectives by properly masking, or taking appropriate steps to ensure such masking of the applicant's identity".

46 EHRM, 17 juli 2008 (*I. t. Finland*), verzoekschrift nr. 20511/03 *European Human Rights Cases (EHRC)*, 10 september 2008, vol. 9, 9: 1136-1140. Men leze Råman 2008: 562-564.

47 EHRM, *I. t. Finland*, § 36.

48 EHRM, *I. t. Finland*, § 38.

49 EHRM, *I. t. Finland*, § 38.

50 EHRM, *I. t. Finland*, § 40.

51 EHRM, *I. t. Finland*, § 47.

52 Aquiliaanse aansprakelijkheid houdt in dat een fout de oorzaak is van de hinder.

53 EHRM, *I. t. Finland*, § 44: "The Court notes that the applicant lost her civil action because she was unable to prove on the facts a causal connection between the deficiencies in the access security rules and the dissemination of information about her medical condition. However, to place such a burden of proof on the applicant is to overlook the acknowledged deficiencies in the hospital's record keeping at the material time. It is plain that had the hospital provided a greater control over access to health records by restricting access to health professionals directly involved in the applicant's treatment or by maintaining a log of all persons who had accessed the applicant's medical file, the applicant would have been placed in a less disadvantaged position before the domestic courts. For the Court, what is decisive is that the records system in place in the hospital was clearly not in accordance with the legal requirements contained in section 26 of the Personal Files Act, a fact that was not given due weight by the domestic courts."

54 "The Court finds it established that the applicant must have suffered non-pecuniary damage as a result of the State's failure to adequately secure her patient record against the risk of unauthorised access. It considers that sufficient just satisfaction would not be provided solely by the finding of a violation and that compensation has thus to be awarded. Deciding on an equitable basis, it awards the applicant EUR 8,000 under this head" (EHRM, *I. t. Finland*, § 47).

55 Vgl. Voorbereidende notitie *Beginsel Accountability*, blz. 15.

56 EHRM, 25 november 2008 (*Armonas t. Litouwen*), verzoekschrift nr. 36919/02, *EHRC*, 2009, nr. 6, noot Gerards.

57 Het was niet duidelijk of de voortzetting van een geding mogelijk is voor nabestaanden van het oorspronkelijke slachtoffer van een mogelijke schending van een verdragsrecht. Het Hof antwoordt hier positief over. Het Hof is van oordeel dat eiser zich wel degelijk als slachtoffer kan wenden tot het Europees Hof. Het Hof heeft eerder al geoordeeld dat het een zaak niet-ontvankelijk zal verklaren indien de grond van de zaak te nauw verbonden is met de overledene en dus niet kan overgebracht worden op de erfgenamen. In casu is dit echter niet het geval. Na publicatie van het artikel zag het gezin zich genoodzaakt te verhuizen en bovendien had de nationale rechter geoordeeld dat het artikel de communicatiemogelijkheden van het gezin had beperkt. Het artikel had daarom een negatieve weerslag

zowel op verzoekster als op haar minderjarig kind. Ook het argument van de Litouwse overheid dat verzoekster geen slachtoffer meer was, omdat de nationale rechter reeds een schending van haar privéleven had vastgesteld en een schadevergoeding had toegekend werd van tafel geveegd. Dit doet geen afbreuk aan een mogelijke kwalificatie als slachtoffer. Vgl. EHRM, *Micallef t. Malta*, verzoekschrift nr. 17056/06, 15 oktober 2009, *EHRC* 2009, blz. 125; Centrale Raad van Beroep, 4 mei 2010, nr. 09/819 BESLU + 09/1232 BESLU, LJN BM5682, via http://jure.nl/bm5682.

58 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 36.

59 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 37.

60 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 39.

61 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 39.

62 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 47.

63 EHRM, 25 november 2008 (*Armonas t. Litouwen*), § 47.

64 Hof van Justitie, *Bodil Lindqvist*, zaak C-101/01, arrest van 6 november 2003 via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0101:EN:HTML. In dit arrest oordeelt het Hof van Justitie dat de elektronische publicatie van persoonsgegevens door middel van een website op internet onder de werkingssfeer van Richtlijn 95/46/EG betreffende de gegevensbescherming van natuurlijke personen valt. De zaak betrof een vrijwilligster van een protestantse kerkelijke gemeente in Zweden die op eigen initiatief, op een door haar ontwikkelde internetpagina, namen, telefoonnummers en informatie over werkzaamheden en liefhebberijen had opgenomen, niet alleen over haar zelf, maar ook over haar collega-vrijwilligsters. Bovendien vermeldde zij dat een van haar collega's haar voet had bezeerd en gedeeltelijk met ziekteverlof was. Men leze Blok 2004: 30-36; Winkelhorst en Van der Linden-Smith 2004: 627-631; Overkleeft-Verburg 2004: 114-116; De Hert en Schreurs 2004: 127-138.

65 Rechtbank Amsterdam 11 september 2009, *LJN* BK1859. Cf. Volgende blogs: http://copsincyberspace.wordpress.com/2009/11/05/geenstijl-en-de-dronken-maastrichtse-praeses-culpa-in-causa/; http://jurel.nl/2009/10/28/dronken-maastrichtse-praeses-culpa-in-causa/ en http://blog.iusmentis.com/2009/09/28/geenstijl-moet-privacyschendend-majesteit-filmpje-verwijderen-van-dumpert/.

66 Voor deze overweging kan steun gevonden worden in EHRM, *Reklos & Davourlis t. Griekenland*, 15 januari 2009, nr. 1234/05, *NJ* 2009, 524, noot E.J. Dommering, § 40 e.v.

67 Onder verwijzing naar het arrest *Armonas t. Litouwen* en andere soortgelijke arresten.

68 Zie voor dit laatste EHRM, *Reklos & Davourlis t. Griekenland*, 15 januari 2009, nr. 1234/05, *NJ* 2009, 524, noot E.J. Dommering, § 47.

69 Merken we op dat de zaak inmiddels ook voor de rechtbank van Amsterdam is gebracht. Deze rechtbank heeft geoordeeld dat GeenStijl.nl een schadevergoeding moet betalen. Cf. Rechtbank Amsterdam, vonnis 14 juli 2010, via http://www.geenstijl.nl/archives/images/GeenStijl2010-2.pdf.

70 Europees Parlement, de Raad en de Commissie, 'Handvest van de Grondrechten van de Europese Unie', *Pb.*, C 364 van 18 december 2000, 1-22 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:364:0001:0022:NL:PDF).

71 Europees Parlement, de Raad en de Commissie, 'Handvest van de Grondrechten van de Europese Unie (2007/C 303/01)', *Pb.*, C 303, 14 december 2007: 1-16 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:NL:PDF). Het Verdrag van Lissabon verleent het handvest bindende kracht door de opname van een vermelding waardoor het dezelfde rechtskracht krijgt als de Verdragen. Te dien einde werd het handvest in december 2007 een tweede keer afgekondigd.

72 Verdrag van Lissabon van 13 december 2007 tot wijziging van het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, ondertekend te Lissabon, *Pb.*, C 306, 17 december 2007, 1-231 (http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:NL:HTML). Het verdrag trad in werking op 1 december 2009.

73 Over het ontbreken van het doelbindingprincipe in het recht van de Verenigde Staten, leze men De Hert en Bellanova 2008.

74 OESO-Richtlijnen: OECD-Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 september 1980 in *Guidelines governing the protection of privacy and transborder data flows of personal data*, Parijs, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317.

75 Verdrag van Straatsburg: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, nr. 108; *International Legal Materials*, 1981, I: 422.

76 Richtlijn 95/46/EG 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, *Pb.,* L 381 van 23 november 1995.

77 Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken, *Pb.*, L 350, 30 december 2009: 60-71.

78 Over het gebrek aan sturing rond biometrie: voor Europa Kindt en Müller 2009. Voor Nederland; De Hert en Sprokkereef 2009.

79 Cf. Baldor 2010. "Comparing the digital age to the dawn of automobiles, analysts said more government regulations may be the only way to force the public and private sectors to adequately counter cyber threats. They compared the need for new oversight to regulations for seat belts and safety equipment that made the highways safer."

80 Richtlijn 97/66/EG van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector, *Pb., L* 24 van 30 januari 1998: 1-8. Over deze richtlijn: Smits 1993: 50-53; Nugter en Smits 1991: 269; Hoven Van Genderen 1993: 45; Cuny 1998: 62-67; Roy 1995: 52-57.

81 Hoven Van Genderen 1993: 45. ISDN staat voor Digitaal Netwerk voor Geïntegreerde Diensten.

82 Art. 5 van Richtlijn 97/66/EG.

83 Art. 8 van Richtlijn 97/66/EG. De richtlijn geeft elke abonnee gratis de mogelijkheid per gesprek nummeridentificatie te blokkeren (uit te schakelen), zodat hij bij een oproep anoniem blijft. Tevens beschikt elke abonnee over de mogelijkheid bepaalde binnenkomende nummers te blokkeren. In een aantal gevallen kan er gedeblokkeerd worden: bij hijgtelefoontjes, in het kader van een strafonderzoek en bij bepaalde nood- en hulpdiensten (art. 9 van Richtlijn 97/66/EG).

84 Art. 6 van Richtlijn 97/66/EG. Sommige gegevens mogen toch bewaard en verkocht worden, maar in dat geval beschikt de abonnee over een recht van verzet in de zin dat hij met de verkoop moet instemmen.

85 Art. 3 van Richtlijn 97/66/EG.

86 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), *Pb.,* L 201, van 31 juli 2002, blz. 37-47.

87 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *Pb*., L 337, 18 december 2009, blz. 11-36. De nieuwe richtlijn moet in nationaal recht omgezet worden tegen 25 mei 2011. Zie hierover Debusseré 2009; Cuijpers 2008: 119.

88 De ePrivacyrichtlijn is een specifieke richtlijn en de nieuwe maatregelen richten zich in hoofdzaak tot aanbieders van openbare elektronische communicatiediensten, zoals telecommunicatiebedrijven en internet service providers. Gezien de toenemende vervlechting tussen de I (*information*) en de C (*communication*) uit ICT is dit evenwel reeds een substantiële groep binnen de informatiemaatschappij. Bovendien leeft de verwachting dat een aantal van de nieuwe maatregelen uit de ePrivacyrichtlijn in de aangekondigde herziening van de algemene richtlijn van 1995 veralgemeend zullen worden, zodat ze van toepassing zullen worden op allen die persoonsgegevens verwerken, dus ook zij die buiten de telecommunicatiesector werken.

89 Een 'inbreuk in verband met persoonsgegevens' wordt ruim gedefinieerd als 'een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens die zijn verstuurd, opgeslagen of anderszins verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Gemeenschap'.

90 In zijn kennisgeving aan de gebruikers moet de aanbieder minstens de aard van de

inbreuk en de contactpunten voor meer informatie vermelden en maatregelen aanbevelen om mogelijke negatieve gevolgen van de inbreuk te verlichten. De individuele gebruiker moet niet in kennis gesteld worden als de aanbieder aan de bevoegde nationale instantie aantoont dat hij de gegevens beschermd heeft met technische beschermingsmaatregelen die de gegevens onbegrijpelijk maken voor onbevoegden. Als de aanbieder beslist om de individuele gebruikers niet in te lichten maar de nationale bevoegde instantie oordeelt dat de inbreuk voor de individuele gebruikers mogelijk ongunstige gevolgen heeft, kan die de aanbieder dwingen de individuele gebruikers toch in te lichten. Die instantie kan ook instructies uitvaardigen over de omstandigheden waarin de kennisgeving noodzakelijk is, het formaat ervan en de manier waarop de kennisgeving moet gebeuren.

91 Onder meer wordt het toepassingsgebied van het verbod uitgebreid. Onder de oude regeling was dit beperkt tot de situatie waarin de toegang tot en het opslaan van informatie op de gebruikersapparatuur gebeurde door middel van *elektronische communicatienetwerken*. Het was echter niet duidelijk of de regeling ook van toepassing was op de situatie waarin cookies, spyware en dergelijke op de gebruikersapparatuur terechtkwamen via software op externe gegevensdragers (zoals cd-roms en usb-sticks) of downloads. Om ook deze zeker binnen het toepassingsgebied te brengen, werden de woorden 'door het gebruik van elektronische communicatienetwerken' geschrapt.

92 Cf. de verklaring van de staatssecretaris van Economische Zaken in zijn brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal, 30 mei 2008, *Tweede Kamer der Staten-Generaal*, Vergaderjaar 2007–2008, 31200 XIII, nr. 57.

93 Cbp, «RFID Veelbelovend of onverantwoord? Bijdrage aan de maatschappelijke discussie over RFID», 2006 via http://www.cbpweb.nl/Pages/av_29_rfid.aspx

94 "Heemskerk gaf aan vooralsnog niks te voelen voor verdere wetgeving. Ten eerste zie ik niet in hoe we een wettelijk dichtgetimmerde zorgplicht up to date kunnen houden in een uiterst dynamisch technologisch klimaat. Verder houd ik mijn hart vast als het gaat over de administratieve lasten en de handhaving van zulke regelgeving," uit Heemskerk 2008.

95 Artikel 11.3 van de wet bevat waarborgen 'in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers': aanbieders van openbare elektronische communicatiediensten en netwerken moeten passende technische en organisatorische maatregelen nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen dienen, rekeninghoudend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te garanderen dat in verhouding staat tot het desbetreffende risico (art. 11.3 lid 1 Tw); tevens moeten ze er zorg voor dragen dat de abonnees worden geïnformeerd over de bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van het aangeboden netwerk of de aangeboden dienst en de beschikbare middelen waarmee de bedoelde risico's kunnen worden uitgesloten of verkleind en de kosten die daarmee gemoeid zijn (art. 11.3, lid 2 Tw).

96 Men leze het consultatiedocument van de Opta beschikbaar via *http://www.opta.nl/download/Consultatie_Voorlichting.pdf*

97 Voorbereidende notitie *Beginsel Accountability*, blz. 15.

98 Over deze 'politics of scale', leze men De Hert 2004: 55-102.

99 Voorbereidende notitie *Beginsel Accountability*, blz. 12-13. Zie hierover Koedooder 2009.

100 "Identiteitsfraude valt niet of nauwelijks als zodanig in de systemen te traceren omdat het geen zelfstandig delict betreft en aangiftes achter de brede noemer van art. 231 Sr (fraude met reisdocumenten) en art. 326 Sr (oplichting) verdwijnen. Dienders worstelen met het fenomeen: burgers die aangifte willen doen wordt gemeld dat niet zij, maar hun bank het slachtoffer is." (Ibid.).

101 Voor kritiek op het bestaande meten van identiteitsfraude, leze men Van Eeten 2011. Zie ook Kaspersen 2009: 222.

102 "Willen we de onzekerheid ten aanzien van de risico's terugdringen en daartoe meer inzicht verkrijgen in aard en omvang van identiteitsfraude, dan heb ik in aanvulling op het bovenstaande nog meer wensen: specifieke voorlichting (zowel richting publiek als de diender op straat), landelijke ruchtbaarheid aan het Meldpunt dat deze week z'n definitieve status kreeg en absoluut: serieuze aandacht voor structurele samenwerking tussen publieke en private (waaronder financiële instellingen) partijen. En wellicht – voor de noodzakelijke coördinatie tussen het enorme scala aan partijen dat bij de problematiek is betrokken – een landelijk ID-fraude officier (met team). En als inderdaad blijkt dat burgers het slachtoffer zijn van identiteitsfraude moet de overheid meer te bieden hebben dan het opnemen van de aangifte alleen. Ook moet ze de helpende hand rijken in herstellen of reduceren van ellende. Zowel overheid als bedrijfsleven hebben in de huidige samenleving van complexe en oneindig gekoppelde informatiesystemen, hier hun verantwoordelijkheid te nemen". Prins 2010: 537.

103 Met verwijzing naar Steennot 2008: 555-561; Spindler 2007.

104 EHRM, *Reklos & Davourlis t. Griekenland*, 15 januari 2009, nr. 1234/05, *NJ* 2009, 524, noot E.J. Dommering, § 39.

105 EHRM, *K.U. t. Finland*, 2 december 2008, verzoekschrift nr. 2872/02. Zie Voorhoof 2009: 113-127 en Groothuis 2009: 281-289.

106 De Finse wetgeving maakte het op het ogenblik van de feiten slechts voor een beperkt aantal misdrijven mogelijk om ISP's te verplichten om identiteitsgegevens aan politie of justitie te verstrekken. Het opsporen van de identiteit van wie mogelijk aansprakelijk was voor lasterlijke informatie op internet, was niet een van de mogelijkheden voorzien bij wet. Deze afwijzing door de rechtbank werd later bevestigd door het hof van beroep. Ook het beroep bij het Hooggerechtshof werd afgewezen.

107 Het betreft bijvoorbeeld Aanbeveling n° R(95) 13 betreffende strafprocedurele problemen gerelateerd aan informatietechnologie. Daarin worden staten onder meer aangemoedigd om verplichtingen op te leggen aan *service providers "who offer telecommunication services to the public, either through public or private networks,*

[in order] to provide information to identify the user, when so ordered by the competent investigating authority". Vermeld wordt ook de *Convention on Cybercrime* van 23 november 2001 en de *Guidelines for the cooperation between law enforcement and internet service providers against cyber crime* van 1-2 april 2008. Ook de Verenigde Naties hebben verschillende resoluties aangenomen over deze materie (55/63 en 56/121). Voorts is er op het vlak van de Europese Unie de Richtlijn 2006/24 van 15 maart 2006 betreffende de bewaring van gegevens (...). Het Europees Hof wijst er nog op dat in de meeste lidstaten van de Raad van Europa voorzien is in een specifieke wetgeving die service providers verplicht, ongeacht de aard van het misdrijf, data over te dragen aan de bevoegde onderzoeksinstanties.

108 EHRM, *K.U. t. Finland*, 2 december 2008, verzoekschrift nr. 2872/02, § 47.

109 EHRM, *K.U. t. Finland*, § 48.

110 EHRM, *K.U. t. Finland*, § 49.

111 EHRM, *K.U. t. Finland*, § 49.

112 EHRM, *K.U. t. Finland*, § 50. Het Hof acht het niet noodzakelijk de klacht met betrekking tot artikel 13 EVRM te onderzoeken.

113 Wet van 18 juli 2009 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten in verband met het verbeteren en versterken van de vaststelling van de identiteit van verdachten, veroordeelden en getuigen (Wet identiteitsvaststelling verdachten, veroordeelden en getuigen) *Stb.* 2009: 317. Men leze *SC online*, 8 juli 2009; X 'Scherpere maatregelen tegen misbruik identiteit' *P& I*, 2009, nr. 5, blz. 241.

114 HvJ, 16 oktober 2008, C-298/07, *Mediaforum* 2008, 11/12, blz. 437-437. Zie De Jong en Erents 2009: 170; Pemmelaar 2009: 1-2.

115 Data Protection Conference organised by DG Justice, Freedom and Security, European Commission, 19-20 May 2009, Brussels http://ec.europa.eu/justice_home/news/events/news_events_en.htm The Conference webcast: http://webcast.ec.europa.eu

116 Zie over het verschil tussen kennis en reflectie en de vormen van kennis: Hermes 2008.

117 Over cynisme over de rol van de media en de hoge dosis zelfveronderstelde mediageletterdheid bij een groep Nederlandse respondenten Hermes 2008: 119.

118 Zie ook Selnow 1998; Goethals & Nelson 1973 aangehaald door D'Haenens 2003: 103. Vgl. ook Keen 2007.

119 Erg kritisch hierover in het licht van de sociale ongelijkheid Hartman 2008.

120 Cf. zijn bespreking van 'the idea of the public forum' (p. 22-26). Het recht om te betogen op straten en pleinen impliceert een plicht voor belastingbetalers om dit recht mogelijk te maken: "A distinctive feature to the public-forum doctrine is that it creates a right of speaker's access, both to places and to people. Another distinctive feature is that the public-forum doctrine creates a right (...) to ensure government subsidies of speech. There is no question that taxpayers are required to support expressive activity that, under the public-forum doctrine, must be permitted on the streets and parks" (blz. 23).

121 Sunstein spreekt over kranten als 'general interest intermediaries' en merkt op dat deze de taak als public forum beter vervullen dan traditionele pleinen en straten (blz. 29).

122 Stippen we aan dat er ethici zijn die vertrekkend vanuit eenzelfde analyse minder vergaande voorstellen formuleren en (slechts) oproepen tot lessen mediakritiek voor jongeren. Cf. "De invloed van het Internet op de normen en waarden van de volgende generatie wordt enorm. 90 procent van de Vlaamse jongeren is momenteel online. Driekwart van de 13-jarigen keek al naar porno. Daar moeten we in de toekomst rekening mee houden, vrees ik, want hoe je het draait of keert: dat zijn ook voorbeelden. Ik pleit voor lessen mediakritiek. We moeten jongeren leren hoe ze met die schitterende uitvinding internet om moeten gaan. Een kind is immers niet langer een kind. In de traditionele, achterhaalde visie was het een wezen dat niets kon en langzaam de wereld in werd gegidst door ouders en leraars. Dat gaat niet langer op. Een kind zit vanaf drie jaar voor tv en vanaf tien jaar op internet. Daar ziet het alles. De onschuldige kindertijd is verdwenen, maar dat is niet zo erg als het misschien klinkt, zolang we hen maar goed blijven begeleiden". Raes 2010: 34.

123 Met verwijzing naar onder meer EHRM, *Handyside t. Verenigd Koninkrijk*, 7 december 1976, *NJ* 1978, 236, § 49 en EHRM, *Sunday Times t. Verenigd Koninkrijk*, 26 april 1979, *NJB*, 1980, 146, § 66.

124 EHRM, *TV Vest As & Rogaland Pensjonistparti t. Noorwegen*, 11 december 2008, *NJ* 2010, 208, blz. 2031-2040, *Media Forum,* 2009, 3: 104-114, noot J.J.C. Kabel.

125 EHRM, *Appleby e.a. t. Verenigd Koninkrijk*, 6 mei 2003, *NJ* 2010, 207, blz. 2024-2031; *AB* 2004, 37, nr. 319.

126 Over de modellen van horizontale werking in Nederland, Duitsland, Frankrijk en België Van Leuven 2009: 187-279.

127 EHRM, *Appleby e.a. t. Verenigd Koninkrijk*, § 43.

128 EHRM, *Appleby e.a. t. Verenigd Koninkrijk*, § 49.

129 Cf. § 47: "That provision, (*Het Hof verwijst naar artikel 10 EVRM)* notwithstanding the acknowledged importance of freedom of expression, does not bestow any freedom of forum for the exercise of that right. While it is true that demographic, social, economic and technological developments are changing the ways in which people move around and come into contact with each other, the Court is not persuaded that this requires the automatic creation of rights of entry to private property, or even, necessarily, to all publicly owned property (government offices and ministries, for instance). Where, however, the bar on access to property has the effect of preventing any effective exercise of freedom of expression or it can be said that the essence of the right has been destroyed, the Court would not exclude that a positive obligation could arise for the State to protect the enjoyment of the Convention rights by regulating property rights. A corporate town where the entire municipality is controlled by a private body might be an example."

130 Wet van 29 december 2008, *Stb.* 583 (Mediawet 2008).

131 Vgl. het interview met ex-secretaris-generaal van Amnesty International Irene

Khan in G. Goris 'Ook bedrijven moeten de mensenrechten respecteren'. Interview met Irene Khan in *MO magazine*, 2010, 20-23 april. Deze mensenrechtenactiviste legt probleemloos de link tussen debatten over multinationals en debatten over de informatiemaatschappij. Er is geen natuurlijke volgorde van rechten die eerst moeten worden gerealiseerd. Alle rechten zijn belangrijk en 'informatiemaatschappij'-rechten zoals recht op openbaarheid en goede informatie kunnen ervoor zorgen dat in corrupte regimes beter omgesprongen wordt met hulpgelden. Ook Khan maakt zich om die reden zorgen wat er in de media verschijnt en wie dat controleert.

LITERATUUR

Baldor L.J. (2010) 'Experts say US must do more to secure the internet', The Associated Press http://www.washingtonpost.com/wp-dyn/content/article/2010/02/23/AR2010022304211.html

Brems, E. (2004) 'Europees Hof voor de Rechten van de Mens: Rechtspraakoverzicht 2003', *Tijdschrift voor Bestuurswetenschappen en Publiek Recht* 9: 575-577.

Bodard, K. (2001) 'Aansprakelijkheid van Internet Service Providers in Europees perspectief', blz. 285-331 in K. Byttebier, R. Feltkamp & E. Janssens, (red.), *Internet & Recht*, Antwerpen: Maklu.

Boel, L. de (2009) 'European Commission issues Recommendation on privacy in RFID applications', *Stibbe ICT Law Newsletter*, September 35: 5.

Blok, P.H. (2004) 'Inkomens, Internet en informationele privacy', *Nederlands tijdschrift voor Europees recht,* 1/2: 30-36.

Cohen-Jonathan, G. (1989) La *Convention européenne des droits de l'homme*, Parijs: Economica 375.

Cuijpers, C. (2008) 'Herziening Richtlijn 2002/58/EG', *Computerrecht* 4: 119.

Debusseré, F. (2009) 'Europa vernieuwt e-privacyregels', *De Juristenkrant*, december, 2.

Doorenbosch, Th. (2007) 'Mobieltje wordt kwetsbaarder. Telecomaanbieders voelen zich niet aangesproken', *Automatisering Gids* 48:3.

Dowty T. (2008) 'Overlooking children: an experiment with consequences', *Idis. Identity in the Information Society*, 1, 1: 109-121.

Dijk, P. van (1998) 'Positive obligations implied in the European Convention on Human Rights: are the states still the masters of the convention?' in M. Castermans-Holleman, Fr. van Hoof & J. Smith, J. (red.) *The Role of the nation-state in the 21st century. Human rights, international organisations and foreign policy. Essays in honour of Peter Baehr*, Den Haag: Kluwer Law International.

Eeten, M. van (2011) 'De baten van onveiligheid. Afwegingen rond de risico's van informatietechnologie' in *De staat van informatie,* WRR-verkenning 25, Den Haag: WRR.

Europese Commissie (2009) *Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification*, SEC 585, 12 mei 2009, C 3200 final, Brussel: Europese Commissie http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

Europese Commissie (2009) 'Kleine chips met een groot potentieel: nieuwe EU aanbevelingen zorgen ervoor dat barcodes van de 21ste eeuw privacy respecteren', IP/09/740, 12 mei 2009, Brussel: Europese Commissie europa.eu/rapid/pressReleasesAction.do?reference=IP/09/740

Esch, R. van (2001) 'Recente ontwikkelingen in het vermogensrecht op het terrein van de elektronische handel', *W.P.N.R.* 132: 379-381.

Finkielkraut, A. (2001) *Een stem van de overkant*, Amsterdam: Uitgeverij Contact.

Fuller, L. (1972) 'The Forms and Limits of Adjudication', *Harvard Law Review*, 92: 353 e.v.

Goris, G. (2010) 'Ook bedrijven moeten de mensenrechten respecteren', Interview met Irene Khan in *MO magazine*, 4:20-23.

Groothuis, M. (2009) 'Beschermen van minderjarigen op Internet. Annotatie bij EHRM, K.U. t. Finland', *NJCM-Bulletin* 3: 281-289.

Grijpink, J. (2006) 'Identiteitsfraude en overheid', *Justitiële verkenningen*, 32, 7: 37-57.

Gutwirth S., P. de Hert & L. de Sutter (2008) 'The trouble with technology regulation: Why Lessig's 'optimal mix' will not work', blz. 193-218 in R. Brownsword & K. Yeung (red.), *Regulating technologies: Legal futures, regulatory frames and technological fixes*, Oxford: Oxford University Press.

Haenens, L. d' (2003). ICT in de multiculturele samenleving, blz. 91-113 in *ICT en samenleving: de sociale dimensie van technologie*. Amsterdam: Boom.

Hartman I. (2008) 'Burgerschap en patronen van politieke participatie' blz. 133-158 in G. Alberts, M. Blankesteijn, B. Broekhans & Y. van Tilborgh (red.), *Burger in uitvoering. Jaarboek Kennissamenleving 2008*, Amsterdam: Aksant.

Hermes, J. (2008) 'Mediawijs, wars van politiek. Alledaags burgerschap in de kennissamenleving', blz. 109-132 in G. Alberts, M. Blankesteijn, B. Broekhans & Y. van Tilborgh (red.) *Burger in uitvoering. Jaarboek Kennissamenleving 2008*, Amsterdam: Aksant.

Hert, P. de (2004) 'Division of competencies between national and European levels with regard to Justice & Home Affairs' in J. Apap (red.) *Justice and Home Affairs in the EU. Liberty and security issues after enlargement,* Cheltenham: Edward Elgar Publishing Limited, blz. 55-102.

Hert, P. de (2009) *Citizens' data and technology. An optimist perspective*, Den Haag: Dutch Data Protection Authority.

Hert, P. de & W. Schreurs (2004) 'De bescherming van persoonsgegevens op het Internet: nuttige verduidelijking door de rechtspraak', 6 november 2003 (Bodil Lindqvist Zweden), *Auteurs & Media*, 2004/2: 127-138.

Hert, P. de & S. Gutwirth (2001) 'Editoriaal: Cassatie en geheime camera's. Meer gaten dan kaas', *Panopticon. Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk* 22, 4: 309-318.

Hert, P. de & R. Bellanova (2008) *Data protection from a transatlantic perspective: the EU and US move towards an International Data Protection Agreement?*, Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), Brussels, European Parliament, 2008.

Hert, P. de & K. Van Laethem (2008) 'Ondernemingen als nieuwe dragers van mensenrechtenplichten?' in J. Wouters & C. Ryngaert (red.) *Mensenrechten. Actuele brandpunten*, Leuven-Den Haag, Acco.

Hert P. de & A. Sprokkereef (2009) *The use of privacy enhancing aspects of biometrics. Biometrics as a PET (privacy enhancing technology) in the Dutch private and semi-public domain*, Tilburg: TILT http://www.uvt.nl/faculteiten/frw/onderzoek/tilt/frw/reportpets/sprokkereef.pdf

Hert, P. de & A. Sprokkereef (2009) 'Case study The Netherlands' in E. Kindt & L. Müller (red.) *The privacy legal framework for biometrics*, Fidis mei: 80-93, http://www.

fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf

Hins, H. (2010) 'Publieke media op Internet: zorgplicht en concurrentievervalsing', blz. 93-108 in L. Mommers et al. (red.), *Het binnenste buiten. Liber amicorum prof. dr. Aernout H.J. Schmidt*, Leiden: Leiden University Press.

Human Rights Council (2008) *Joint NGO statement to the eight session of the Human Rights Council*, http://www.hrw.org/en/news/2008/05/19/joint-ngo-statement-eighth-session-human-rights-council.

Jong, H. de & G. Erents (2009) 'Online Overeenkomstenrecht 2008-2009', *Tijdschrift voor Internetrecht* 6: 166-173.

Kaspersen, H. (2009) 'Internetveiligheid', *Computerrecht* 2009: 222.

Kindt, E. & L. Müller (red.)(2009) *The privacy legal framework for biometrics*, http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/fidis_deliverable13_4_v_1.1.pdf

Kindt, E. (2007) 'Biometric applications and the data protection legislation (The legal review and the proportionality test)' *Datenschutz and Datensicherheit* 31: 166-170.

Knapen, M. (2007) 'Groot privacyrisico RFID volgens Europa', *Overheid Innovatief* 8, 5: 18-20.

Koedooder, M. (2009) 'Slachtoffer van identiteitsfraude', 28 februari 2009, http://mkoedooder.devos.eu/?blogitem=225

Lawson, R. (1995) 'Positieve verplichtingen onder het EVRM: opkomst en ondergang van de faire balance-test' (deel 1), *NJCM-Bulletin* 5: 559-567.

Lawson, R. & L. Verheij (2002) 'Kroniek van de grondrechten 2002', *Nederlands Juristenblad* 77, 10: 513-523.

Leuven, N. van (2009) 'Mensenrechten en contracten: een geslaagd duo', *Tijdschrift voor Mensenrechten* 3: 11-14.

Liu, Y. (2009) 'The principle of proportionality in biometrics: Case studies from Norway', *Computer Law & Security Review*, 25: 237-250.

Lockton, V. & R. Rosenberg (2006) 'RFID: The next serious threat to privacy', *Ethics and Information Technology* 7: 221-231.

Lucas, A. (2001) 'La responsabilité civile des acteurs de L'internet', *Auteur&Media* 1: 42-52.

Net, C. van der (2002) 'De civielrechtelijke aansprakelijkheid van internetproviders na de Richtlijn elektronische handel', *JAVI* 1: 10-15.

Nys, H.,'Recente wetgeving ter bescherming van de persoon en de goederen van fysiek of mentaal gehandicapte personen', R.W. 1991-1992, 350-360.

Overkleeft-Verburg, G. (2004) Annotatie bij EU Hof van Justitie 6 november 2003, *Jurisprudentie Bestuursrecht* 114-116.

Pemmelaar, W. (2009) 'European Court of Justice rules that ISPs do not need to mention their telephone numbers on their website', *Stibbe ICT Law Newsletter* 33: 1-2.

Pop, V. (2010) 'Ripples of discontent as MEPs reject US bank data deal', EUobserver, http://euobserver.com/9/29455/?rk=1

Prins, J.E.J. (2010) 'Identiteitsfraude: verantwoordelijkheid nemen', *NJB* 9: 537.

Råman, J. (2008) 'European Court of Human Rights: failure to take effective information security measures to protect sensitive personal data violates right to privacy – I. v. Finland, no. 20511/03, 17 July 2008', *Computer Law & Security Report*, 24, 6:562-564.

Raes, K. (2010) in 'Geluk is een neveneffect' door Jef van Baelen, *Knack*, 14 april 2010: 34.

Renchon J.-L. (1994) 'La Convention européenne et la régulation des relations affectives et familiales dans une société démocratique' blz. 98-102 in P. Lambert (red.) *La mise en oeuvre interne de la convention européenne des droits de l'homme*, Brussel: Ed. du jeune barreau de Bruxelles.

Russo, L., M.M.V.P. Trichilo & F. Marotta (1995) 'Article 8, § 1' in *La Convention européenne des droits de l'homme. Commentaire article par article*, L.E. Pettiti, E. Decaux & P.H. Imbert (red.), Parijs: Economica, 308.

Schellekens, M. (2001) *Aansprakelijkheid van Internetaanbieders*, Den Haag: Sdu.

Schutter, O. de (2005) 'Reasonable accommodations and positive obligations in the European Convention on Human Rights' blz. 35-64 in A. Lawson & C. Gooding (red.), *Disability rights in Europe: from theory to practice*, Oxford: Hart.

Special Representative to the Secretary-General on Business and Human Rights (2008) *Protect, respect and remedy: a framework for business and human rights*, A/HRC/8/5.

Spindler G. (2007) *Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären: Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler*, Universität Göttingen: Bundesamt für Sicherheit in der Informationstechnik.

Sunstein C. (2001) *Republic.com*, Princeton, NJ: Princeton University Press.

Sutter, L. de & S. Gutwirth, (2004), 'Droit et cosmopolitique. Notes sur la contribution de Bruno Latour à la pensée du droit', *Droit et Société* 56-57: 259-289.

Tongue, C. (2009) 'Why a UNESCO Convention on Cultural Diversity of Expression', blz. 241-272 in C. Pauwels, H. Kalimo, K. Donders & B. Van Rompuy (red.), Rethinking European Media and Communications Policies, Brussel: VUB Press.

UN Sub-Commission on the Promotion and Protection of Human Rights (2003) *Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights*, 55th session, E/CN.4/Sub.2/2003/12/Rev.2.

UN Commission on Human Rights (2004) *Report to the economic and social council on the sixtieth session of the commission*, Resolution 2004/116, E/CN.4/2004/L.11/Add.7.

UN Commission on Human Rights (2005) *Human rights and transnational corporations and other business enterprises*, 61st session, Resolution 2005/69, E/CN.4/2005/L.87 (2005).

Vande Lanotte & Y. Haeck (2005) *Handboek EVRM: Deel I Algemene beginselen*, Antwerpen: Intersentia.

Voorhoof, D. (2009) 'Commercieel portretrecht in België', blz. 145-165 in D. Visser, R. van Oerle, J. Spoor et al. *Commercieel portretrecht*, Amsterdam: Uitgeverij deLex.

Voorhoof, D. (2009) 'Recente arresten van het EHRM in verband met artikel 10 EVRM

(vrijheid van meningsuiting en informatie) November-december 2008', *Auteurs & Media* 1-2: 113-127.

Vries, U. de, H. Tigchelaar, M. van der Linden & A. Hol (2007) *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*, WODC 271: 12.

Winkelhorst, C. & T. Van der Linden-Smith (2004) 'Persoonsgegevens op Internet. Een (ver)melding waard?', *Nederlands Juristenblad* 79, 12: 627-631.

3 OVERHEIDSVERANTWOORDELIJKHEID IN HET INFORMATIETIJDPERK: EEN PLEIDOOI VOOR HET CREËREN VAN GENORMEERDE EXPERIMENTEERRUIMTE

Albert Meijer

3.1 OVERHEIDSVERANTWOORDELIJKHEID IN HET INFORMATIETIJDPERK

Veel van de bestaande overheidstaken en instituties zijn ooit ontwikkeld in reactie op de uitwassen van de industriële revolutie. Grote delen van het staatsbestel vinden hun oorsprong in de negentiende en de vroege twintigste eeuw. Inmiddels zijn we ruim een eeuw verder en beland in het informatietijdperk. De snelle ontwikkeling van informatie- en communicatietechnologie en de enorme informatiestromen die hierdoor mogelijk zijn, vragen om een herijking van de historisch gegroeide invulling van de verantwoordelijkheden van de overheid. In dit essay probeer ik daarom op een systematischer manier na te denken over overheidsverantwoordelijkheden in het informatietijdperk. De centrale vraag van dit essay luidt als volgt:

Wat zijn de belangrijkste vraagstukken waar de overheid zich voor ziet geplaatst als het gaat om de invulling van haar verantwoordelijkheden op het gebied van informatie en technologie?

Deze algemene vraag werk ik uit in twee clusters van specifiekere vragen:

1 *Gebruiksverantwoordelijkheid*. Wat zijn de belangrijkste vraagstukken voor de overheid wanneer zij zelf informatietechnologie gebruikt? Hierbij gaat het vooral om de verantwoordelijkheid voor de inrichting en het functioneren van de overheidsorganisatie zelf. Hoe kan de overheid zelf informatietechnologie op een deugdelijke manier gebruiken? Wat betekent het bijvoorbeeld om op een verantwoorde manier om te springen met grote hoeveelheden gegevens over individuele burgers?
2 *Systeemverantwoordelijkheid*. Wat zijn de belangrijkste vraagstukken voor de overheid rondom de toepassing van informatietechnologie in de samenleving? In hoeverre dient de overheid te voorkomen dat maatschappelijke partijen misbruik maken van technologische mogelijkheden? Welke verantwoordelijkheid heeft de overheid voor het goed functioneren van internet en, meer in het algemeen, voor de bijdrage van informatie en technologie aan de welvaart van de samenleving?

Er zijn nog andere verantwoordelijkheden te benoemen. Zo zou men kunnen zeggen dat de overheid, als *launching customer*, ook een verantwoordelijkheid heeft voor technologische innovatie. Hoewel dit een interessant vraagstuk betreft, beperk ik dit essay op verzoek van de WRR tot de bovengenoemde vragen rondom gebruiksverantwoordelijkheid en systeemverantwoordelijkheid.

Dit essay levert inzicht op in de centrale vraagstukken die spelen bij de invulling van verantwoordelijkheden op beide niveaus. Mijn uitgangspunt is dat sociale wetenschappers technologiekritiek moeten bedrijven: een kritische bespreking van technologie kan de kwaliteit van de maatschappelijke keuzen over technologie verhogen (Winner 1986). Hoe dient de overheid ICT te gebruiken? Op welke manier kan de overheid waarborgen dat ICT een positieve bijdrage levert aan de samenleving? Waar liggen de dilemma's? Een identificatie van deze dilemma's vormt een startpunt voor een politiek en maatschappelijk debat over de invulling van de verantwoordelijkheden van de overheid in de informatiesamenleving. In de concluderende paragraaf formuleer ik een manier om met deze dilemma's om te gaan: ik pleit voor een genormeerde experimenteerruimte voor de overheid.

Vooraf wil ik benadrukken dat ik de tekortkomingen ken van de begrippen die ik in dit essay gebruik: '*de* verantwoordelijkheden' van '*de* overheid'. Ik ben me er van bewust dat de overheid geen eenheid is en veeleer bestaat uit een complex geheel van organisaties en functionarissen. Voor een preciezere analyse dient te worden gekeken naar de specifieke verantwoordelijkheden van deze concrete organisaties en functionarissen (zie onder andere Meijer 2009; Snijders 2011). Voor de politiek-theoretische analyse die ik wil uitvoeren kan een simplificatie van dit geheel tot 'de overheid' nuttig zijn om een startpunt te bieden voor de complexe discussie over overheidsverantwoordelijkheden.

3.2 VERANTWOORDELIJKHEID ALS TAAK, DEUGD, VERMOGEN EN AANSPRAKELIJKHEID

'Verantwoordelijkheid' is een begrip dat vaak en gemakkelijk wordt gebruikt in discussies over politiek en bestuur. Achter het begrip 'verantwoordelijkheid' gaan echter verschillende opvattingen schuil (Cooper 1990; Bovens 1990; Koppell 2005). Het is een *essentially contested concept*, dat vele invullingen kent die elk plausibel kunnen zijn, maar elkaar lang niet altijd verdragen (Bovens 1990: 29).

In mijn analyse zal aandacht worden besteed aan de volgende vormen van verantwoordelijkheid: verantwoordelijkheid als taak, verantwoordelijkheid als deugd, verantwoordelijkheid als vermogen en verantwoordelijkheid als aansprakelijkheid. Deze vormen zijn met elkaar verbonden: verantwoordelijkheid betreft de onderkenning van bevoegdheden en plichten, de intentie om deze

deugdelijk uit te voeren en het vermogen om dit ook te doen. Tekortschieten in het uitoefenen van verantwoordelijkheden zal kunnen leiden tot aansprakelijkheidsstelling. Deze verschillende vormen van verantwoordelijkheid werk ik hier verder uit.

Zorgt de overheid ervoor dat individuele rechten van burgers in het informatietijdperk zijn gewaarborgd? Bovens (1990: 33) geeft aan dat van *verantwoordelijkheid als taak* sprake is wanneer iemand een bepaalde sociale (of politieke) rol vervult, een ambt bekleedt of een taak of functie in een organisatie heeft toebedeeld gekregen waaruit niet alleen bevoegdheden voortvloeien maar ook plichten tegenover anderen (zie ook Hart 1968: 212). Deze bevoegdheden en plichten noemen we tezamen de verantwoordelijkheden van deze organisatie of persoon. In mijn analyse zal ik de taakverantwoordelijkheid gebruiken om te analyseren wat het domein is van de verantwoordelijkheid van de overheid voor informatie en technologie. Waarborgen van individuele rechten in het informatietijdperk is een van deze taken.

Gaan overheden op een juiste manier om met al deze nieuwe technologieën? Over *verantwoordelijkheid als deugd* schrijft Bovens (1990: 33) dat dit wijst op het serieus nemen van taken en plichten, op weloverwogen optreden en op het zich rekenschap geven van de gevolgen van het handelen voor anderen (zie ook Haydon 1978). Belangrijk bij het deugdelijk handelen is een adequate perceptie van en aandacht voor dreigende normschendingen. Omgang met technologie dient te zijn gebaseerd op onderkenning van mogelijke gevaren en afweging van onderling conflicterende normen en belangen. Ook is omgang met technologie verantwoord te noemen wanneer deze is gebaseerd op een morele code (en niet op emoties) en de code en omgang ermee voor buitenstaanders toetsbaar en begrijpelijk is. Barnard (1938: 263) benadrukt dat verantwoordelijkheid de macht van een specifieke morele code is om het gedrag van een individu te beheersen, terwijl er sterke verlangens of impulsen zijn om ander gedrag te vertonen.

In hoeverre kunnen overheidsorganisaties de mogelijkheid bieden om ervoor te zorgen dat technologische ontwikkelingen tot collectief wenselijke uitkomsten leiden? De overheid kan bevoegdheden en plichten onderkennen en deze op een deugdelijke manier willen uitvoeren, maar hiertoe toch niet in staat zijn. Bovens (1990: 32, 33) geeft aan dat het bij *verantwoordelijkheid als vermogen* gaat om het in staat zijn om verantwoordelijkheid uit te oefenen. Uitoefenen van verantwoordelijkheid in het informatietijdperk kan gecompliceerd zijn wanneer de snelle technologische ontwikkelingen het lastig, zo niet onmogelijk, maken om ontwikkelingen in de gewenste richting te sturen.

Bij de bovengenoemde vormen van verantwoordelijkheid gaat het om 'actieve' verantwoordelijkheid. De overheid kan hier zelf invulling aan geven. Daarnaast

kan de overheid door anderen verantwoordelijk worden gehouden voor zaken of gebeurtenissen. In dat geval is er sprake van passieve verantwoordelijkheid of *verantwoordelijkheid als aansprakelijkheid*. Hierbij kan het gaan om politieke, morele en/of juridische aansprakelijkheid (Bovens 1990: 32; Hart 1968: 215). In dit essay zal ik mij vooral richten op de politiek-bestuurlijke aansprakelijkheid. Kunnen politici en bestuurders aansprakelijk worden gesteld voor misstanden die voortvloeien uit het gebruik van nieuwe technologieën? Een analyse van juridische en morele aansprakelijkheden is belangrijk, maar valt buiten mijn expertise.

Met dit kader zal ik vraagstukken rondom de verantwoordelijkheden van de overheid in het informatietijdperk analyseren. Daarbij ga ik achtereenvolgens in op de gebruiksverantwoordelijkheid en de systeemverantwoordelijkheid van de overheid. In beide analyses staat één vorm van verantwoordelijkheid centraal en zijn de andere vormen van verantwoordelijkheid de basis voor een aanvullende analyse. Bij de gebruiksverantwoordelijkheid staat de verantwoordelijkheid als deugd centraal, bij de systeemverantwoordelijkheid vormt de verantwoordelijkheid als taak het startpunt van de analyse. Doel van deze analyse is, zoals eerder opgemerkt, het identificeren van vraagstukken op het gebied van verantwoordelijkheid.

3.3 GEBRUIKSVERANTWOORDELIJKHEID: VERANTWOORD GEBRUIK VAN ICT DOOR DE OVERHEID

Overheden gebruiken informatie en technologie voor de uitvoering van allerlei – misschien wel bijna alle – overheidstaken. ICT wordt gebruikt in de *backoffice* om gegevens te beheren, berekeningen uit te voeren, scenario's te ontwikkelen en beleid te ondersteunen. Ook in de *frontoffice*, de contacten tussen overheid en burgers en bedrijven, speelt vooral internet een centrale rol, maar ook de mobiele telefoon en allerlei mobiele applicaties worden steeds belangrijker. Daarnaast speelt ICT een essentiële rol in de afstemming van werkzaamheden tussen verschillende overheidsorganisaties in tal van *beleidsketens en netwerken*.

De vraag bij het gebruik van ICT door overheden is niet zozeer of overheden wel de juiste taken uitvoeren, maar veeleer of de instrumenten die zij gebruiken bij deze taakuitvoering adequaat worden gebruikt. De analyse richt zich daarmee allereerst op verantwoordelijkheid als deugd. Vervolgens zal ook gekeken worden naar het vermogen om dit te doen. Betoogd kan namelijk worden dat de grip die de overheid kan hebben op technologische dynamiek zeer beperkt is. Wat kan de overheid wel en wat niet? En ten slotte zal kort worden ingaan op de aansprakelijkheid van politici en bestuurders. We verkennen daarbij de toenemende frictie tussen de behoefte aan rechtsstatelijke stabiliteit en hoge technologische turbulentie.

3.3.1 VERANTWOORDELIJKHEID ALS DEUGD: LEGAAL, NEUTRAAL, BEHOORLIJK EN TRANSPARANT GEBRUIK VAN ICT DOOR DE OVERHEID

De criteria voor verantwoord overheidsoptreden kunnen ontleend worden aan de gangbare eisen van de rechtsstaat. In de afgelopen twee eeuwen is, in reactie op de groei in aard en omvang van het overheidsoptreden, ook het stelsel van rechtsstatelijke normen en beginselen sterk uitgebreid en dit stelsel is nog steeds in beweging. De verschillende lagen, instituties en beginselen van de moderne rechtsstaat zijn door Bovens (2003) weergegeven in het 'huis van de rechtsstaat' (zie ook Van Klink & Witteveen 2002). Uit dit 'huis' kunnen vier criteria afgeleid worden voor een verantwoord gebruik van ICT door de overheid:

1 *Legaal bestuur*. De basis voor verantwoord gebruik van ICT is de wet. Van belang zijn hier meer specifiek het materieel wetsbegrip, de rechtszekerheid, de rechtsgelijkheid, *nulla poena* (geen straf zonder wettelijke grond) en het verbod op terugwerkende kracht van nieuwe wetten.
2 *Neutraal bestuur*. Aanvullend kan ook van de overheid worden geëist dat er geen sprake is van vooringenomenheid. Van belang zijn het primaat van de politiek, de ambtelijke neutraliteit en de scheiding van beleid en uitvoering.
3 *Behoorlijk bestuur*. Een modernere eis aan de overheid is dat bestuur ook behoorlijk is. Hiertoe zijn de beginselen van behoorlijk bestuur geformuleerd en ook de eisen van de Nationale Ombudsman over behoorlijkheid.[1]
4 *Transparant bestuur*. Een eis die is geformuleerd naar aanleiding van een beschouwing van de positie van de overheid in een samenleving waar informatie van steeds groter belang is, is de eis van transparantie. Kenbaarheid van de wet en ook inzicht in relevante informatie is cruciaal.

Op basis van een nader onderzoek van deze vier criteria kunnen verschillende dilemma's en knelpunten worden geïdentificeerd.

Legaal bestuur: rechtsgelijkheid versus effectiviteit

Een interessant punt bij de legaliteit is het waarborgen van de rechtsgelijkheid van burgers. Daarbij spelen allereerst onbedoelde verdelingseffecten een rol. Wanneer overheden via nieuwe media communiceren, kunnen zij alleen communiceren met de burgers die toegang hebben tot deze media en deze media effectief kunnen gebruiken. De 'digitale kloof' lijkt voor een groot deel geslecht nu bijna iedereen snelle toegang heeft tot internet. Recent onderzoek van Van Deursen en Van Dijk (2008) laat echter zien dat het vermogen om gebruik te maken van deze voorzieningen sterk uiteen loopt: hoogopgeleide burgers zijn veel beter in staat om gebruik te maken van deze nieuwe mogelijkheden om informatie te verkrijgen.

Een belangrijke bedreiging voor de rechtsgelijkheid is ook het toenemende gebruik van *profilering* op basis van gegevens in grote databanken (Custers 2003; Hildebrandt & Gutwirth 2008). Profilering kan worden gebruikt om risicovolle

groepen en risicovolle gedragspatronen te identificeren. Op basis van deze risicoanalyses maakt de politie bijvoorbeeld keuzen over de inzet van schaarse capaciteit. Een dergelijke aanpak is vanuit managementoverwegingen goed te begrijpen en wellicht zelfs toe te juichen, maar heeft consequenties voor de rechtsgelijkheid van burgers. Het kan bijvoorbeeld betekenen dat een Nederlander die in Marokko is geboren een grotere kans heeft om te worden gecontroleerd aan de grens dan een Nederlander die in Gelderland is geboren.

Vooral de spanning tussen gelijke behandeling en intelligente segmentering van burgers roept spanningen op. In welke mate kan met profilering worden gewerkt? Belangrijk hierbij lijkt dat profilering op basis van *gedrags*kenmerken (bijvoorbeeld: deze persoon reist vaak naar Zuid-Amerika) een ander karakter heeft dan profilering op basis van *persoons*kenmerken (bijvoorbeeld: deze persoon is in Marokko geboren). Profilering op basis van gedragskenmerken is al staande praktijk bij de Belastingdienst en lijkt minder problematisch vanuit het criterium van rechtsgelijkheid (al kunnen bepaalde specifieke gedragskenmerken – kerkbezoek, halal eten, enzovoorts – wel worden beschouwd als persoonskenmerken en dient de overheid hier dus voorzichtig mee om te gaan).

Ook het gebruik van gegevens voor nieuwe doeleinden kan leiden tot vragen over de rechtsgelijkheid. Oud-minister Hirsch Ballin heeft voorgesteld om biometrische gegevens van migranten ook te gebruiken voor opsporing (zie ook Brouwer 2009). Van migranten zijn immers de vingerafdrukken opgeslagen en deze zouden kunnen worden gebruikt om criminelen te vinden. Het gevolg van een dergelijk gebruik is dat de opsporingskans van een criminele migrant groter is dan van een crimineel die in Nederland is geboren. Principes van rechtsgelijkheid worden daarmee ondergeschikt gemaakt aan de effectiviteit van de opsporing.

Neutraal bestuur: verambtelijking versus politisering

De overheid heeft de taak ervoor te zorgen dat de formulering van algemene principes op basis van politieke besluitvorming en de uitvoering hiervan op basis van technische expertise en kennis over regelgeving worden gescheiden om enerzijds willekeur en anderzijds technocratie te voorkomen. De scheiding tussen politieke en ambtelijke macht is een centraal element in ons staatsbestel.

Nu laat de literatuur over de betekenis van het gebruik van ICT voor het openbaar bestuur zien dat deze scheiding wordt uitgedaagd (Snellen & Van de Donk 1998). Twee risico's doen zich voor:

1 *Verambtelijking van de politiek*. Het complexe ontwikkelingstraject van informatiesystemen bevat allerlei politieke keuzen. De complexiteit hiervan belemmert echter politieke betrokkenheid bij deze keuzen. Ambtenaren en systeemontwikkelaars maken daardoor in deze trajecten politieke keuzen, zonder dat zij over deze keuzen politieke verantwoording afleggen. Meijer (2009) laat zien

hoe de ontwikkeling van informatiesystemen in het migratiebeleid al sterk verambtelijkt is.

2 *Politisering van de ambtenarij*. Een ander, en zelfs contrasterend, risico is dat het gebruik van ICT de mogelijkheid biedt voor politici om zich op microniveau bezig te houden met beleidsuitvoering. Willems (2009) laat zien hoe de Tweede Kamer zeer nauw betrokken was bij keuzen omtrent de taaltoets voor immigranten. Deskundige uitvoering van algemene politieke keuzen werd belemmerd door directe politieke betrokkenheid.

De overheid staat voor de taak om een nieuwe invulling te geven aan de scheiding tussen politieke besluitvorming en ambtelijke uitvoering. Oude *checks and balances* voldoen niet meer (De Mulder 1998; Bovens 1999). Door verschillende wetenschappers zijn voorstellen gedaan voor aanvullingen op de bestaande instituties. Soms gaat het hierbij om versterking van reeds bestaande organen zoals het College bescherming persoonsgegevens (Brouwer 2009). Andere zijn radicaler in hun voorstellen: De Mulder (1998) pleit voor een 'tetras politica' in de vorm van een 'monitorende macht': toezicht op grootschalige uitoefening van macht door overheden. Zelf zie ik de afnemende scheiding als ten dele onontkoombaar en wil ik pleiten voor een lerende benadering waarbij continue reflectie op de uitkomsten van technologisch ondersteunde beleidsuitvoering wordt ingebouwd in besluitvormingspraktijken. Complexiteit kan niet vooraf worden beheerst, maar op de wenselijkheid van uitkomsten van het gebruik van complexe technologische systemen kan wel worden gereflecteerd.

Behoorlijk bestuur: efficiency versus behoorlijkheid

De uitvoering van wet- en regelgeving moet voldoen aan de eisen van behoorlijk bestuur. Bij de Algemene Beginselen van Behoorlijk Bestuur gaat het om beginselen die aanvankelijk door de rechter zijn ontwikkeld om het gedrag van de overheid ten opzichte van de burger te reguleren, zoals zorgvuldigheid, motivering, rechtszekerheid, gelijkheid, vertrouwen, fair play en gebruik van de bevoegdheden alleen voor de gegeven doelen (In 't Veld & Koeman 1979; Groothuis 2009). De Nationale Ombudsman (2009) heeft hier normen aan toegevoegd op het gebied van zorgvuldige bejegening zoals administratieve nauwkeurigheid, actieve en adequate informatieverstrekking en adequate organisatorische voorzieningen. Daarmee is een breed palet aan criteria ontstaan waaraan het gedrag van de overheid wordt getoetst.

Aanvullend heeft Franken (1993) specifiek voor informatievoorziening principes van behoorlijke informatisering geformuleerd (zie ook Groothuis 2005). Het gaat hierbij om principes zoals vertrouwelijkheid (bescherming van de persoonlijke levenssfeer), integriteit (juistheid, volledigheid en actualiteit van de gegevens) en authenticiteit (geldigheid van de informatie en de mogelijkheid van verificatie bij de bron). Deze principes reguleren en ordenen het informatieverkeer tussen

burgers, bedrijven en de overheid en zorgen voor 'veilige' en behoorlijke elektronische relaties.

Voor dit essay gaat het te ver om systematisch al deze behoorlijkheidsvereisten af te lopen. Dat zou een apart essay vergen. Wel wil ik privacy als centraal aandachtspunt belichten om zo spanningen rond de verantwoordelijkheden van overheden aan te geven. De hoeveelheden gegevens over burgers die door overheden worden opgeslagen nemen steeds verder toe en roepen in toenemende mate weerstand op. De voorgestelde introductie van het Elektronisch Patiëntendossier laat duidelijk zien dat er vragen leven rondom de vertrouwelijke omgang met deze gegevens.

Dilemma's kunnen hier vooral ontstaan op grond van de volgende patronen:
- Technologische mogelijkheden kunnen leiden tot groeiende behoorlijkheidseisen. Afspraken over behandelingstermijnen, bijvoorbeeld, kunnen onder druk komen te staan, doordat burgers een snellere afhandeling gewend raken. De eisen omtrent administratieve nauwkeurigheid, bijvoorbeeld in de omgang met gegevens van patiënten en migranten, zullen toenemen.
- De behoorlijkheid van het overheidsbestuur is in toenemende mate gebonden aan het karakter van het medium. Wetgeving over de digitale handtekening (Groothuis & Van der Hof 2009) en het verlenen van digitale beschikkingen (Groothuis 2005) verhoogt de behoorlijkheid van het bestuur, maar kan ook vragen oproepen over het vertrouwen in de overheid wanneer hackers deze systemen weten te breken.
- De mogelijkheden van efficiency- en effectiviteitswinst zullen de behoorlijkheid van overheidsbestuur onder druk kunnen plaatsen. Koppelingen van databanken en hergebruik van gegevens voor nieuwe doelen worden gepresenteerd als belangrijke manieren om de veiligheid te versterken, maar zijn in strijd met beginselen zoals gebruik van bevoegdheden voor de gestelde doelen en vertrouwelijkheid (Broeders 2010). Woodward et al. (2001) spreken in een dergelijk geval van *function creep*: gegevens die zijn verzameld voor het ene doel worden – onbedoeld en soms ongeautoriseerd – gebruikt voor een ander doel.

Net als bij de bovenstaande dilemma's lijkt het hier ook weer te gaan om het zoeken naar een juiste balans tussen privacy en collectief belang, tussen zorgvuldigheid en effectiviteit, tussen openheid voor nieuwe media en keuze voor systemen die hebben bewezen dat ze te vertrouwen zijn. De verlokking van de technologie lijkt hierbij de balans te doen doorslaan richting effectiviteit en nieuwe technologie.

Transparant bestuur: balanceren tussen openheid en beslotenheid

President Obama heeft transparantie tot een van de kernpunten gemaakt van zijn beleid: via transparantie hoopt hij het vertrouwen van de burger in de overheid te herstellen. In Nederland is er ook veel aandacht voor het vergroten van de trans-

parantie van de overheid en daarbij wordt met name gewezen op de mogelijkheden van internet. Een transparant bestuur houdt in dat de overheid de plicht heeft om burgers te voorzien in informatie die in handen is van de overheid en cruciaal is voor het maatschappelijk functioneren van burgers (Bovens 2003: 99). Daarbij gaat het allereerst om alle informatie die behulpzaam kan zijn bij het vaststellen van de juridische positie van de burger als onderdaan. Daarnaast is beleidsinformatie belangrijk vanuit het perspectief van de burger als citoyen. Deze informatie biedt burgers de mogelijkheid om deel te nemen in publieke besluitvorming. Verder kunnen openbare informatieverzamelingen de burger als maatschappijlid in staat stellen om zijn sociaal-economische positie te versterken.

Belangrijk is ook dat burgers inzicht kunnen hebben in de informatie die over hen is opgeslagen in databases. Brouwer (2009) laat zien dat het voor migranten vaak lastig is om te achterhalen op basis van welke informatie overheden hen op een bepaalde manier behandelen (bijvoorbeeld toegang tot een land weigeren). Het is cruciaal om deze vorm van transparantie niet alleen formeel te regelen, maar er ook voor te zorgen dat burgers op de hoogte zijn van het bestaan van de verschillende databanken en eenvoudige mogelijkheden hebben om een verzoek in te dienen tot inzage in de registraties in deze databanken.

Daartegenover zijn er ook belangen die beperkingen kunnen stellen aan deze openbaarmaking (Bovens 2003: 100, 101). Openbaarmaking dient de privacy van burgers en het bedrijfsgeheim niet te schaden. Daarnaast kunnen overwegingen van staatsveiligheid, diplomatieke belangen, de ongestoorde opsporing van strafbare feiten, en financiële belangen redenen zijn om de openbaarheid te beperken. Verder kan de interne besluitvorming geschaad worden wanneer interne beraadslagingen volledig en tot individuele personen herleidbaar naar buiten worden gebracht. De Commissie Toekomst Overheidscommunicatie (2001) pleitte ooit voor ruimte voor een zekere mate van 'beleidsintimiteit': ambtenaren dienen een zekere ruimte te hebben in vroege fasen van beleidsprocessen om ideeën te kunnen ontwikkelen en bespreken zonder dat deze besprekingen openbaar gemaakt kunnen worden. Een te grote nadruk op openbaarheid zou volgens de commissie de kwaliteit van het openbaar bestuur kunnen schaden doordat ideeën in de kiem worden gesmoord.

Dilemma's ontstaan in het spanningsveld tussen rechtvaardigheidsgronden voor openbaarmaking en belangen om dit niet te doen:

– Openbaarmaking van financiële gegevens stelt de burger in staat democratische besluitvorming te controleren, maar kan tegelijkertijd het financieel belang van de overheid schaden. Dit dilemma speelt onder andere rondom overheidsaanbestedingen.
– Openbaarmaking van gegevens over beleidsontwikkeling stelt de burger in staat om te participeren in publieke besluitvorming, maar kan tegelijkertijd de

ruimte inperken die ambtenaren nodig hebben om creatieve oplossingen voor maatschappelijke problemen te zoeken.
– Openbaarheid van persoonlijke gegevens stelt burgers in staat om zich adequaat te verweren tegen aantijgingen, maar tegelijkertijd hebben inlichtingendiensten een legitiem belang om gegevens geheim te houden om zo de landsveiligheid beter te kunnen beschermen.

Een deugdelijke invulling van de gebruiksverantwoordelijkheid van de overheid betekent het zoeken naar de juiste balans in deze dilemma's. Maatschappelijk – en ook juridisch – wordt bepaald wat wordt gezien als een juiste balans.

3.3.2 VERANTWOORDELIJKHEID ALS VERMOGEN: NIEUWSTE MOGELIJKHEDEN BENUTTEN OF KIEZEN VOOR OUDE ZEKERHEDEN?

Gebruik van ICT door overheden roept dus allerlei normatieve vragen op. Een overkoepelende vraag betreft verantwoordelijkheid als vermogen: kunnen overheden wel een deugdelijke invulling geven aan het gebruik van ICT? Overheden gebruiken technologieën die zij zeker niet volledig kennen en waarbij ook geldt dat de ontwikkeling van deze technologieën op verre plaatsen plaatsvindt en nauwelijks kan worden gestuurd. Is de overheid eigenlijk wel in staat om te zorgen voor een legaal, neutraal, behoorlijk en transparant bestuur? Vragen over verantwoordelijkheid als vermogen vloeien vooral voort uit de grote dynamiek van de technologische ontwikkelingen.

Een mooi voorbeeld van problemen bij de invulling van de gebruiksverantwoordelijkheid vormt Overheid.nl. Deze *portal* werd opgezet om de transparantie van de overheid te vergroten door burgers via een website toegang te geven tot alle informatie van de overheid. Het ontwikkelen van deze portal was een enorme klus die allerlei vormen van afstemming tussen overheidsorganisaties vroeg en daardoor veel tijd vergde. Toen Overheid.nl eenmaal was gelanceerd bleek deze echter nauwelijks te worden gebruikt: burgers bleken niet via een portal naar informatie te zoeken maar via zoekmachines, met name Google. De poging om transparantie te creëren met nieuwe technologieën was daarmee al snel achterhaald door de dynamiek van internet.

Naast de grote technologische dynamiek beperkt ook de internationale samenwerking de mogelijkheden voor Nederlandse overheden om invulling te geven aan gebruiksverantwoordelijkheden. Meijer (2009) laat zien hoe de Europese samenwerking in informatiesystemen op het gebied van migratie betekent dat nationale overheden de kwaliteit van deze systemen niet meer kunnen waarborgen (zie ook Broeders 2011). Kan de Nederlandse overheid nog wel een invulling geven aan haar gebruiksverantwoordelijkheid voor ICT wanneer deze technologie voor een groot deel wordt ingevuld door organen buiten Nederland?

Een specifiek probleem bij het vermogen tot verantwoord gebruik van ICT betreft de groeiende rol van bedrijven en consultants (zie ook Broeders 2011). Dit probleem doet zich op verschillende manieren voor. In de systeemontwikkeling spelen bedrijven een sleutelrol en daarmee moet worden onderkend dat de expertise van overheden lijkt af te nemen. De vraag is of overheden wel voldoende in staat zijn om het opdrachtgeverschap goed in te vullen. Dit leidt tot problemen om de verantwoordelijkheid te kunnen nemen voor de resulterende systemen. Een volgend probleem doet zich voor bij het beheer van de systemen dat ook in toenemende mate wordt uitbesteed aan private bedrijven. Ook hierbij geldt dat een contract nooit uitputtend kan worden ingevuld en er dus problemen ontstaan voor het vermogen van overheden om de verantwoordelijkheid te nemen voor het beheer. Samenwerking met bedrijven is zowel bij de ontwikkeling als het beheer noodzakelijk, omdat al de benodigde kennis niet aanwezig is bij overheden. Ook leidt dit tot efficiencywinst. De kosten die hier tegenover staan kunnen vooral worden uitgedrukt in termen van een toenemende mate van afhankelijkheid en het risico dat slecht functionerende bedrijven het deugdelijk gebruik van ICT door overheden ondermijnen (en kunnen leiden tot aansprakelijkheidsstelling van overheden).

Concreet kunnen we hier kijken naar de mogelijkheden die overheden hebben om privacy te garanderen en gegevens adequaat te beschermen. Kunnen gemeenten voorkomen dat databases worden gehackt? Van overheidsorganisaties kan worden geëist dat zij gebruikmaken van de hoogste standaarden. Toch is het echter ook mogelijk dat deze standaarden niet voldoende blijken te zijn. In een dergelijke situatie is de overheid in sterke mate afhankelijk van (private/technologische) ontwikkeling(en) op het gebied van gegevensbescherming. Ontwikkelen Norton en McAfee adequate beschermingssoftware? Voorkomt Microsoft *bugs* in haar software? De afhankelijkheid van overheden van deze private bedrijven betreft de verwerking van informatie en raakt daarmee de kern van het functioneren van overheden. Deze afhankelijkheid kan het vermogen tot een deugdelijke gebruiksverantwoordelijkheid beperken.

Een andersoortig probleem rondom het vermogen tot verantwoord gebruik van ICT betreft het aansturen van informatisering. De Algemene Rekenkamer (2007) heeft aangegeven dat overheden vaak te grote verwachtingen koesteren over de mogelijkheden van informatiesystemen. Overheden willen te veel en te snel. En daarbij wordt vaak ook nog gekozen voor de allernieuwste technologie die zich nog niet heeft bewezen. Op deze manier overvragen overheden de ontwikkelaars van technologie. De Algemene Rekenkamer laat helder zien dat dit in vele gevallen leidt tot mislukte projecten van informatisering.

Bij het gebruik van technologie bestaat er een principiële spanning. Niet gebruiken van nieuwe technologieën leidt wellicht tot het voorkomen van nieuwe risico's,

maar tegelijkertijd tot een onderbenutting van mogelijkheden. Het wel gebruiken van technologieën leidt tot nieuwe mogelijkheden, maar ook tot nieuwe risico's. Het dilemma is hier dat een traditionele invulling (nadruk op papier, nadruk op eenheid van staat en territorium, nadruk op primaat van hogere bestuursorganen) zich het meest bewezen heeft als deugdelijke invulling van gebruiksverantwoordelijkheid, maar tegelijkertijd tekort lijkt te schieten wanneer het gaat om de snel veranderende samenleving. De enige manier om hiermee om te gaan is een rigoureuzere invulling van een lerende omgang met technologie. Naast bestaande controles dienen openbare reflectiemomenten te worden ingebouwd. Signalen zoals evaluaties, klachten en rechtszaken moeten actief worden verwerkt en deze informatie moet de input vormen voor een politieke en publieke monitoring van technologische systemen. Publieke besluitvorming kan zich niet beperken tot ex ante sturing, maar zal steeds meer het karakter moeten krijgen van ex post monitoring (Meijer 2009).

3.3.3 VERANTWOORDELIJKHEID ALS AANSPRAKELIJKHEID: VERGROTEN VAN EFFECTIVITEIT OF MINIMALISEREN VAN RISICO'S?

De beschikbaarheid van technologie plaatst overheden in een zeer lastige situatie: zowel door ICT wel te gebruiken als door deze niet te gebruiken kunnen overheden tekortschieten. Bestaat de mogelijkheid dat dit leidt tot problemen rond de politieke en bestuurlijke aansprakelijkheid? Recente en minder recente ervaringen met uitvoeringsproblemen op het gebied van belastingen, studiefinanciering (Zouridis 2000) en immigratie (Dijstelbloem & Meijer 2009) laten zien dat gebrekkig functionerende technologie kan leiden tot politieke problemen voor de verantwoordelijke bestuurders. Problemen met de uitkering van toeslagen leidden tot een vloed aan Kamervragen en zelfs tot het vertrek van de hoogste ambtenaar van het ministerie van Financiën.

Bij de politieke en bestuurlijke aansprakelijkheid voor de gebruiksverantwoordelijkheid gaat het vooral om de vraag welke verwachtingen burgers hebben over de invulling van deze verantwoordelijkheid. Daarbij lijken de algemene normen – transparant, behoorlijk, legaal en neutraal bestuur – nog steeds te worden onderschreven. Wel kan het steeds lastiger worden om hier een invulling aan te geven: de verwachtingen van burgers kunnen hoger zijn dan wat de overheid kan waarmaken (Noordegraaf 2004: 57). En als de technologie meer mogelijk maakt kunnen de verwachtingen van burgers navenant stijgen. Bij dit vermogen bestaat het risico dat politici en bestuurders in toenemende mate aansprakelijk worden gehouden voor de frictie tussen de behoefte aan rechtsstatelijke stabiliteit en de grote technologische turbulentie.

De recente ervaringen van politiekorpsen in het oosten van het land vormen een mooi voorbeeld van dit spanningsveld (*de Volkskrant*, 29 januari 2010). Acht korp-

sen in het noorden en oosten van het land konden gedurende enkele weken slechts beperkt gebruikmaken van informatiesystemen. Deze bedrijfsprocessensystemen waren eerder geïntroduceerd om de effectiviteit en de efficiency van de politie te verhogen en de samenwerking te faciliteren door de invoer van gegevens te standaardiseren en de beschikbaarheid van informatie te vergroten. Uitval van de systemen leidde er echter toe dat agenten moeilijk aangiften van burgers konden invoeren en zelfs cruciale gegevens over gezochte criminelen niet konden achterhalen. De oorzaak van de storing leek nogal triviaal: bij de verandering van de zogenaamde *serverpack* is een programmaatje niet meegenomen en daardoor sloegen alle servers van de politie op hol. Dit voorbeeld laat allereerst zien dat overheden voor een lastig spanningsveld staan: geen gebruikmaken van informatiesystemen bij de uitvoering van taken leidt tot een afname van effectiviteit, maar gebruik van deze voorzieningen leidt tot grote afhankelijkheden. Deze afhankelijkheden blijken door de korpsen zelf moeilijk te kunnen worden beheerst: de korpsen zijn afhankelijk van de Voorziening tot Samenwerking Politie Nederland (VtSPN). Burgers verwachten van de politie dat dergelijke fouten niet worden gemaakt en daarom is er in dit geval zeker sprake van risico's voor de politiek-bestuurlijke aansprakelijkheid. Van politici en ambtenaren wordt verwacht dat informatisering probleemloos tot verbeteringen leidt.

Een manier om de risico's van politiek-bestuurlijke aansprakelijkheid te beperken is het vermijden van vernieuwende vormen van technologiegebruik. De Algemene Rekenkamer (2007) pleit er daarom voor dat de overheid vaker kiest voor *proven technology* en zich behoudend opstelt bij het gebruik van nieuwe mogelijkheden. Risicomijding dus. Dit is een beproefde manier om de risico's van politiek-bestuurlijke aansprakelijkheid te beperken, maar levert tegelijkertijd het risico op dat de overheid ervan wordt beschuldigd nieuwe mogelijkheden niet te benutten. In het algemeen zal echter het niet gebruiken van nieuwe mogelijkheden minder grote risico's opleveren dan het wel gebruiken van deze mogelijkheden. Of een dergelijke houding wenselijk is, is iets anders. Ik vrees dat een dergelijke strategie zal leiden tot een overheid die niet van grote fouten kan worden beschuldigd, maar als gevolg daarvan zal inleveren op mogelijk realiseerbare winsten op het gebied van effectiviteit en efficiency.

3.3.4 BELANGRIJKSTE VRAAGSTUKKEN BIJ GEBRUIKSVERANTWOORDELIJKHEID VOOR ICT

Onze analyse van de literatuur en de vertaling van nieuwe ontwikkelingen naar normatieve vragen vormt de basis voor de beantwoording van de eerste deelvraag. De volgende vraag was geformuleerd: wat zijn de belangrijkste vraagstukken als het gaat om de invulling van verantwoordelijkheden van de overheid bij eigen gebruik van informatietechnologie? De volgende (veelal samenhangende) vraagstukken zijn geïdentificeerd:

- *Rechtsgelijkheid versus effectiviteit.* Nieuwe systemen bieden mogelijkheden om de effectiviteit van de overheid te versterken. Vaak is dit natuurlijk alleen maar wenselijk, maar in specifieke gevallen kan dit tot problemen leiden. Vooral inzet van ICT in de opsporing roept de vraag op of de rechtsgelijkheid niet wordt bedreigd door profilering en koppeling van databases.
- *Verambtelijking versus politisering.* Besluitvorming over complexe technologieën roept nieuwe vragen op over de verhouding tussen ambtelijke en politieke besluitvorming. Nieuwe checks and balances lijken nodig te zijn en meer nadruk op de invulling van ex post leerprocessen.
- *Efficiency versus behoorlijkheid.* Informatiesystemen worden veelal toegepast om de interne efficiency te versterken, maar kunnen daarmee de behoorlijkheid van contacten tussen overheid en burgers bedreigen. Principes voor behoorlijke informatisering zijn geformuleerd, maar toepassing hiervan lijkt nog beperkt (mede doordat dit de efficiency zou kunnen verkleinen).
- *Openheid versus beslotenheid.* De nieuwe technologieën creëren allerlei mogelijkheden om de openbaarmaking te versterken. Er zijn echter ook andere redenen dan kosten om de openbaarmaking te beperken. De nieuwe mogelijkheden roepen echter wel nieuwe vragen op over openbaarmaking, zeker ook omdat openbaarheid in het internetgedrag van burgers een nieuwe betekenis lijkt te krijgen.
- *Nieuwe mogelijkheden versus oude zekerheden.* Het informatietijdperk vraagt om een hoge mate van flexibiliteit en dit wringt met de traditionele nadruk op stabiliteit. Ambtelijke molens werken traag, terwijl internet juist informatie verwerkt met de snelheid van het licht. Niet benutten van nieuwe mogelijkheden leidt tot het missen van kansen, terwijl wel benutten ervan nieuwe risico's oproept.

Deze vraagstukken zijn niet nieuw, maar krijgen een nieuwe invulling in het informatietijdperk. Technologieën creëren nieuwe mogelijkheden en leggen ook een accent op andere waarden. Het instrumentele en institutionele karakter van de technologieën leidt tot principiële vragen aangaande de invulling van de gebruiksverantwoordelijkheden van de overheid.

3.4 SYSTEEMVERANTWOORDELIJKHEID: OVERHEIDSVERANTWOORDELIJKHEID VOOR ICT IN DE SAMENLEVING

Een steeds groter deel van het maatschappelijk leven speelt zich af in de virtuele wereld. Burgers interacteren met elkaar op internet en daar vinden ook allerlei misstanden plaats zoals diefstal en identiteitsfraude. Daarnaast is de maatschappelijke afhankelijkheid van internet enorm. Velen van ons merken dat direct wanneer het netwerk even uit de lucht is en er niet meer kan worden ge-e-maild en gesurft. Wat betekent dat voor overheidsverantwoordelijkheden? In tegenstelling tot de voorgaande paragraaf is voor de analyse van de systeemverantwoordelijkheid van

de overheid 'taakverantwoordelijkheid' juist wel het centrale begrip. De taken zijn hier immers niet gegeven, maar zijn afhankelijk van het antwoord op de vraag of de overheid een systeemverantwoordelijkheid heeft voor ICT in de samenleving.

3.4.1 VERANTWOORDELIJKHEID ALS TAAK: BURGERS BESCHERMEN EN OPLOSSINGEN VOOR SYSTEEMFALEN

In het algemeen kan worden gesteld dat de overheid burgers dient te beschermen tegen externe bedreigingen en problematische situaties die ontstaan door systeemfalen dient op te lossen. Daarbij merkt Van Eeten (2011) terecht op dat bij bescherming keuzen moeten worden gemaakt over wie waartegen wordt beschermd. In deze algemene beschouwing zal ik echter geen onderscheid maken tussen groepen burgers (net zomin als ik een onderscheid heb gemaakt tussen verschillende overheden). Het benoemen van bescherming van burgers tegen externe dreigingen zoals cybercriminaliteit en het oplossen van systeemfalen zoals het uitvallen van internet als systeemverantwoordelijkheden van de overheid roept ook direct een vervolgvraag op: op welke terreinen dient de overheid burgers te beschermen en oplossingen aan te dragen voor systeemfalen? We verkennen daarbij de volgende domeinen:

- Welke systeemverantwoordelijkheid heeft de overheid voor het bestaan van een ICT-infrastructuur?
- Welke taken heeft de overheid rondom het gebruik van de technologische infrastructuur voor informatie-uitwisseling?
- Welke verantwoordelijkheden heeft de overheid voor de inhoud van de digitale informatie in het publieke domein?

Nadat deze vragen zijn beantwoord bespreek ik ook de andere aspecten van verantwoordelijkheid. Wat betekent een deugdelijke invulling van deze systeemverantwoordelijkheid? In hoeverre is de overheid in staat om hier invulling aan te geven en welke risico's spelen rond de politiek-bestuurlijke aansprakelijkheid?

ICT-infrastructuur: kerntaak en afhankelijkheid van private partijen

De eerste vraag die rijst, is of de overheid überhaupt verantwoordelijk is voor het tot stand komen van een maatschappelijke ICT-infrastructuur. Is (het stimuleren of ondersteunen van) de inrichting van landelijke ICT-netwerken eigenlijk wel een overheidstaak, of moet dit worden overgelaten aan het spel van de maatschappelijke krachten? Dit raakt aan het kerntakendebat. Er is een aantal standaardredeneringen waarom overheidsingrijpen gerechtvaardigd kan zijn. Bovens et al. (2007: 84-98) noemen verschillende redenen voor overheidssturing. Ik bespreek daarvan de drie belangrijkste redenen als het gaat om vragen over de verantwoordelijkheid voor een maatschappelijke infrastructuur. Per reden kan worden beargumenteerd dat de overheid een taakverantwoordelijkheid heeft als het gaat om de maatschappelijke ICT-infrastructuur.

De eerste reden voor overheidssturing is het beschermen van de markt door preventie van monopolies en kartels. Duidelijk is dat er op het gebied van ICT risico's bestaan van onvolledige marktwerking door monopolie- en kartelvorming. Een voorbeeld zijn de Amerikaanse en Europese rechtszaken tegen Microsoft die jaren hebben gesleept (Cohen 2004). Ook voor nieuwe technologieën zal de overheid steeds de marktwerking in de gaten moeten houden. Bescherming van de marktpositie van burgers is een blijvend aandachtspunt. Anderzijds kan een te strikt toezicht de mogelijkheden voor bedrijven om technologieën te ontwikkelen remmen. Beperken van de positie van bedrijven als Microsoft, Apple en Google kan de kartelvorming tegengaan, maar ook de innovatie belemmeren.

Een tweede reden voor overheidssturing is aanvullen van de markt door de productie van collectieve goederen. Vanuit theorieën over overheidstaken wordt benadrukt dat de overheid een verantwoordelijkheid heeft voor vitale infrastructuren zoals het stelsel van dijken, het elektriciteitsnet en het wegennet. Dijken en het moderne wegennet zijn in hoge mate collectieve goederen, het is technisch onmogelijk, of zeer problematisch om het gebruik te individualiseren. Het marktsysteem kan hier falen. Systeemfalen kan ook optreden bij de ICT-infrastructuur. Het is ondoenlijk om voor elk huis aparte glasvezelkabelnetwerken te trekken. Het geheel aan technologieën en informatievoorzieningen dient te worden beschouwd als een vitale infrastructuur, want zonder deze infrastructuur valt het economische en sociale leven in Nederland voor een groot deel stil. Internet is tegenwoordig zowel van groot economisch als van enorm maatschappelijk belang. De verantwoordelijkheid van de overheid betreft het bestaan van een technologische infrastructuur voor informatie-uitwisseling. De verantwoordelijkheid betreft een resultaatverantwoordelijkheid: een dergelijke infrastructuur moet bestaan en goed functioneren. Dit betekent overigens niet dat de overheid ook degene is die de informatie-infrastructuur moet bouwen en beheren. Dit kan worden overgelaten aan private of publieke partijen zolang de overheid waarborgen heeft gecreëerd voor het bestaan van deze infrastructuur (wat natuurlijk wel eisen stelt aan het vermogen van de overheid om invulling te geven aan goed opdrachtgeverschap).

Een derde reden voor overheidssturing is compenseren van de markt door herverdeling. Het is voorstelbaar dat het voor bedrijven in bepaalde gevallen ongunstig is om internetvoorzieningen aan te leggen of om dekking te realiseren voor mobiele telefonie en mobiel internet – waarbij dit overigens in dunner bevolkte landen als Canada en Zweden (Birdsall 2000) een groter probleem zal zijn dan in Nederland. Desalniettemin kunnen overheden bijvoorbeeld via subsidieregelingen voor burgers in dunner bevolkte gebieden garanderen dat iedereen in Nederland toegang heeft tot internet. Tekortkomingen van het systeem worden zo opgelost. Een nadeel van deze benadering is dat hier hoge kosten aan verbonden kunnen zijn voor de betreffende overheden. Ook zou men kunnen betogen dat een derge-

lijke overheidsbetrokkenheid uiteindelijk voorkomt dat de markt zelf passende oplossingen voor de 'nichemarkten' ontwikkeld.

Daarmee zijn drie redenen genoemd om de inrichting van landelijke ICT-netwerken te stimuleren en ondersteunen. Aanvullend heeft de overheid ook een taakverantwoordelijkheid bij het beschermen van de ICT-infrastructuur. Clarke & Knake (2010) wijzen op het risico van *cyber wars*: aanvallen op de ICT-netwerken van een land. Een dergelijke aanval – een Distributed Denial of Services Attack – heeft in 2007 plaatsgevonden op Estland en daardoor werden vele websites onbereikbaar. Iran heeft recentelijk bekendgemaakt te zijn aangevallen met het computervirus Stuxnet. Bescherming van ICT-infrastructuren zal een steeds belangrijker onderdeel worden van de beveiliging van een land.

Informatie-uitwisseling: betekenis van grondrechten in het digitale tijdperk
Een volgende vraag is of de overheid ook een verantwoordelijkheid heeft voor wat plaatsvindt op deze technologische infrastructuur voor informatie-uitwisseling. Heeft de overheid ook een verantwoordelijkheid voor het informatieverkeer? Ook hier kan het vruchtbaar zijn om de parallel te trekken met andere vitale maatschappelijke infrastructuren. Ook daarvoor geldt dat de overheid normen heeft ontwikkeld voor en toezicht uitoefent op het maatschappelijk verkeer. Zo geldt bijvoorbeeld voor het verkeer op het wegennet dat de overheid niet alleen een verantwoordelijkheid voor het bestaan van een wegennet heeft, maar ook dient te waarborgen dat dit wegennet veilig is.

Een groot deel van de liberale, politieke en sociale grondrechten die in de afgelopen eeuwen zijn ontwikkeld, zijn in feite te lezen als opdrachten aan de overheid om, door handelen of nalaten, de rechten van burgers in het maatschappelijk verkeer, of in het verkeer met de overheid zelf te waarborgen. Deze catalogus van grondrechten geldt niet alleen voor het analoge maatschappelijke verkeer, maar is evenzeer van toepassing op het digitale maatschappelijke verkeer. Het is de algemene taak van de overheid om deze rechten te waarborgen, ongeacht de aard van de infrastructuur waarop deze worden uitgeoefend. Voor toepassing op de moderne informatie-infrastructuur is wel een vertaling nodig van de verschillende begrippen (huisrecht, demonstratie, huisvesting) naar het digitale tijdperk. Eerder heeft Bovens (2003) betoogd dat in de informatiesamenleving bovendien nog een extra laag van informatierechten aan het 'huis van de rechtsstaat' dient te worden toegevoegd.

Laten we de verschillende soorten rechten aflopen (waarbij ik overigens wederom niet de pretentie heb om alle rechten uitputtend te bespreken). We beginnen hierbij onderop bij het waarborgen van de vrijheidsrechten. Een interessante vraag is welke betekenis wordt gegeven aan het huisrecht in het informatietijdperk. Het huisrecht betreft de vrijheid om te doen en laten wat je wilt in je eigen huis zonder

dat iemand deze woning mag binnentreden. Maar wat betekent binnentreden in het informatietijdperk? Koops, Schooten en Prinsen (2004) geven aan dat huizen steeds meer veranderen in elektronische netwerken en dat daarmee het vermogen om elektronisch deze huizen 'binnen te treden' toeneemt. De huidige waarborgen voor het huisrecht schieten volgens hen tekort en daarom moet artikel 12 van de Grondwet worden uitgebreid met een elektronisch huisrecht (om haar taak om dit recht te waarborgen in het informatietijdperk goed in te vullen).

Ook allerlei digitale bedreigingen voor de vrijheid van burgers plaatsen overheden voor uitdagingen bij het invullen van de systeemverantwoordelijkheid. Hoe kunnen overheden reageren op *identity theft* (zie ook Choenni et al. 2011)? Wat kunnen overheden met virtuele vormen van stalking en lastigvallen? Hoe kan worden gereageerd op inbraken in computers? Overheden zijn nu reeds bezig met het vertalen van rechtsprincipes naar digitale praktijken. Er bestaat een wet op de computercriminaliteit en stalken op internet is ook strafbaar gemaakt. Duidelijk is wel dat de vertaling van offline vrijheidsrechten naar digitale vrijheidsrechten niet triviaal is. De schade die wordt toegebracht met digitaal stalken lijkt voor een 'digitale migrant', iemand die internet instrumenteel gebruikt en hier niet mee is opgegroeid (Prensky 2001), beperkt en niet in verhouding te staan met stalken in het echte leven. Voor een *digital native*, die een groot deel van zijn leven doorbrengt op internet, is digitaal stalken echter misschien nog wel bedreigender en minder vermijdbaar dan stalken op straat.

Het waarborgen van politieke rechten lijkt weinig problematisch: internet biedt meer mogelijkheden dan ooit om deze rechten uit te oefenen. Burgers kunnen petities opstellen via petities.nl en krijgen stemadvies via de stemwijzer. Ze kunnen eenvoudig politieke allianties vormen en contact zoeken met gelijkgestemden op internet. De enige taak die hier relevant lijkt voor de overheid is het waarborgen dat bepaalde politieke verenigingen niet worden geweigerd door internetproviders. Voor zover ons bekend, doet zich dit probleem in Nederland echter niet of nauwelijks voor. Ook kunnen ondersteunende maatregelen voor mensen die niet op internet komen in de vorm van toegang tot computers in bibliotheken en training belangrijk zijn. Opvallend is echter dat dergelijke vormen ook steeds sterker door de markt worden opgepakt. Algemene educatie lijkt belangrijker te zijn dan specifieke aandacht voor digibeten (Van Deursen & Van Dijk 2008).

Ook voor het waarborgen van de sociale rechten lijkt de technologische ontwikkeling niet direct problemen te creëren. Men zou kunnen betogen dat de technologieontwikkeling leidt tot verlies aan bepaalde banen, maar tegenwoordig ontstaan er vooral banen door deze ontwikkelingen. Ook lijken de nieuwe technologieën vooral bij te dragen aan de mogelijkheden tot scholing, bijvoorbeeld voor mensen die in afgelegen gebieden wonen (Porter 1997).

Een groep rechten die typerend is voor het informatietijdperk zijn natuurlijk de informatierechten. Bovens (2003: 98) maakt een onderscheid tussen het recht op toegang tot overheidsinformatie (primaire rechten), het recht op toegang tot informatiekanalen (secundaire rechten) en het recht van burgers op informatie van private rechtspersonen (tertiaire rechten). Qua systeemverantwoordelijkheid zijn de tertiaire rechten het meest interessant. Bovens (2003: 107) geeft aan dat in een tijdperk waarin nationale overheden niet langer de centrale actoren zijn, toegang tot informatie van derden vaak cruciaal kan zijn voor het democratisch debat. Als voorbeeld noemt hij jaarverslagen van maatschappelijke organisatie en bronnen die worden gebruikt in het publieke debat. Deze taak kan relatief eenvoudig worden ingevuld, maar leidt wel tot een discussie over de rechten van bedrijven en maatschappelijke organisaties op geheimhouding. Hoever gaan de tertiaire informatierechten van burgers? En wanneer botsen deze met bedrijfsgeheimen en privacy? Duidelijk is dat de normen hieromtrent schuiven: blootgeven van de inkomens van topbestuurders is niet langer een taboe. Ook dienen bedrijven steeds meer informatie te geven over milieugedrag. Het adagium op internet 'information wants to be free' lijkt ook hier te leiden tot een groeiende openbaarheid.

Kwaliteit van de publieke sfeer: feiten of propaganda?

Wanneer de overheid heeft gewaarborgd dat er een goede infrastructuur is en dat de mogelijkheden tot informatie-uitwisseling gewaarborgd zijn, is nog niet gegarandeerd dat er een goed functionerende publieke sfeer op internet ontstaat. Sunstein (2001) noemt in zijn boek *Republic.com* het creëren van mediapluralisme dé uitdaging voor de toekomst. De overheid heeft vanuit haar taak als behartiger van de democratie ook een systeemverantwoordelijkheid voor de kwaliteit van de informatie in de publieke sfeer, aangezien de markt en de publieke sfeer ook hierin kunnen falen. Terughoudendheid is hierbij van belang, aangezien betrokkenheid bij de publieke sfeer en overheidspropaganda dicht bij elkaar kunnen liggen. Is overheidsinformatie over inentingen een poging om de kwaliteit van de publieke sfeer te verbeteren of gaat het om overheidspropaganda? De grens tussen informatie en propaganda is dun (Jowett & O'Donell 2006).

Via de volgende rollen kan de overheid invulling geven aan de verantwoordelijkheid voor de kwaliteit van de publieke sfeer.

– *Marktmeester*. De overheid dient te waarborgen dat er voldoende pluriformiteit in de media blijft bestaan. Deze rol heeft de overheid ook bij de massamedia: concentratie van massamedia in de handen van een bedrijf is onwenselijk. Ook op internet dient de pluriformiteit te worden gewaarborgd. Vanuit deze rol kunnen bijvoorbeeld vraagtekens geplaatst worden bij de centrale positie van Google bij de ontsluiting van (publieke) informatie (Vise & Malseed 2005).
– *Toezichthouder*. De overheid stelt als toezichthouder grenzen aan de inhoud van informatie in de publieke sfeer. Bekende voorbeelden zijn de filmkeuring,

het verbieden van *Mein Kampf* en het labelen en de certificering van producten. Ook op internet zijn dergelijke vormen van toezicht op de inhoud van informatie relevant. Aanzetten tot haat mag niet en verschaffen van valse informatie over producten ook niet. De vraag wanneer er sprake is van aanzetten tot haat is echter inzet van doorgaand maatschappelijk en juridisch debat.
– *Producent.* De overheid kan zelf informatie produceren om daarmee de kwaliteit van de publieke sfeer te versterken. Bekend zijn de spotjes van Postbus 51 en de publieksvoorlichting van SIRE. Recente, saillante, voorbeelden zijn de voorlichting over de inentingen tegen de virussen HPV en H1N1 waarbij de informatie van de overheid door grote groepen burgers ter discussie werd gesteld.

Daarmee zijn voor de overheid twee taken jegens alle burgers geformuleerd – waarborgen van het bestaan van een vitale infrastructuur en waarborgen van een vitale publieke sfeer – en een taak jegens individuele burgers – het waarborgen van hun individuele rechten. Deze taakgebieden bakenen de taakverantwoordelijkheden van overheden voor het gebruik van ICT in de samenleving af. Nu kunnen we de invulling van deze taken verder bespreken in termen van verantwoordelijkheid als deugd, als vermogen en als aansprakelijkheid.

3.4.2 VERANTWOORDELIJKHEID ALS DEUGD: LEGE OVERHEID OF LEIDERSCHAP?

En hoe kan de overheid al deze complexe verantwoordelijkheden op een deugdelijke manier invullen? Een deugdelijk gebruik van ICT binnen de overheid is al lastig, een deugdelijke invulling van deze systeemverantwoordelijkheid is nog complexer. Het vraagt van de overheid namelijk dat een adequate perceptie plaatsvindt van veranderingen in ICT-infrastructuren, ontwikkelingen die de informatierechten beïnvloeden en ontwikkelingen die van belang zijn voor de kwaliteit van de informatie in de publieke sfeer. Vervolgens dienen gevaren te worden onderkend en normen en belangen moeten worden afgewogen.

Dat de adequate perceptie van de noodzaak tot ingrijpen problematisch is, is gebleken bij de millenniumbug (Gutteling & Kuttschreuter 2002). Wereldwijd hebben overheden hun verantwoordelijkheid genomen en maatregelen getroffen om te voorkomen dat er in de samenleving allerlei problemen zouden ontstaan. Achteraf is iedereen vooral met de vraag blijven zitten of er nu een probleem was, want er ging niets mis. Men zou kunnen zeggen dat dit kwam doordat iedereen zich had voorbereid, maar ook in landen waar men relatief weinig voorbereidingen had getroffen, deden zich geen problemen voor. Vergelijkbare problemen met de perceptie van de omgeving treden op allerlei terreinen op. Hoe belangrijk is nu eigenlijk Universal Mobile Telecommunications System (UMTS), een systeem voor mobiele telecommunicatie? Is het nodig om via allerlei maatregelen de positie van digibeten te verbeteren? De dynamiek van de technologische ontwikkeling is zeer moeilijk te doorgronden en wordt ook steeds moeilijker te doorgronden,

doordat het aantal actoren dat hier wereldwijd bij betrokken is alleen maar toeneemt. De overheid moet zich een beeld vormen van de veranderingen, maar weet tegelijkertijd dat dit beeld in meer of mindere mate inadequaat zal zijn.

Deugdelijk handelen wordt verder gecompliceerd door het ontbreken van heldere criteria en normen. Dit probleem speelt bij de systeemverantwoordelijkheid van de overheid veel sterker dan bij de gebruiksverantwoordelijkheid (waarbij de communis opinio is dat bestuur legaal, neutraal, behoorlijk en transparant moet zijn). Politieke en maatschappelijke overtuigingen over de systeemverantwoordelijkheid van de overheid lopen veel sterker uiteen. Sommige politieke partijen vinden bijvoorbeeld dat de overheid helemaal geen rol heeft te spelen in een kwalitatief sterk publieke informatievoorziening, terwijl andere partijen dit cruciaal vinden.

Uiteindelijk zal de vraag over een deugdelijke systeemverantwoordelijkheid zich vooral toespitsen op de rolopvatting van de overheid. In de informatiesamenleving krijgt de overheid steeds meer de rol van een regisseur en procesmanager. De vraag is echter welke inhoudelijke betrokkenheid er nog overblijft. Wat is bijvoorbeeld precies een deugdelijke invulling van de systeemverantwoordelijkheid voor technologieën zoals de OV-chipkaart en het EPD?[2] Moet de overheid vooral 'leeg' zijn, zoals Paul Frissen (1999) heeft betoogd? Of is er meer behoefte aan leiderschap vanuit de overheid? De verheerlijking van de markt lijkt voorbij te zijn en de financiële crisis heeft geleid tot een herwaardering van de rol van de overheid. Het gestuntel rondom de OV-chipkaart laat zien dat een leidende rol van de overheid niet eenvoudig is, maar wel maatschappelijk wordt verwacht (Van 't Hof et al. 2010).

3.4.3 VERANTWOORDELIJKHEID ALS VERMOGEN: SAMENWERKING OF AUTONOMIE?

Het vermogen om invulling te geven aan de systeemverantwoordelijkheid wordt ook nog sterker dan de gebruiksverantwoordelijkheid uitgedaagd. Hoe kan de nationale overheid een internationale infrastructuur beïnvloeden? Zelfs de Chinese overheid heeft grote moeite om enige grip te krijgen op de anarchistische wereld van internet. Rechtsstatelijke reacties op technologische ontwikkelingen zijn per definitie traag, terwijl de technologische dynamiek blijft doorjakkeren. Bovens (2003: 22) schrijft hierover: "(…) de wetgever dreigt hiermee in een *catch-22*-situatie terecht te komen. Aan de ene kant vragen de trias en de rechtszekerheid om een zorgvuldige, stabiele en duidelijke wetgeving, terwijl aan de andere kant de maatschappelijke ontwikkeling vraagt om open normen en snelle aanpassingen. (…). Met name in de ICT-sfeer is de kans groot dat een wet al verouderd is tegen de tijd dat zij het *Staatsblad* bereikt." Dat het *Staatsblad* sinds 2009 alleen nog digitaal verschijnt lost dit probleem van dynamiek niet op.

De technologische dynamiek is direct verbonden met andere trends die de systeemverantwoordelijkheid van de overheid uitdagen zoals deterritorialisering, horizontalisering en dematerialisering (Bovens 2003; WRR 1998). Over deterritorialisering schrijft Bovens (2003: 20): "Het internationale karakter van de informatiemaatschappij ondermijnt (...) het nationale karakter van het huis van de rechtsstaat." Hij verwijst hierbij naar de toenemende samenwerking tussen nationale staten en de groeiende rol van internationale organisaties (EU) en verdragen (WTO). Zowel de genoemde bedreigingen voor het functioneren van markten als de bedreigingen van vrijheidsrechten zoals eigendom en een veilige digitale omgeving trekken zich weinig aan van nationale grenzen. Wat kan de Nederlandse overheid doen aan hackers uit Nigeria? Hoe kan de Nederlandse overheid voorkomen dat Google een monopolie op het ontsluiten van informatie opbouwt?

De enige manier waarop de overheid haar vermogen om burgers te beschermen kan vergroten is via internationale samenwerking. Samenwerking met andere landen kan helpen om criminele organisaties aan te pakken. Ook kan Europese samenwerking de mogelijkheid vergroten om marktverstoringen aan te pakken. Een gevolg van deze internationale samenwerking is echter wel dat de Nederlandse overheid zelf minder sturingsmogelijkheden krijgt en wordt gereduceerd tot een van de vele actoren in een internationaal netwerk. Een groeiende kloof met Nederlandse burgers kan hiervan het gevolg zijn omdat de inputlegitimiteit van de overheid afneemt.

Ook het vermogen om systeemfalen aan te pakken is beperkt. Welke kennis over ICT-infrastructuren, informatie-uitwisseling en informatie in de publieke sfeer is bij de overheid aanwezig? De enige mogelijkheid om tot zinvolle aanpakken te komen is het ontwikkelen van samenwerkingsverbanden met marktpartijen en maatschappelijke organisaties. Ook hier is echter sprake van een *Faustian Pact*: dergelijke verbanden reduceren het vermogen van de overheid om een autonome invulling te geven aan taken.

3.4.4 VERANTWOORDELIJKHEID ALS AANSPRAKELIJKHEID: BUREAUCRATISERING?

En wat zijn hier dan de risico's voor de aansprakelijkheid? Ook hier geldt dat de politiek-bestuurlijke aansprakelijkheid sterk afhankelijk is van de verwachtingen die er zijn over de invulling van deze systeemverantwoordelijkheid. Ik zie twee mogelijkheden: (1) de verwachtingen van het publiek over de systeemverantwoordelijkheid groeien en het onvermogen om hieraan te voldoen leidt tot politiek-bestuurlijke problemen en (2) de verwachtingen van het publiek nemen af en het publiek onderkent dat de mogelijkheden voor de overheid om invulling te geven aan de systeemverantwoordelijkheid beperkt zijn. De invulling van deze mogelijkheden is sterk afhankelijk van de perceptie van de overheid: is de over-

heid eindverantwoordelijk of heeft de overheid een procesmatige verantwoordelijkheid?

De neiging van de overheid is om de aansprakelijkheid voor de bescherming van burgers tegen externe dreigingen zoveel mogelijk te leggen bij individuele burgers en maatschappelijke partijen. Gebruikmakend van het werk van Foucault noemt Burchell (1991) deze beweging 'responsibilisering'. Veilig internetgebruik wordt voorgesteld als het resultaat van individuele keuzen rondom beveiliging door burgers en aanvullende maatregelen van providers. De vergelijking dringt zich op met campagnes gericht op het voorkomen van het bewaren van kostbaarheden in auto's. Via deze campagnes schuift de overheid de verantwoordelijkheid voor de bestrijding van inbraak naar individuele burgers die kostbaarheden in de auto laten liggen. Dit is vergelijkbaar met de nadruk die overheden leggen op 'veilig computergebruik' en voorlichting aan burgers over het installeren van beveiligingssoftware op computers.

Ook bij het ingrijpen bij systeemfalen ligt de aansprakelijkheid niet direct bij de overheid. Wie is er aansprakelijk wanneer een monopolist jarenlang de kwaliteit van een kritieke infrastructuur heeft laten versloffen? Kan OPTA dergelijke problemen voorkomen? De overheid als toezichthouder wordt steeds vaker ter verantwoording geroepen wanneer er iets misgaat. Misschien is de overheid in juridische zin niet verantwoordelijk. Echter, in politiek-bestuurlijke zin gaat bij maatschappelijke rampen zoals de brand in 't Hemeltje in Volendam en de vuurwerkramp in Enschede de aandacht al snel uit naar de toezichthouder 'die dit maar allemaal heeft laten gebeuren'. Bureaucratisering geldt vaak als reactie op dergelijke verwijten. Een verdergaande bureaucratisering van het toezicht op ICT-infrastructuren is te verwachten, zeker wanneer deze infrastructuren een keer uitvallen en de grote afhankelijkheid hiervan zichtbaar wordt.

3.4.5 BELANGRIJKSTE VRAAGSTUKKEN BIJ SYSTEEMVERANTWOORDELIJKHEID VOOR ICT

Op basis van de analyse van de literatuur en vertaling van nieuwe ontwikkelingen naar normatieve vragen kan nu de tweede deelvraag worden beantwoord. We hadden de volgende vraag geformuleerd: wat zijn de belangrijkste vraagstukken als het gaat om de invulling van verantwoordelijkheden van de overheid bij de rol van informatie en technologie in de samenleving? De volgende (veelal samenhangende) vraagstukken zijn geïdentificeerd.

– *Waarborgen van de ICT-infrastructuur*. Bij het waarborgen van een ICT-infrastructuur gaat het om een verdeling van rollen tussen overheid en private sector. De overheid zal hierbij steeds moeten bekijken welke regulerende en ook complementerende rol moet worden ingenomen. De grote (technologische) dynamiek van de sector maakt dit een lastige opgave.

- *Waarborgen van informatie-uitwisseling*. De lastige vraag op het terrein van het waarborgen van informatie-uitwisseling is welke mate van openbaarheid van bedrijven en maatschappelijke actoren kan worden geëist. De maatschappelijke betekenis van deze actoren maakt openbaarheid van belang, maar tegelijkertijd kan openbaarheid botsen met de belangen van de betreffende bedrijven en organisaties.
- *Waarborgen van de publieke sfeer*. In de publieke sfeer worden opinies gevormd en debatten gevoerd. In verschillende rollen – marktmeester, toezichthouder en producent – kan de overheid een bijdrage leveren aan de kwaliteit van de publieke sfeer. Daarbij ligt echter steeds het risico van overheidspropaganda op de loer.
- *De interventieparadox*. De overheid heeft steeds minder mogelijkheden om haar systeemverantwoordelijkheden in te vullen, maar de verwachtingen van deze verantwoordelijkheid lijken toe te nemen. Er is sprake van een interventieparadox (Noordegraaf 2004): de (technologisch) complexe samenleving roept om meer sturing, maar staat minder sturing toe.
- *Samenwerking of autonomie*. De invulling van systeemverantwoordelijkheden gebeurt in toenemende mate in samenwerking met andere maatschappelijke actoren en (Europese) overheden. Deze samenwerking versterkt het sturende vermogen, maar beperkt de autonomie. Een groeiende kloof met burgers kan van het laatste het gevolg zijn.
- *Bureaucratisering*. De overheid kan de systeemverantwoordelijkheid invullen door deze sterk procedureel in te vullen. Bureaucratisering is een reactie op juridisering en een manier om verantwoordelijkheden hanteerbaar te maken. De vraag is wel in hoeverre bureaucratisering daadwerkelijk kan bijdragen aan het waarborgen van het adequaat functioneren van het gehele systeem.

Opvallend aan deze vraagstukken is dat deze weliswaar ten dele met het karakter van de technologie te maken hebben, maar tegelijkertijd ook direct verbonden zijn met grotere vragen over de overheid in een complexe, globaliserende samenleving (Bovens 2001; Noordegraaf 2004). Complexe vraagstukken en hoge verwachtingen plaatsen de overheid voor een lastige opgave. Daarbij versterkt de grote technologische dynamiek de moeilijkheid van deze opgave. Strategieën van responsibilisering – het afschuiven van verantwoordelijkheden naar burgers, bedrijven en maatschappelijke organisaties – vormen een logisch antwoord op deze ontwikkeling, maar leiden tot verdampende verantwoordelijkheden en wellicht onvoldoende waarborgen voor collectief wenselijke uitkomsten. Ook in het informatietijdperk lijkt er nog steeds een belangrijke rol te zijn weggelegd voor de overheid, omdat de overheid de enige is met een verantwoordelijkheid voor het gehele systeem.

3.5 KLASSIEKE ORGANISATIEKUNDIGE EN POLITIEK-FILOSOFISCHE SPANNINGEN IN EEN NIEUW JASJE

In de tekst zijn een aantal lastige dilemma's voor de overheid benoemd. Antwoorden op de deelvragen zijn gepresenteerd en de belangrijkste vraagstukken op het gebied van gebruiks- en systeemverantwoordelijkheden voor ICT zijn benoemd. In deze slotparagraaf keren we terug naar de centrale vraagstelling: wat zijn de belangrijkste vraagstukken waar de overheid zich voor ziet geplaatst als het gaat om de invulling van haar verantwoordelijkheden op het gebied van informatie en technologie? De specifieke antwoorden zijn al gepresenteerd, nu zal ik proberen de dilemma's op een hoger niveau van abstractie te benoemen. Gezien het grote onderscheid tussen de twee soorten verantwoordelijkheden, zullen deze hier ook gescheiden besproken worden. Het antwoord op de centrale vraag is dat de overheid voor twee cruciale vragen staat: hoe kan de overheidsorganisatie zowel stabiel als flexibel zijn en hoe kan de overheid zowel verantwoordelijkheid geven als verantwoordelijkheid nemen? Ik presenteer de idee van de genormeerde experimenteerruimte als een mogelijke oplossingsrichting voor deze twee vraagstukken.

3.5.1 GEBRUIKSVERANTWOORDELIJKHEDEN: STABILITEIT VERSUS FLEXIBILITEIT

De spanningen rondom de gebruiksverantwoordelijkheden van de overheid kunnen worden geduid aan de hand van de organisatiewetenschappelijke idee van contingentie. Contingentietheorie (Mintzberg 1983) leert ons dat een machinebureaucratie – een organisatie die wordt gekenmerkt door een hoge mate van standaardisatie en formalisering – past bij een simpele en eenvoudige omgeving. De technologische omgeving moet echter worden beschouwd als turbulent en complex. En de mate van turbulentie en complexiteit lijkt alleen verder toe te nemen (Teeuw et al. 2007): de tijd tussen de ontwikkeling van een technologie en de brede toepassing ervan wordt steeds korter. Ook beïnvloedt technologie een steeds groter domein van het menselijk handelen: waar het vroeger nog uitsluitend ging om rekencapaciteit en dataverwerking raakt de technologie nu ingebed in de haarvaten van de samenleving en het openbaar bestuur.

Contingentietheorie leert ons dat een passende reactie op een turbulente en dynamische omgeving de creatie van een adhocratie is (Mintzberg 1983: 253). Een adhocratie is een organische structuur met een beperkte formalisatie van gedrag. Deze structuur is het meest in staat tot geavanceerde innovatie. Een adhocratie verhoudt zich echter slecht tot de rechtsstatelijke eisen die aan de overheid worden gesteld. De eisen tot transparantie, betrouwbaarheid, neutraliteit, voorspelbaarheid, enzovoorts kunnen juist het beste worden gewaarborgd door een machinebureaucratie. Een adhocratie zou nog transparant kunnen zijn, maar betrouwbaarheid, neutraliteit en (vooral) voorspelbaarheid zijn niet gewaarborgd. Sterker nog: een adhocratie wil juist niet voorspelbaar zijn. Ook de democratische

eis dat de overheid gehoorzaamt aan de volkswil zoals belichaamd door het parlement vraagt eerder om een machinebureaucratie dan om een adhocratie. Bij een adhocratie is het risico van een *run away bureaucracy*, een overheid die uitgaat van de eigen belangen, juist groot (en wenselijk gezien de noodzaak tot innovatie).

De technologie biedt mogelijk uitkomsten om met het spanningsveld dat ontstaat door tegenstrijdige eisen uit de technologische en politiek-juridische omgeving om te gaan. Meijer (2004) heeft laten zien hoe de technologie kan worden ingezet om schijnbaar onverenigbare eisen aan de organisatie van de overheid – met name dynamiek versus stabiliteit – vorm te geven door intelligente combinaties van kenmerken van netwerkorganisaties en machinebureaucratieën. Meijer beschrijft het ideaaltype van de netwerkbureaucratie die tegelijkertijd kenmerken heeft van een adhocratie en van een machinebureaucratie. De crux hier is dat informele en horizontale arrangementen de ruimte krijgen, maar zich wel ontwikkelen in de schaduw van formele, hiërarchische arrangementen. Deze combinaties zijn mogelijk doordat netwerktechnologieën zoals e-mail tegelijkertijd zowel informele, horizontale als formele, verticale interactiepatronen kunnen ondersteunen.

Een mooi voorbeeld van de combinatie van horizontale en verticale manieren van sturing zien we in het gebruik van 'netcentrisch werken' in de bestrijding van rampen (Wolbers 2009). Gebruik van netwerksystemen maakt het mogelijk dat de verschillende betrokkenen bij de bestrijding van rampen minder afhankelijk zijn van verticale communicatie en daardoor sneller en adequater kunnen reageren op rampen. Tegelijkertijd vindt deze manier van werken plaats binnen een systeem van verticale verantwoordelijkheden. Duidelijk blijft dat cruciale beslissingen volgens de *chain of command* moeten verlopen. Mooi aan netcentrisch werken is wel dat de chain of command de uitwisseling van informatie niet langer beperkt en daardoor bijdraagt aan het verbeteren van de communicatie.

Combineren van verticale en horizontale manieren van sturen kan betekenen dat overheden experimenteerruimte krijgen, maar tegelijkertijd over het gebruik van deze ruimte ter verantwoording kunnen worden geroepen. Deugdelijk gedrag zal moeten groeien uit deze nieuwe praktijken. De overheid kan bijvoorbeeld wel de ruimte krijgen om nieuwe vormen van dienstverlening te ontwikkelen, maar deze vormen worden na ontwikkeling wel getoetst op deugdelijkheid. Function creep wordt niet vooraf afgewezen, maar achteraf getoetst op wenselijkheid. De overheid zal achteraf moeten bewijzen dat zij verantwoord met technologie kan omgaan. De adhocratie maakt experimenteren mogelijk, de machinebureaucratie oogst de experimenten en zorgt voor een zorgvuldige inbedding van de uitkomsten.

3.5.2 SYSTEEMVERANTWOORDELIJKHEID: PROCESMATIGE VERANTWOORDELIJKHEID GEVEN VERSUS VERANTWOORDELIJKHEID NEMEN

Veranderingen in de systeemverantwoordelijkheid kunnen het beste begrepen worden vanuit de belangrijkste structurele transformatie van onze samenleving van dit moment: de vorming van een netwerksamenleving (Castells 1996). Het vermogen van de overheid om vanuit een centraal punt te sturen neemt steeds verder af. En waarschijnlijk ook ten dele de noodzaak om dit te doen. De samenleving krijgt steeds sterker de vorm van een polycentrisch systeem: sturing vindt vanuit vele punten plaats. Wat is de systeemverantwoordelijkheid van de overheid in een dergelijk netwerk?

Een algemene lijn in de ontwikkeling van overheidsverantwoordelijkheid is een trend van responsibilisering (Burchell 1993). Verantwoordelijkheden worden zoveel mogelijk van de overheid bij andere partijen gelegd. Illustratief is hierbij ook de wijze waarop via *informed consent* de verantwoordelijkheid voor medische informatie bij individuele burgers wordt gelegd (Keizer 2011). Deze trend van responsibilisering kan begrepen worden vanuit de gedachte dat de samenleving steeds meer bestaat uit netwerken. Als de sturing vanuit vele punten plaatsvindt, is het ook logisch dat verantwoordelijkheden op verschillende plaatsen worden belegd. Deze verspreiding van verantwoordelijkheden roept echter een aantal belangrijke knelpunten op, zoals met name het probleem van de vele handen (Thompson 1980). Wie kan erop worden aangesproken als er iets misgaat? Ook dient voorkomen te worden dat verantwoordelijkheden op de schouders van relatief zwakke burgers worden gelegd.

Bij de systeemverantwoordelijkheid wordt de overheid gedwongen haar positie in een netwerksamenleving te heroverwegen. Principes van netwerkmanagement en governance zullen hier in toenemende mate leidend moeten zijn (Kjaer 2004; De Bruijn et al. 1998). Het wordt namelijk steeds lastiger, en misschien wel fundamenteel onmogelijk, om een centrale rol te spelen in de turbulente, complexe, technologische netwerken. In plaats van een overkoepelende verantwoordelijkheid zal de overheid steeds sterker twee andere verantwoordelijkheden kunnen nemen: een procesmatige verantwoordelijkheid en een restverantwoordelijkheid.

Een procesmatige verantwoordelijkheid betekent dat de overheid niet langer de verantwoordelijkheid neemt voor de uitkomsten, maar wel voor de kwaliteit van het proces. In dit perspectief hoeft de overheid geen ICT-infrastructuur te ontwikkelen, zoals dit wel is gebeurd met allerlei andere nutsnetwerken (transport, water, gas, elektriciteit). Wel dient de overheid ervoor te zorgen dat partijen gestimuleerd worden om dit op een goede manier te doen. Ook is de overheid niet verantwoordelijk voor een veilige digitale omgeving, maar dient de overheid wel te zorgen dat

partijen die een dergelijke veiligheid kunnen creëren (providers, moderators, knooppunten, internetbestuur, ICT-ontwikkelaars, enzovoorts) via een goed proces gezamenlijk werken aan veiligheid.

Een restverantwoordelijkheid heeft een ander – en wellicht aanvullend – karakter. In dit perspectief dient de overheid te waarborgen dat de relevante partijen werken aan bescherming van burgers en het voorkomen van systeemfalen: de overheid dient nu ook de taken op zich te nemen die door andere partijen niet worden vervuld. De overheid dient er bijvoorbeeld voor te zorgen dat er geen burgers worden uitgesloten van de nieuwe nutsnetwerken en de discussie over netneutraliteit is daarvan een mooi voorbeeld. En als de veiligheid van burgers in de digitale omgeving onvoldoende wordt gewaarborgd, dient de overheid aanvullende acties te ondernemen.

Over de procesverantwoordelijkheid lijkt een hoge mate van overeenstemming te bestaan over het gehele politieke spectrum. Vanuit pragmatische overwegingen wordt breed onderkend dat de overheid in hoge mate afhankelijk is van andere landen (deterritorialisering) en andere partijen in Nederland (horizontalisering). De restverantwoordelijkheid ligt gevoeliger. Waar houdt de verantwoordelijkheid van burgers en maatschappelijke partijen op en waar begint de verantwoordelijkheid van de overheid? Waar de gebruiksverantwoordelijkheid uiteindelijk werd geduid als een klassieke organisatiekundige spanning – organiseren van stabiliteit versus organiseren van flexibiliteit – in een nieuw jasje zien we dat een analyse van de systeemverantwoordelijkheid resulteert in een actualisering van een klassieke politiek-filosofische spanning – verantwoordelijkheid geven versus verantwoordelijkheid nemen.

3.5.3 GENORMEERDE EXPERIMENTEERRUIMTE: INTELLIGENT MANOEUVREREN DOOR ONBEKEND GEBIED

Mumford (1970) waarschuwt voor een technologie die niet meer wordt gecontroleerd, omdat daarbij menselijke wensen en behoeften ondergeschikt worden gemaakt aan de logica van technologische systemen. Kan voorkomen worden dat de technologie oncontroleerbaar wordt? Dat weten we niet. De technologie is een enorm sterk middel en de betekenis hiervan is vaak pas achteraf te doorgronden. Pas na de scherpe analyses van de televisie van McLuhan (1964) en Postman (1986) zijn we erin geslaagd de betekenis van de televisie voor samenlevingspatronen goed te doorgronden. En ook die betekenis verandert nog steeds. McLuhan laat zien dat we nieuwe technologieën alleen kunnen zien vanuit het perspectief van oude technologieën. Een auto werd daarom gezien als een *horseless carriage*. Simpel gezegd betogen McLuhan en Postman eigenlijk dat we niet weten wat we aan het doen zijn wanneer we nieuwe technologieën creëren. Dit betekent dat we nu al wel werken aan de vormgeving van de digitale overheid, maar wat dit bete-

kent kunnen we nog niet doorgronden. De overheid manoeuvreert door onbekend gebied.

Hoe kan de overheid op een intelligente wijze manoeuvreren door onbekend gebied? De analyse heeft laten zien dat zowel het gebruiken van nieuwe technologieën als het niet-gebruiken ervan leidt tot risico's, onzekerheden en problemen rondom overheidsverantwoordelijkheden. Té happig gebruik van nieuwe technologieën kan leiden tot *run away technology* en té terughoudend gebruik tot een in zichzelf gekeerde overheid. Hoe kan de overheid intelligent laveren tussen deze Skylla en Charybdis? Ik wil pleiten voor het creëren van een *genormeerde experimenteerruimte*: overheden dienen in bepaalde gevallen en onder bepaalde (proces)condities de mogelijkheid te krijgen om te experimenteren met nieuwe technologieën. Op deze wijze wordt een tijdelijke gedoogzone gecreëerd om nieuwe technologieën te ontwikkelen zonder dat de overheid zich direct overgeeft aan deze nieuwe technologieën. In de experimenteerruimte functioneert de overheid als een adhocratie, later vindt formalisering naar de (machine)bureaucratie plaats. In de gedoogzone kan worden geëxperimenteerd met nieuwe verdelingen van verantwoordelijkheden tussen overheden, burgers, bedrijven en maatschappelijke organisaties, voordat deze verantwoordelijkheden worden geformaliseerd.

Het creëren van genormeerde experimenteerruimte betekent dat bepaalde eisen aan het functioneren van de overheid tijdelijk worden opgeschort. In de experimenteerfase kan sprake zijn van enige mate van rechtsongelijkheid, onvoorspelbaarheid, onbehoorlijkheid en gebrek aan transparantie. Geaccepteerd wordt dat het tijdelijk opschorten van deze eisen ertoe kan bijdragen dat op termijn juist een betere invulling kan worden gegeven aan deze eisen, doordat nieuwe technologieën op een adequate wijze worden gebruikt. Codificatie van eisen aan het gebruik van nieuwe technologieën vindt niet vooraf plaats, maar op basis van deze experimenten.

Het invullen van een experimenteerruimte vergt allereerst een kader voor de terreinen waarop kan worden geëxperimenteerd. Wanneer is vallen en opstaan acceptabel? Welke risico's kunnen worden geaccepteerd? In het algemeen kan worden gesteld dat de ernst van de risico's bepaalt in welke mate er ruimte kan worden gegeven om te experimenteren. Zo zijn financiële risico's meer acceptabel dan risico's betreffende levens van burgers of pilaren van de democratische rechtsstaat. Vanuit deze gedachte is experimenteren ten behoeve van financieel beheer eerder acceptabel dan experimenteren met rechtsprekende computers of stemcomputers. Risico's op een onterechte veroordeling of fouten in de uitslag van verkiezingen zijn immers minder acceptabel dan het risico van financieel verlies door de overheid. Ook geldt dat de experimenteerruimte van de overheid kleiner zal zijn dan de ruimte van bedrijven, omdat er sprake is van een dwangrelatie met burgers en bedrijven. Idols zal eerder kunnen experimenteren met nieuwe tech-

nieken om te stemmen op de kandidaten dan de kiesraad. In de beurshandel kan eerder worden geëxperimenteerd met kennissystemen die de aankoop en verkoop van aandelen sturen dan in de rechtszaal waar besluiten over individuen worden genomen.

Daarnaast vergt de vormgeving van genormeerde experimenteerruimte beginselen voor de invulling van deze ruimte. Bij het formuleren van deze beginselen kan worden gekeken naar een andere sector met veel technologische vernieuwing en grote risico's: de farmaceutische sector. Voor de introductie van geneesmiddelen is een strikt traject geformuleerd dat bestaat uit vier fasen waarin het experiment steeds verder wordt uitgebreid. Er vindt een screening vooraf plaats – mag het geneesmiddel worden getest – en na elke fase worden de resultaten weer bekeken. Ook vindt er na de introductie van het geneesmiddel *postmarketing surveillance* plaats: de effecten van het geneesmiddel worden systematisch gemonitord. Op deze wijze kan er op gecontroleerde wijze om worden gegaan met risico's. In het geval van de geneesmiddelen is het College ter Beoordeling van Geneesmiddelen de toezichthouder. Bij experimenteren door overheden zal de volksvertegenwoordiging een dergelijke rol kunnen spelen.

Bij de oorspronkelijke vormgeving van de overheid werd door denkers als Max Weber (1968) met name gekeken naar stabiele instituties zoals het leger en de katholieke kerk. Invulling van verantwoordelijkheden van de overheid in het informatietijdperk vraagt om een nieuw model. Wellicht dient nu te worden gekeken naar hightech- en highrisk-bedrijven zoals deze bijvoorbeeld te vinden zijn in de farmaceutische sector. In deze sector worden nieuwe manieren van regulering ontwikkeld die gebaseerd zijn op geconditioneerde markttoelating. In een experimentele fase kunnen medicijnen onder strikte voorwaarden en gekoppeld aan strakke rapportageverplichtingen op de markt worden toegelaten (Boon et al. 2010). De systemen voor genormeerde experimenteerruimte die in deze sectoren zijn ontwikkeld kunnen helpen om de nieuwe verantwoordelijkheden van de overheid vorm te geven en intelligent te manoeuvreren in de virtuele wereld.

NOTEN

1 Een overzicht van de behoorlijkheidseisen van de Nationale Ombudsman is te vinden op http://www.ombudsman.nl/ombudsman/beoordeling/index.asp.

2 Zie hierover Pluut, B. (2010) *Het landelijk EPD als black box. Besluitvorming en opinies in kaart*, webpublicatie beschikbaar op www.wrr.nl.

LITERATUUR

Algemene Rekenkamer (2007) *Lessen uit ICT-projecten van de overheid,* Deel A, Den Haag.

Barnard, C. (1938) *The functions of the executive*, Cambridge MA: Harvard University Press.

Birdsall, W.F. (2000) 'The digital divide in the liberal state: a Canadian perspective', *First Monday* 5, 12 (beschikbaar op www.firstmonday.org).

Boon, W.P.C., E.H.M. Moors, A. Meijer & H. Schellekens (2010) '*Conditional approval as regulatory instrument for stimulating responsible drug innovation in Europe'*, Clinical Pharmacology & Therapeutics, 88, 6: 848-853.

Bovens, M.A.P. (1990) *Verantwoordelijkheid en organisatie. Beschouwingen over aansprakelijkheid, institutioneel burgerschap en ambtelijke ongehoorzaamheid,* Zwolle: W.E.J. Tjeenk Willink.

Bovens, M.A.P. (1999) *De digitale rechtsstaat. Beschouwingen over informatiemaatschappij en rechtsstaat*, Alphen aan den Rijn: Samsom.

Bovens, M.A.P., P. 't Hart, M.J.W. van Twist, & U. Rosenthal (2007) *Openbaar Bestuur; Beleid, organisatie en Politiek*, 7e editie, Alphen aan den Rijn: Kluwer.

Bovens, M. (2003) *De digitale republiek. Democratie en rechtsstaat in de informatiemaatschappij*, Amsterdam: Amsterdam University Press.

Broeders, D. (2010) 'EU, ICT en grensoverschrijdende mobiliteit van personen', WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.

Brouwer E. (2009) '*Juridische grenzen aan de inzet van migratietechnologie',* blz. 191-227 in Huub Dijstelbloem en Albert Meijer (red.) *De migratiemachine. De rol van technologie in het migratiebeleid*, Amsterdam: Van Gennep.

Bruijn, H. de, E.F. Ten Heuvelhof & R.J. in 't Veld, (1998) *Procesmanagement. Over procesontwerpen en besluitvorming,* Schoonhoven.

Burchell, G. (1993) Liberal government and techniques of the self. *Economy and society*: 22(3), 267-282.

Castells, Manuel (1996) *The rise of the network society, The information age: Economy, society and culture Vol. I.* Cambridge, MA/Oxford, UK: Blackwell.

Choenni, S., E. Leertouwer & T. Busker (2011) 'Klachten over toepassingen van informatietechnologie. Analyse van een aantal overheidsbestanden', WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.

Clarke, R.A. & R. Knake (2010) *Cyber war. The next threat to national security and what to do about it,* New York: Harper Collins.

Cohen, A. (2004) 'Surveying the Microsoft antitrust universe', *Berkeley Technology Law Journal* 19, 1: 333-364.

Commissie Toekomst Overheidscommunicatie (Commissie-Wallage) (2001) *In dienst van de democratie*: Den Haag.

Cooper, T.L. (1990) *The responsible administrator: An approach to ethics for the administrative role*, San Francisco, CA: Jossey-Bass.

Custers, B.H.M. (2003) 'Effects of unreliable group profiling by means of data mining', blz. 290-295 in G. Grieser, Y. Tanaka & A. Yamamoto (red.) *Lecture notes in artifi-*

cial intelligence, Proceedings of the 6th International Conference on Discovery Science (DS 2003) Sapporo, Japan. Berlin, Heidelberg, New York: Springer-Verlag, Vol. 2843.

Deursen, A.J.A.M. van & J.A.G.M. van Dijk (2008) *Digitale vaardigheden van Nederlandse burgers. Een prestatiemeting van operationele, formele, informatie en strategische vaardigheden bij het gebruik van overheidswebsites,* Enschede: Universiteit Twente.

Dijstelbloem, H. & A. Meijer (red.) (2009) *De migratiemachine. De rol van technologie in het migratiebeleid*, Amsterdam: Van Gennep.

Eeten, M. van (2011) 'Gedijen bij onveiligheid. Afwegingen rond de risico's van informatietechnologie', WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.

Franken, H. (1993) 'Kanttekeningen bij het automatiseren van beschikkingen', blz. 7-50 in *Beschikken en automatiseren*, VAR-reeks 110, Alphen aan den Rijn: Samsom H.D. Tjeenk Willink.

Frissen, P.H.A. (1999) *De lege staat*, Amsterdam: Nieuwezijds.

Groothuis, M.M. (2005) *Beschikken en digitaliseren. Over normering van de elektronische overheid,* (ITeR, 72), Den Haag: Sdu Uitgevers.

Groothuis, M.M. (2009) 'E-government en elektronisch bestuurlijk verkeer. Recente ontwikkelingen in jurisprudentie en wetgeving', *Tijdschrift voor Internetrecht*, 2: 9-13.

Groothuis, M.M. & S. van der Hof (2009) 'De elektronische handtekening in het bestuursrecht: ontwikkelingen in Nederland en Europa', *Computerrecht*, (5): 193-198.

Gutteling, J.M. & M. Kuttschreuter (2002) 'The role of expertise in risk communication: laypeople's and expert's perception of the millennium bug risk in the Netherlands', *Journal of Risk Research* 5 (1): 35-47.

Hart, H.L.A. (1968) *Punishment and responsibility: Essays in the philosophy of law,* New York: Oxford University Press.

Haydon, G. (1978) 'On being responsible', *The Philosophical Quarterly* 28: 46-57.

Hert, P. de (2010) *Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting*. WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.

Hildebrandt, M. & S. Gutwirth (2008) *Profiling the European citizen: Cross disciplinary perspectives*, Dordrecht: Springer.

Hof, C. van 't, R. van Est en F. Daemen (2010) *Check in/check out. De digitalisering van de openbare ruimte,* Rotterdam: NAi Uitgevers.

Jowett, G.S. & V. O'Donell (2006) *Propaganda and persuasion*, Thousand oaks, CA: Sage Publications.

Keizer, A. (2010) **'**De digitale patiënt centraal. Medische informatie in een digitale wereld' WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.

Kjaer, A. (2004) *Governance,* London: Sage.

Klink, B.M.J. van & W.J. Witteveen (2002) *De sociale rechtsstaat voorbij. Twee ontwerpen*

voor het huis van de rechtsstaat, Voorstudies en achtergronden WRR, Den Haag: Sdu Uitgevers.
Koops, B.-J., H. van Schooten & M. Prinsen (2004) *Recht naar binnen kijken: een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Driebergen-Rijsenburg: EJure.
Koppell, J.G.S. (2005) 'Pathologies of accountability: ICANN and the challenge of 'Multiple accountabilities disorder'', *Public Administration Review* 65, 1: 94-108.
Lyon, D. (2009) *Identifying citizens,* Cambridge: Polity Press.
Marx, G. (2009) 'A tack in the shoe and taking off the shoe', *Surveillance and society*, 6(3): 294-306.
McLuhan, M. (1964) *Understanding media: The extensions of Man*, New York: McGraw-Hill.
Meijer, A. (2004) *CC'tje naar de baas. E-mail en verandering in ambtelijke organisaties,* Den Haag: Boom Juridische Uitgevers.
Meijer, A. (2009) 'Informatietechnologie en verantwoordelijkheid: een onbeheersbare migratiemachine', blz. 157-189 in H. Dijstelbloem & A. Meijer (red.) *De migratiemachine. De rol van technologie in het migratiebeleid*, Amsterdam: Van Gennep.
Mintzberg, H. (1983) *Structure in fives. Designing effective organizations,* Englewood Cliffs: Prentice Hall.
Mulder, R. de (1998) 'The Digital Revolution: From Trias to Tetras Politica', blz. 46-56 in: I. Th. M. Snellen & W.B.H.J. van de Donk (red.) *Public administration in an information age. A handbook*, Amsterdam: IOS Press.
Mumford, L. (1970) *The myth of the machine: The pentagon of power, New York*: Harcourt Brace Jovanovich.
Nationale Ombudsman (2009) *Behoorlijkheidswijzer,* Den Haag.
Noordegraaf, M. (2004) *Managen in het publieke domein. Issues, instituties en instrumenten*, Bussum: Coutinho.
Porter, L.R. (1997) *Creating the virtual classroom: Distance learning with the Internet*, New York: John Wiley & Sons.
Postman, N. (1986) *Amusing ourselves to death*, New York: Penguin Books.
Prensky, M. (2001) Digital Natives, Digital Immigrants, *On the horizon*, 9(5): 1-6.
Snellen, I.Th.M. & W.B.H.J. van de Donk (1998) *Public administration in an information age. A handbook,* Amsterdam: IOS Press.
Snijders, T. (2011) Chief Information Officers bij de rijksoverheid, WRR-verkenning 25 *De staat van informatie*, Amsterdam: Amsterdam University Press.
Sunstein, C. (2001) *Republic.com,* Princeton, NJ: Princeton University Press.
Teeuw, W. et al. (2007) *Impact of converging technologies on future security applications,* Enschede: Telematica Instituut.
Thompson, D.F. (1980) 'Moral responsibility of public officials: the problem of many hands', *The American Political Science Review* 74, 4: 905-916.
Veld, Joris in 't & N.S.J. Koeman (1979) *Beginselen van behoorlijk bestuur*, Zwolle: W.E.J. Tjeenk Willink.
Vise, A. David & Mark Malseed (2005) *The Google story*, New York, NY.

Volkskrant, de (29 januari 2010, p. 2) 'Toe dan pc'tje, ik weet dat je het kan'; Acht politieregio's in het noorden en oosten kampen met haperende computers.

Weber, M. (1968) *Economy and society,* edited by Guenther Roth and Claus Wittich, New York: Bedminister Press.

Wetenschappelijke Raad voor het Regeringsbeleid (1998) *Staat zonder land. Een verkenning van de bestuurlijke gevolgen van informatie- en communicatietechnologie*, Den Haag: Sdu.

Willems, W. (2009) 'De politiek aan de knoppen van de machine: spraaktechnologie in het inburgeringsbeleid', blz. 123-156 in Huub Dijstelbloem & Albert Meijer (red.) *De migratiemachine. De rol van technologie in het migratiebeleid,* Amsterdam: Van Gennep.

Winner, L. (1977) *Autonomous technology. Technics-out-of-control as a theme in political thought,* Cambridge: MIT Press.

Winner, L. (1986) *The whale and the reactor. A search for limits in an age of high technology,* Chicago: The University of Chicago Press.

Wolbers, J. (2009) *Facing dilemmas in disaster management. Comparing structural arrangements for supporting an emergent reality,* Unpublished master thesis, Utrecht University.

Woodward, J.D., K.W. Webb, E.M. Newton, M. Bradley & D. Rubenson (2001) *Army biometric applications, identifying and addressing sociocultural concerns,* Santa Monica: RAND.

Zouridis, S. (2000) *Digitale disciplinering. Over ICT, organisatie, wetgeving en het automatiseren van beschikkingen,* Tilburg: Dissertatie Universiteit van Tilburg.

4 GEDIJEN BIJ ONVEILIGHEID. AFWEGINGEN ROND DE RISICO'S VAN INFORMATIETECHNOLOGIE

Michel van Eeten

4.1 WAAR MAKEN WE ONS DRUK OVER?

Stel, een financiële dienstverlener wil een internationaal betaalsysteem introduceren waarmee mensen betalingen op internet kunnen verrichten, tot duizenden euro's aan toe. Het enige dat ze nodig hebben is een getal van zestien cijfers dat op een kaartje is gedrukt, soms aangevuld met drie cijfers op de achterkant. Die gebruiksvriendelijkheid betekent ook dat iedereen die deze getallen weet ook het geld van de betreffende persoon kan uitgeven, overal en altijd, voor een ontelbaar aantal diensten. Bovendien is het systeem zo ingericht dat het getal zelden of nooit verandert en dat het in de loop van de tijd op honderdduizenden plekken opgeslagen zal worden.

De kans dat een zo fraudegevoelig systeem goedgekeurd zou worden lijkt klein. Mocht het daadwerkelijk tot invoering komen, dan lijkt het slechts een kwestie van tijd voor de eerste gevallen van fraude tot grote politieke verontwaardiging zouden leiden over de gebrekkige veiligheid.

Vergelijk dit voorstel met een ander systeem: een elektronisch betaalmiddel waarmee kleine bedragen kunnen worden afgerekend bij één specifieke dienstverlener, niet via internet, maar bij fysieke toegangslocaties. De kaarten waarmee wordt betaald bevatten versleutelde informatie die de klant zelf niet kan lezen. Via gespecialiseerde apparatuur zou de kaart gekopieerd kunnen worden, mits de fraudeur deze apparatuur fysiek nabij de kaart kan houden. Het geld dat zo buitgemaakt zou kunnen worden, kan alleen in kleine hoeveelheden besteed worden bij diezelfde dienstverlener.

Hoe groot is in dit geval de kans op goedkeuring? In ieder geval groter dan die van het eerste systeem, zou je denken. Het tweede systeem draait om beperkte, overzienbare risico's, ook in politiek opzicht.

De realiteit logenstraft deze inschatting. Het eerste voorstel, een vereenvoudigde beschrijving van het creditcardsysteem, is enkele decennia geleden ingevoerd. Het wordt inmiddels ruim vijftien jaar gebruikt voor internetbetalingen. Ondanks het grootschalig optreden van fraude, heeft het nog niet tot politieke ophef geleid. Het tweede voorstel, een vereenvoudigde beschrijving van de OV-chipkaart, is recent ingevoerd. Het heeft, ondanks het feit dat fraude vooralsnog voornamelijk in theorie voorkomt, geleid tot veel politiek tumult over de zogenaamd gebrekkige

veiligheid van het systeem[1]. De invoering van het systeem raakte vertraagd, politieke interventies dwongen aanvullende veiligheidsmaatregelen af en kostenramingen werden ruimschoots overschreden.

4.2 IS HET VEILIG?

Wat leert ons de merkwaardige uitkomst van deze vergelijking? Dat publieke oordeelsvorming over de veiligheid van informatietechnologie vaak de verkeerde vragen stelt. Het debat wordt gedomineerd door de vraag of iets veilig is. Die vraag kent strikt genomen maar één antwoord: nee. Dat antwoord is weinig zinvol – ook al is het correct, omdat gegeven eindige middelen veiligheid altijd onvolkomen zal zijn (Herley 2010). Of, zoals het fatalistische cliché stelt: honderd procent veiligheid bestaat niet.

De merkwaardige preoccupatie met de vraag of iets veilig is, komt mede voort uit het feit dat veiligheid zich verzelfstandigd heeft als specialisme – in het geval van informatietechnologie als een primair technisch specialisme. Dat heeft het misverstand geschapen dat deze mensen in staat zijn vast te stellen of iets veilig is. Het oordeel 'veilig' kan echter nooit gegeven worden. De expert zal aangeven wat de resterende risico's zijn en hoe deze eventueel gereduceerd kunnen worden. Vaak gaan experts een stap verder en stellen ze dat het ook wenselijk of zelfs noodzakelijk is dat deze risico's gereduceerd worden. Het is een bekend mechanisme dat experts optreden als belangenbehartigers van het probleemgebied waarop zij expertise bezitten – of dat nu duurzaamheid, armoedebestrijding, onderwijs of veiligheid is. Hun aanbevelingen komen voort uit een mengeling van goede bedoelingen, betrokkenheid en eigenbelang. Op het gebied van informatietechnologie zijn veel deskundigen tevens verkopers van veiligheidsadviezen en oplossingen. De meeste experts opereren dan ook vanuit een eenvoudig normatief schema: meer veiligheid is beter. Het feit dat er voortdurend veiligheidsincidenten optreden zien ze als afdoende bewijs voor de geldigheid van dat schema.

De vraag of meer veiligheid wenselijk is kan echter nooit beantwoord worden op basis van inzicht in de technische risico's of het optreden van incidenten. Er liggen allerlei impliciete en expliciete afwegingen ten grondslag aan veiligheidskeuzes. Veiligheid kost geld. Alleen al daarom is het economisch wenselijk een zekere mate van onveiligheid te tolereren. Of iets veilig genoeg is hangt af van de gevolgen van hogere of lagere veiligheid voor andere waarden, zoals efficiëntie, bruikbaarheid, toegankelijkheid, transparantie, vrijheid en innovatievermogen.

Het is begrijpelijk dat politiek en media zich wenden tot veiligheidsexperts bij het beoordelen van risico's. Daar is niets op tegen. Het probleem ontstaat pas doordat men veronderstelt dat de omvang van een risico bepaalt of dat risico acceptabel is. De vergelijking van OV-chipkaart en de creditcard maakte duidelijk dat die

veronderstelling niet deugt. De risico's van de OV-chipkaart zijn onweerlegbaar kleiner dan die van de creditcard en toch heeft men deze als onacceptabel beoordeeld. Een veel belangrijkere vraag is dan ook wie de gevolgen draagt van onveiligheid. In het geval van de OV-chipkaart leek fraude bij de gebruiker te belanden. Bij creditcards is contractueel geregeld dat de gebruiker gevrijwaard wordt van fraude. De vergelijking wijst uit dat het niet gaat om hoe groot een risico is in technisch opzicht, maar om wie dat risico draagt. Dat is het vertrekpunt van dit essay.

4.3 KOSTEN EN BATEN VAN ONVEILIGHEID

Elke vorm van informatietechnologie is intrinsiek onveilig. De constatering dat een systeem te kraken is of anderszins kan falen, kan nooit als een verrassing komen. Het uitgangspunt van elk debat over de veiligheid van informatietechnologie moet dan ook zijn: elk systeem zal falen, elk systeem is onveilig. De vragen die in de publieke oordeelsvorming centraal dienen te staan zijn de volgende. Wat zijn de consequenties van dat falen? Hoe waardevol is het terugdringen daarvan? Hoe zorgen we voor een balans tussen de kosten en baten van onveiligheid? Ja, er zijn ook maatschappelijke baten, soms zelfs zeer omvangrijke baten, verbonden met onveiligheid.

Dit vraagt om een economisch perspectief op veiligheidsrisico's van informatietechnologie. Werk op dit terrein heeft de laatste jaren een stormachtige ontwikkeling doorgemaakt. Een centrale uitkomst van het onderzoek is dat actoren onwenselijk grote risico's op falen nemen wanneer ze niet de totale kosten van dat falen dragen . In economische termen spreken we dan van een negatieve externaliteit – een vorm van marktfalen waarbij, in dit geval, een actor te weinig investeert in veiligheid, omdat de gevolgen van falen worden afgewenteld op andere spelers. Het omgekeerde treedt ook op: actoren die wel de baten, maar niet de kosten dragen van hogere veiligheid, hebben een prikkel om meer veiligheidsinvesteringen te eisen dan maatschappelijk wenselijk is. De OV-chipkaart lijkt hier een voorbeeld van.

Het economische perspectief biedt een helder uitgangspunt voor het bepalen van de rol van de overheid. Het is niet de taak van de overheid om het systeem veilig te maken, maar om de afwenteling van onveiligheid – de zogenaamde externaliteiten – op te sporen en arrangementen te ontwikkelen om die kosten neer te leggen bij de partijen die de baten incasseren van de veiligheidsrisico's. Het streven is dan, kort gezegd, naar een optimaal niveau van onveiligheid.

Juist rondom informatietechnologie treden externaliteiten op, omdat veel diensten het product zijn van netwerken en ketens van organisaties. Dat betekent dat er veel onderlinge afhankelijkheden bestaan en dat de veiligheid van een individuele actor mede wordt bepaald door de keuzes van anderen. Dat maakt de vraag

urgent welke mogelijkheden de overheid heeft in het terugdringen van veiligheidsexternaliteiten.

In dit essay dienen de termen 'kosten' en 'baten' breed opgevat te worden. Het zijn handzame termen die negatieve en positieve gevolgen aanduiden, in financiële zin, maar ook ten aanzien van andere waarden zoals toegankelijkheid, innovatie en privacy. Natuurlijk zullen actoren deze gevolgen anders ervaren en waarderen. De taal van het economische perspectief is wat dat betreft enigszins misleidend. Wanneer we spreken over het afwentelen van kosten, klinkt het alsof die kosten een onveranderlijk object zijn dat doorgegeven wordt van de ene actor naar de andere. Bij strikt financiële gevolgen snijdt dat beeld nog wel hout. Maar in veel situaties zullen de kosten en baten uiteenlopende vormen aannemen.
De actor die ze draagt, bepaalt welke gevolgen relevant zijn en of deze positief of negatief gewaardeerd worden. Het verplaatsen van kosten is dan vaak ook een vorm van transformatie. Een voorbeeld: luchtvaartmaatschappijen zijn financieel aansprakelijk voor de schade van een ongeval tijdens een van hun vluchten. Dat betekent dat doden en gewonden in geld uitgedrukt zullen worden. Niemand zal de fout maken te denken dat geld en het verlies van een mensenleven inwisselbaar zijn. Toch kunnen we zeggen dat de aansprakelijkheid, in economische zin, een deel van de kosten van het ongeval terugvoert naar de luchtvaartmaatschappij. Het internaliseren van kosten betekent dus niet dat deze ongewijzigd overgenomen worden – hetgeen in het geval van fatale ongevallen ook tot absurde implicaties zou leiden. Dat hoeft ook niet. Het gaat erom dat de gevolgen van veiligheidskeuzes voor andere actoren proportioneel meewegen in die keuzes. Als de private kosten en baten een weerspiegeling vormen van de sociale kosten en baten, dan zullen die keuzes tot maatschappelijk wenselijke uitkomsten leiden, zo luidt het uitgangspunt van het economisch perspectief op dit vraagstuk. Het laat open of die uitkomst meer of minder veiligheid betekent – en alleen al daarom biedt het perspectief een beter vertrekpunt voor publieke oordeelsvorming over de vraag wanneer we ons werkelijk druk moeten maken over risico's rond informatietechnologie.

Dit essay is als volgt opgebouwd. Eerst wordt besproken waarom falende veiligheid in beginsel een rationele uitkomst kan zijn van decentrale beslissingen waarin actoren de kosten en baten van hun veiligheidskeuzes tegen elkaar afwegen. Pas wanneer de kosten en baten van een actor niet congruent zijn met de kosten en baten voor de maatschappij, met andere woorden, wanneer er een externaliteit optreedt, is er een aanleiding om de decentrale afwegingen bij te sturen. In het tweede gedeelte verkennen we kort drie veiligheidsvraagstukken waarin externaliteiten optreden: de opkomst van botnets, fraude met online betalen en lekken uit grote databases. Daarna identificeren we de mogelijkheden die de overheid heeft om deze externaliteiten te verkleinen. Tot slot reflecteren we kort op de 'systeemverantwoordelijkheid' van de overheid, ook in het licht van andere beginselen, zoals transparantie, efficiëntie, privacy, identiteit en keuzevrijheid.

4.4 HET NUT VAN DECENTRALE AFWEGINGEN RONDOM VEILIGHEID

De laatste jaren worden we bestookt met berichten dat de schade ten gevolge van onveilige informatietechnologie explosief toeneemt.[2] Dit soort informatie wordt vaak gebruikt om aan te tonen dat marktpartijen de risico's onderschatten en te weinig in veiligheid investeren. Met andere woorden, dat de decentrale afwegingen van actoren tot maatschappelijk onwenselijke uitkomsten leiden. Dat is doorgaans de aanloop naar de bewering dat er meer in veiligheid moet worden geïnvesteerd, een beweging die regelmatig samengaat met de roep om overheidsbemoeienis.

Bij deze claims zijn twee belangrijke kanttekeningen te plaatsen. Ten eerste, de empirische onderbouwing van de bewering dat de schade snel oploopt is omstreden. Ten tweede, zelfs al loopt de schade op, dan is dat niet per se een indicatie van falende afwegingen van marktpartijen. We gaan kort op beide kanttekeningen in.

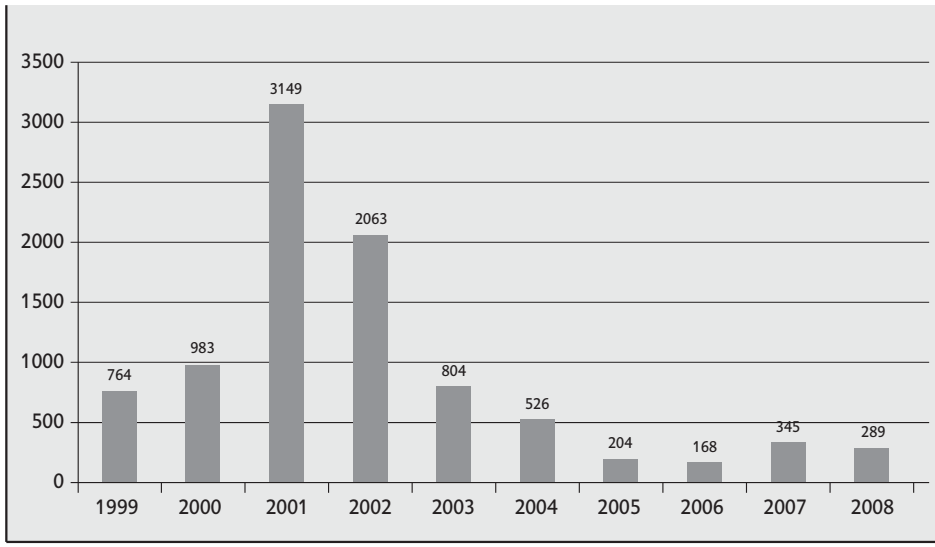
Er circuleren allerlei cijfers die de ernst van het probleem zouden schetsen. Tijdens een recente hoorzitting van het Amerikaanse Congres verklaarde de Chief Security Officer van AT&T dat cybercriminelen meer dan 1 biljoen dollar winst maken per jaar (Amoroso 2009). Eén biljoen, inderdaad. Er circuleren al jaren zulke onwaarschijnlijke schattingen. In 2000 publiceerden InformationWeek Research en PricewaterhouseCoopers een studie die de kosten van kwaadaardige software schatte op 1.5 biljoen dollar. De impact op Amerikaanse bedrijven met meer dan duizend werknemers werd geschat op 266 miljard dollar, oftewel ongeveer 2,7 procent van het bruto nationaal product (Cavusoglu 2004). Deze cijfers hebben vooral met elkaar gemeen dat de onderliggende data en methodologie niet inzichtelijk worden gemaakt.

Af en toe verschijnen er schattingen die transparanter onderbouwd zijn. Een studie naar enkele hypothetische wormuitbraken heeft op basis van een aantal aannames een schatting gemaakt van de schade (Weaver & Paxson 2004). Afhankelijk van de gehanteerde aannames gaat het om enkele tientallen tot enkele honderden miljarden dollars schade in de Verenigde Staten (VS) per uitbraak. Dat betreft vooral productiviteitsverliezen en de kosten van herstel.

Er zijn echter ook tegenstrijdige signalen over de schade. De slachtoffers van aanvallen spreken zelf regelmatig de schattingen tegen die experts maken over de schade die deze slachtoffers geleden zouden hebben (Denning 2000). Daarnaast is er de jaarlijkse *Computer Crime and Security Survey* van het Computer Security Institute – een van de weinige systematische pogingen om te achterhalen hoeveel schade publieke en private organisaties elk jaar leiden (CSI 2008). De organisaties die deelnemen aan de enquête rapporteren al jarenlang een afnemende hoeveelheid

schade, dwars tegen alle andere signalen in (figuur 4.1). De meeste schade vond plaats in de eerste jaren van de grootschalige worm- en virusuitbraken. Sindsdien namen de gerapporteerde verliezen ten gevolge van allerlei soorten veiligheidsincidenten snel af. De laatste jaren schommelen ze rond een stabiel laag peil.

Figuur 4.1 **Gemiddelde verliezen per organisatie door veiligheidsincidenten met informatietechnologie (in duizenden dollar)**



Bron: CSI Computer Crime & Security Survey 2008

Critici wijzen op de beperkingen van de enquête – zoals het kleine aantal respondenten, de zelfselectie door respondenten en de onderschatting van respondenten van de werkelijk geleden schade. Maar dat laat onverlet dat dit een van de schaarse herhaalde empirische metingen betreft. Het is weinig overtuigend om deze data te negeren ten gunste van speculatie en anekdotische informatie.

Ook technische data over het aantal veiligheidsincidenten roepen tegenstrijdige interpretaties op. Er verschijnen regelmatig studies van experts en van commerciële beveiligingsbedrijven die de noodklok luiden over het toenemende aantal aanvallen of de hoeveelheid kwaadaardige software die wordt aangetroffen in het wild (Zittrain 2008; Symantec 2008). Maar deze cijfers zeggen niets over economische schade en eigenlijk ook weinig over de hoeveelheid aanvallen. De tellingen lopen soms op door veranderende technische tactieken van de aanvallers. Een voorbeeld: om antivirussoftware te verslaan hebben de aanvallers methoden ontwikkeld die elk stuk malware – een samentrekking van *malicious software* – in ontelbare varianten in omloop brengen. Het gaat feitelijk om steeds dezelfde malware. De minuscule variaties worden automatisch aangebracht, omdat het detectering en

bestrijding belemmert. Uiteraard loopt daardoor het aantal stukken malware dat in het wild wordt aangetroffen explosief op. Die telling is echter daarmee ook onbruikbaar geworden als een indicator voor de toename van het probleem, omdat het nu niet meer werkelijk verschillende aanvallen betreft. Hetzelfde geldt voor veel andere technische indicatoren. Ze passen niet bij de dynamiek van de wapenwedloop tussen aanvallers en verdedigers van informatietechnologie.

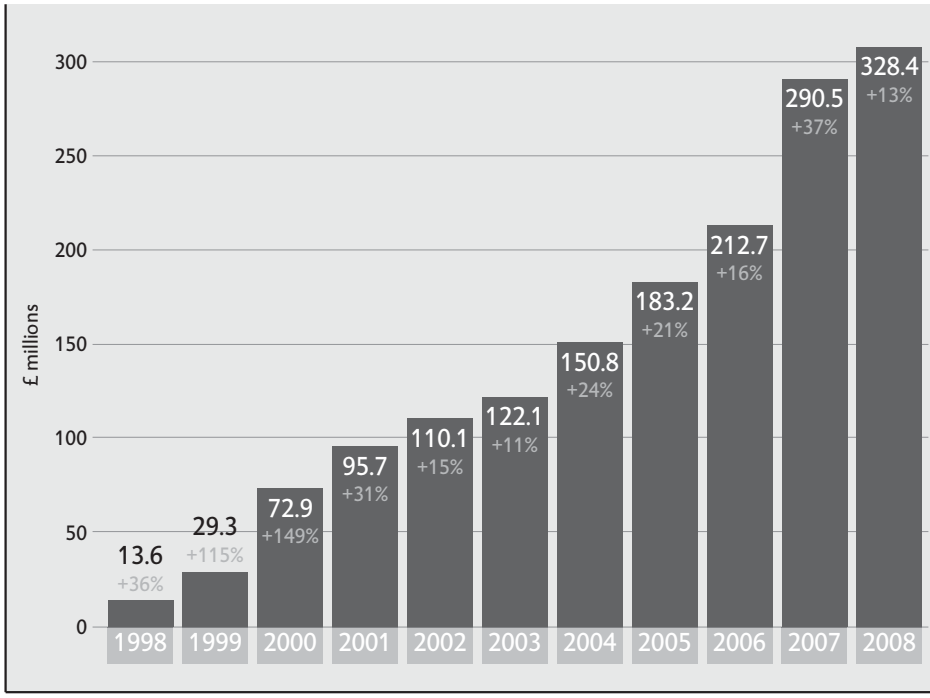
Belangrijker nog is het feit dat het toenemende aantal aanvallen juist het gevolg kan zijn van de effectievere bestrijding en afnemende effectiviteit van diezelfde aanvallen. De aanvallers pogen het verloren terrein steeds te compenseren. Neem *phishing*-aanvallen – pogingen om via misleidende e-mailberichten gebruikers te verleiden tot bepaalde handelingen, zoals het afstaan van inloggegevens. Een recent rapport signaleert een groter aantal aanvallen in 2009. Die worden echter gemiddeld veel sneller geneutraliseerd dan het jaar ervoor (Aaron & Rasmussen 2010). Een andere studie vindt empirische aanwijzingen dat het aantal phishing-aanvallen oploopt omdat de aanvallers met elkaar concurreren in een situatie die lijkt op een *tragedy of the commons*. Het oplopende aantal aanvallen is juist het gevolg van teruglopende opbrengsten, van de afnemende effectiviteit van eerdere aanvallen, zo betogen de onderzoekers (Herley & Florencio 2008).

Kortom, er zijn goede redenen om kritisch te zijn tegenover claims waarin een veiligheidscrisis rondom informatietechnologie wordt afgekondigd. Maar zelfs als de claims waar zijn, dan leidt dat nog niet tot de conclusie dat marktpartijen op dit moment te weinig investeren in veiligheid.

Neem de goed onderbouwde berichten over toenemende fraude met online betalingsverkeer. De beste cijfers uit de financiële sector zijn beschikbaar voor het Verenigd Koninkrijk. Daaruit blijkt dat fraude met online betalingsverkeer (*card-not-present* fraude) al jaren oploopt (APACS 2009). In 2008 bedroeg deze schade ongeveer 360 miljoen euro (zie figuur 4.2). Dit is een stijging van 350 procent ten opzichte van 2000. De groei baart de banken zorgen, ook omdat dit nu de grootste vorm van fraude is geworden. Daar staat tegenover dat in dezelfde periode de waarde van online winkelen in het Verenigd Koninkrijk groeide met 1077 procent, naar ongeveer 45 miljard euro in 2008. In relatieve zin nam de fraude dus af.

Dezelfde trend zien we bij de creditcardmaatschappijen. In 2007 rapporteerde VISA Europe dat hun fraudepeil een historisch dieptepunt had bereikt, namelijk 0,051 procent van het totale transactievolume. Met andere woorden, ongeveer vijf cent per honderd euro (House of Lords 2007). Dat zijn cijfers die representatief zijn voor de sector als geheel (Sullivan 2010; MacCarthy 2010). In dat licht moet ook de stijging gezien worden van andere vormen van online fraude. De Federal Bureau of Investigation (FBI) rapporteerde onlangs dat de schade waarover men klachten ontving, was opgelopen van 265 miljoen dollar in 2008 tot bijna

Figuur 4.2 Card-not-present fraude in het Verenigd Koninkrijk (in miljoenen GPB)



Bron: APACS, 2009

560 miljoen dollar in 2009 (Internet Crime Complaint Center 2010). Die sprong in een jaar mag verrassend zijn, het onderliggende patroon van de afgelopen tien jaar niet. Net als in het Verenigd Koninkrijk nam in die periode de economische waarde van online transacties sneller in waarde toe dan de fraude.

Dat de schade in absolute zin oploopt, maar in relatieve zin afneemt, is cruciaal. In veel gevallen stijgen de baten van de risiconemende activiteiten sneller dan de fraude. Van een crisis is dan geen sprake. Desalniettemin zou je kunnen stellen dat de stijgende fraude onwenselijk is en eisen dat de betreffende organisaties deze proberen terug te dringen. Maar dat gaat voorbij aan een belangrijk gegeven: het nemen van aanvullende veiligheidsmaatregelen heeft vaak een belemmerend effect op de stijging van de baten.

Neem creditcards. De maatschappelijke baten van het laagdrempelig en efficiënt kunnen afwikkelen van financiële transacties via internet zijn vele malen hoger dan de kosten van de nieuwe vormen van fraude. Dat weten we tamelijk zeker, omdat de fraude gedragen wordt door dezelfde partij die een deel van de baten incasseert: de creditcardmaatschappijen. Die partij heeft het meeste inzicht in de reële omvang van de kosten en baten. Terugdringen van risico's is in zulke geval-

len niet altijd wenselijk, omdat het ook snijdt in de baten die gepaard gaan met die risico's. Het transactievolume stijgt zo snel, juist omdat nauwelijks drempels worden gecreëerd voor gebruik. Fraudebestrijding heeft zich tot voor kort vooral in de backoffice van de creditcardmaatschappijen afgespeeld, niet bij het afwikkelen van de transactie door de gebruiker. Maatregelen die wel tot drempels leiden bij het gebruik veroorzaken al snel meer schade – door minder groei – dan ze aan fraude voorkomen. Zolang deze bedrijven de schade van getroffen klanten vergoeden, hoeft een zekere fraudetolerantie geenszins tot afnemend vertrouwen te leiden.

De waarde van decentrale afwegingen geldt ook voor andere vormen van online dienstverlening. Het succes van die diensten is, zoals bekend, nauw verbonden met het feit dat informatietechnologie een radicale daling van de transactiekosten mogelijk maakt. Als veiligheid de transactiekosten verhoogt, hoe bescheiden ook, belemmert het al snel de groei van die diensten – en dus ook van maatschappelijke efficiëntiewinsten die ermee gepaard gaan. Niemand heeft meer inzicht in die kosten en baten dan de marktpartijen zelf. Het decentrale karakter van die afwegingen schept bovendien een variëteit aan strategieën, omdat de onzekerheid over kosten en baten de marktpartijen zal verleiden tot andere inschattingen. Dit versterkt weer het leren via trial and error over de afwegingen tussen veiligheid en andere beginselen, zoals efficiëntie, innovatie, privacy en keuzevrijheid. Een belangrijke voorwaarde voor de effectiviteit van dat leren is dat marktpartijen zelf, in ieder geval gedeeltelijk, de gevolgen dragen van foute inschattingen. Daardoor kunnen ze hun afwegingen bijstellen.

Een voorbeeld: PayPal, de aanbieder van online betalingsdiensten, heeft vanaf het begin moeten vechten tegen fraude. Het succes van de dienst is met name gebaseerd op de eenvoud van het gebruik. Een gebruikersnaam en wachtwoord zijn genoeg. Dat is relatief fraudegevoelig. Toen PayPal werd gekocht door eBay kreeg men nieuwe mogelijkheden om toegankelijkheid, efficiëntie en veiligheid met elkaar in evenwicht te brengen. Doordat eBay veel informatie had over haar gebruikers – dankzij haar uitgebreide reputatiesystemen – kon men de betalingsdiensten koppelen aan reputaties. Dat stelde PayPal in staat om het risico van fraude zo precies in te schatten dat de tarieven omlaag konden en de fraude op een acceptabel niveau gehouden kon worden, zonder extra handelingen van de gebruikers te eisen, die immers weer de transactiekosten zouden verhogen. Hierdoor konden eBay en PayPal samen nieuwe garanties en bescherming bieden voor kopers die betaalden via de dienst. Dat kon veel efficiënter dan bij een *stand alone* financieel dienstverlener, omdat men de risico's aanzienlijk preciezer kon schatten op basis van de reputatie van gebruikers (Anderson 2007). Hier zien we delicate afwegingen tussen privacy, veiligheid en efficiëntie die alleen mogelijk zijn doordat ze decentraal plaatsvinden.

De mogelijkheid om gestuurd door reële ervaringen – in plaats van door experts, generieke normen of modieuze opvattingen – de wenselijke balans te vinden

tussen verschillende waarden is een unieke eigenschap van decentrale afwegingen. Daar waar inzicht en ervaring ontbreken en men bepaalde risico's toch wil afdekken, ontstaan verzekeringen. In de VS zijn polissen voor risico's rond informatietechnologie een van de snelst groeiende segmenten van de verzekeringsmarkt.[3]

Generieke veiligheidsnormen en andere centrale ingrepen werken verstorend in deze afwegingen. Zelfs als ze erin slagen om de schade terug te dringen, hetgeen allerminst vanzelfsprekend is, dan kunnen de maatschappelijke kosten hiervan groter zijn dan de schade die voorkomen wordt.[4] Pas wanneer de kosten en baten van een actor niet congruent zijn met de kosten en baten voor de maatschappij, met andere woorden, wanneer er een externaliteit optreedt, is er een aanleiding om de decentrale afwegingen bij te sturen. In de volgende paragraaf bespreken we het optreden van externaliteiten.

4.5 EXTERNALITEITEN ROND VEILIGHEIDSRISICO'S

Het klassieke voorbeeld van een externaliteit is de milieubelasting die ontstaat tijdens de productie van bepaalde goederen. De kosten van die belasting worden in beginsel niet meegewogen door de producenten, waardoor deze, gegeven een bepaald prijsniveau, meer zullen produceren dan maatschappelijk gezien wenselijk is. Door het opleggen van milieunormen of -heffingen kunnen deze kosten worden geïnternaliseerd bij het bedrijf, waardoor deze, bij benadering, de werkelijke kosten dragen en ze het maatschappelijk optimale productieniveau zouden kiezen.

De externaliteiten rondom informatietechnologie worden regelmatig vergeleken met dit klassieke voorbeeld. In analogie met milieunormen circuleren er pleidooien om bijvoorbeeld softwareproducenten aan kwaliteitsnormen te onderwerpen of om ze aansprakelijk te stellen voor kwetsbaarheden in hun software die schade bij derden veroorzaken (Schneier 2007). De analogie is echter enigszins misleidend. De milieuschade wordt door het producerende bedrijf zelf veroorzaakt. Dat maakt het eenvoudig om de bron aan te wijzen. Belangrijker nog, dat maakt het normatief gezien wenselijk om de milieuschade te internaliseren bij dat bedrijf.

Veiligheidsproblemen vinden echter hun oorsprong vaak in crimineel gedrag. De omvang van de problemen wordt weliswaar beïnvloed door de keuzes van bonafide marktpartijen, maar zij zijn niet de veroorzakers. Dat maakt het principe omstreden dat de kosten geheel moeten worden geïnternaliseerd door die partijen. Of het nu gaat om softwareproducenten wier software fouten bevat, internetserviceproviders (ISP's) waarvan de netwerken kwaadaardig verkeer voortbrengen of eindgebruikers wier besmette machines gebruikt worden voor aanvallen – in al deze gevallen kunnen de betreffende partijen de veiligheidsrisico's verminderen, maar het is onredelijk en onwenselijk om hen de gevolgen van die risico's geheel te

laten dragen. In alle markten komt criminaliteit voor en tot op zekere hoogte tolereren we dit, omdat de nadelen van zero tolerance veel groter zijn.

Met deze kanttekening in het achterhoofd verkennen we kort drie situaties waar de ongelijke verdeling van kosten en baten van veiligheid over marktpartijen aanleiding geeft tot externaliteiten: de opkomst van botnets, fraude met online betalen en lekken uit grote databases. Vervolgens zullen we ingaan op potentiële beleidsmaatregelen om deze externaliteiten terug te dringen.

4.5.1 OPKOMST VAN BOTNETS

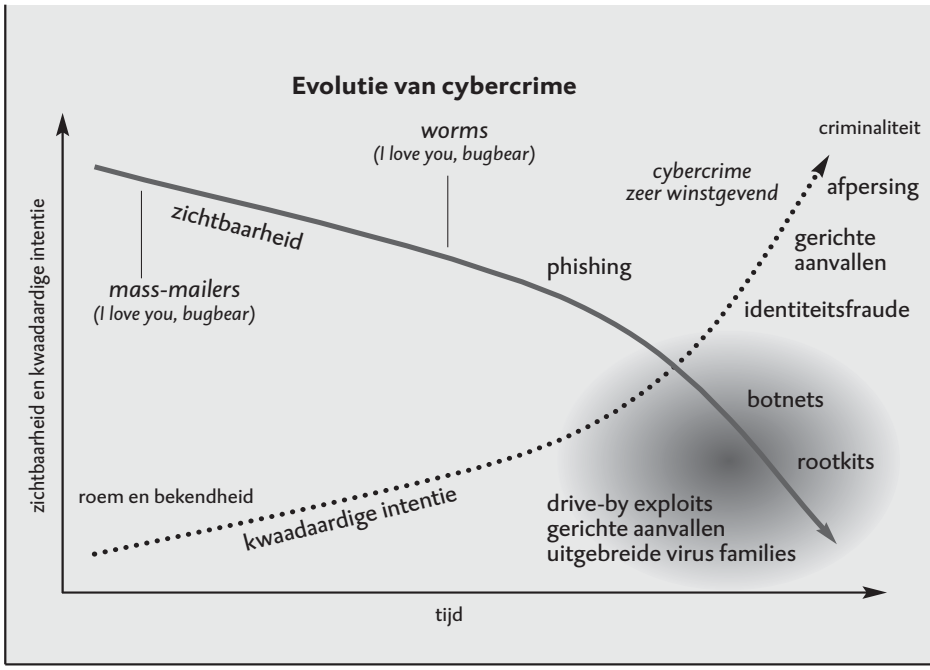
Naar schatting zijn tussen de één en tien procent van alle computers die met internet zijn verbonden, besmet met kwaadaardige software (Clayton 2010). Veel van die machines behoren toe aan eindgebruikers die zelf niet weten dat hun computer geïnfecteerd is. De machines worden door de aanvallers bijeengebracht in netwerken, 'botnets'. De opkomst van botnets wordt gezien als een van de meest kritieke veiligheidsproblemen van dit moment (OECD 2009). Een recente studie heeft aangetoond dat 5-10% van alle Nederlandse internetabonnees in 2009 een besmette computer in een botnet heeft gehad (Van Eeten et al. 2011).

Er zijn honderden botnets gedetecteerd, qua grootte uiteenlopend van enkele duizenden tot enkele miljoenen geïnfecteerde machines.[5] Deze netwerken kan men op afstand voorzien van nieuwe opdrachten en software. Op die manier vormen ze krachtige en flexibele platforms voor allerhande criminele activiteiten, zoals identiteitsfraude, spamdistributie, fraude met online advertentiesystemen, *distributed-denial-of-service* aanvallen, oplichting via frauduleuze veiligheidssoftware (*scareware*) en het hosten van phishing sites (OECD 2009).[6] Daarnaast worden botnets gebruikt voor bijvoorbeeld politieke doeleinden. In het voorjaar van 2007 gebruikte een aan het Kremlin gelieerde jeugdbeweging een botnet van bescheiden proporties om de internetvoorziening van Estland wekenlang te ontregelen (Davis 2007). Tijdens het gewapende conflict tussen Rusland en Georgië werd de laatste getroffen door botnetaanvallen (Markoff 2008). Daarnaast zijn botnets gebruikt voor aanvallen op de zogenaamde *root servers* – die aan de top staan van de technische infrastructuur voor het gebruik van domeinnamen op internet (ICANN 2007).

In de loop van het afgelopen decennium heeft kwaadaardige software (malware) een fundamentele verandering ondergaan. Rond 2001 en 2002 vonden de eerste wereldwijde virus- en wormuitbraken plaats. Deze malware had geen ander doel dan zichzelf te verspreiden en de aandacht te trekken, vaak door de besmette machine te ontregelen. De uitbraken zorgden weliswaar voor substantiële economische schade door productiviteitsverliezen, maar deze malware had verder geen winstmotieven. Dat is in de jaren daarna veranderd. Malware is vooral verder

ontwikkeld om winstgestuurde vormen van criminaliteit te ondersteunen. De ondergrondse economie heeft zich sterk geprofessionaliseerd en gespecialiseerd (Bauer et al. 2008). Voor criminele doeleinden is het veel effectiever om de aanwezigheid van malware op de besmette machines te maskeren, in plaats van luidruchtig kenbaar te maken, zoals de eerdere generaties deden. Malware is inmiddels zo ingenieus dat de gebruiker niet of nauwelijks iets merkt van het feit dat zijn machine wordt ingezet voor kwaadaardige doeleinden. Deze trends zijn samengevat in figuur 4.3, waarin de x-as het tijdsverloop weergeeft.

Figuur 4.3 Trends in kwaadaardige software sinds 2000



Bron: GovCERT.nl

Deze ontwikkelingen hebben de verdeling van kosten en baten over marktpartijen aanzienlijk veranderd. Daarmee is ook de prikkelstructuur, de verzameling van factoren die bepaald gedrag van marktpartijen belonen of ontmoedigen, gewijzigd. Geïnfecteerde eindgebruikers droegen aanvankelijk primair zelf de kosten van hun gebrekkige beveiliging. Inmiddels hebben de kosten zich verplaatst. Malware wordt weliswaar ook ingezet tegen de eigenaar van de machine, maar de meeste vormen van crimineel gebruik richten zich tegen derden. Met andere woorden, de eindgebruikers zijn een belangrijke bron van externaliteiten geworden. Ze wentelen de kosten van hun onveiligheid af op andere marktpartijen, onder andere op ISP's, e-commercebedrijven, banken en beheerders van zoekmachines. Meer diffuus worden er kosten afgewenteld op de samenleving als geheel, door bijvoor-

beeld hogere kosten van online dienstverlening en de kosten van opsporing en vervolging. Anders gezegd: investeren in betere beveiliging wordt ontmoedigd. Eindgebruikers zouden wel de kosten daarvan dragen, maar de baten, een afname van de aanvallen op derden, gaan in belangrijke mate naar andere partijen. In zulke situaties zullen actoren te weinig investeren in veiligheid.

Overheden hebben de afgelopen jaren voorlichtings- en bewustwordingscampagnes ingezet om eindgebruikers te bewegen tot een betere beveiliging. Inmiddels kunnen we vaststellen dat dit weliswaar nuttig is, maar een zeer beperkte effectiviteit heeft. De omvang van de problemen neemt eerder toe dan af. Een recente internationale enquête concludeerde dat tweederde van alle internetgebruikers slachtoffer is geworden van kwaadaardige software of erger . Dit komt ook doordat de aanvallen zo geavanceerd zijn geworden dat de gebruikelijke adviezen aan eindgebruikers achterhaald raken. Virusscanners detecteren tegenwoordig nog maar een gedeelte van de hoeveelheid malware die voorkomt op internet (Grossman 2007). Het is voor eindgebruikers met beperkte technische expertise bijna ondoenlijk geworden om hun machine adequaat te beveiligen.

Daarnaast geldt dat de passiviteit van eindgebruikers in allerlei opzichten rationeel te noemen is. De indirecte kosten van het opvolgen van veiligheidsadviezen zijn vaak hoger dan de verwachte baten van de hogere veiligheid die ermee gewonnen wordt, zelfs voor de samenleving als geheel (Herley 2009). Op het niveau van de individuele gebruiker mag het rationeel zijn, het gevolg is wel dat zij als groep een van de grootste bronnen van externaliteiten zijn geworden (Van Eeten & Bauer 2008).

4.5.2 FRAUDE MET ONLINE BETALINGSVERKEER

Met de toename van online betalingsverkeer is ook de fraude toegenomen. Al jarenlang wordt op grote schaal gefraudeerd met internetbankieren, creditcards en aanverwante diensten als iDeal. De technische tactieken van die aanvallen verschillen, van *social engineering* tot en met het op afstand overnemen van de machine van de eindgebruiker. Bij het gebruik van malware kan de aanvaller de communicatie tussen gebruiker en bank manipuleren, zonder dat een van beide partijen dat waarneemt. De bestaande veiligheidsmaatregelen kunnen zo worden omzeild.

Is er hier sprake van een externaliteit? Er zijn hier drie marktpartijen die in een positie verkeren om het risico te reduceren: eindgebruikers, financiële dienstverleners en softwareproducenten. Die laatste spelen een rol ten aanzien van het belemmeren van de besmetting van de machine, maar komen verder in de discussie nauwelijks voor. Wel helpen ze mee in algemene zin met het bestrijden van malware.

De banken stellen dat de eindgebruiker in principe zelf verantwoordelijk is voor de beveiliging van zijn of haar machine. Daar is veel voor te zeggen. Aan de andere

kant moeten we constateren dat het geen reële eis meer is dat de eindgebruiker de machine adequaat kan beveiligen. Men kan de gebruiker vragen bepaalde voorzorgsmaatregelen te nemen, maar ook met die maatregelen blijft fraude mogelijk. De adviezen uit de campagne '3x kloppen' van de banken waren al verslagen door aanvallers, nog voordat de campagne werd gelanceerd. Het lijkt dan ook een beter uitgangspunt om de machine van de eindgebruiker als intrinsiek onbetrouwbaar te beschouwen en de dienstverlening vanuit dat uitgangspunt te ontwerpen.

De bank kan bepalen hoe de dienst is ingericht en hoe de klant deze kan gebruiken. Het is de keuze van de bank geweest om dienstverlening te laten verlopen via de webbrowser, het meest aangevallen stuk software van het afgelopen decennium. Men koos daarvoor, omdat het de toegankelijkheid van die diensten aanzienlijk zou verhogen. Nu konden ze vanaf elke pc worden gebruikt, zonder dat er speciale software benodigd was.

De keuze om de diensten toegankelijker te maken is zonder meer legitiem. Deze keuze laat echter ook zien welke kosten en baten de banken ervaren rondom veiligheid. Net als de creditcardmaatschappijen verdienen de banken geld per transactie – al is het in geval van internetbankieren vooral de besparing van geld per transactie, omdat transacties via internet nagenoeg gratis zijn, terwijl papieren transacties of lokethandelingen veel meer kosten met zich meebrengen. Die baten betekenen dat zij een zo groot mogelijk transactievolume nastreven. Dat betekent dat men ontmoedigd wordt om maatregelen te nemen die de groei van dat volume zouden belemmeren. Er zijn allerlei maatregelen denkbaar die de risico's voor eindgebruikers zouden verkleinen. Sommige daarvan zijn op zichzelf relatief goedkoop. Men zou bijvoorbeeld gebruikers 'live cd's' kunnen verstrekken, waarmee een computer kan worden opgestart met een schoon besturingssysteem (Krebs 2009). Men zou, nog goedkoper, gebruikers kunnen aanraden een dergelijke cd zelf te maken. De software daarvoor is gratis beschikbaar op internet. Maar die maatregelen stelt men niet voor.

De enige verklaring voor deze keuzes is dat men de drempel voor gebruik niet wil verhogen. Daar is veel voor te zeggen. Als drempels leiden tot een langzamere groei in het gebruik van online financiële diensten, dan zal de schade daarvan voor de banken aanzienlijk groter zijn. Er worden miljarden bespaard door de migratie van transacties van papier en kantoor naar internet. Het gaat om honderden miljarden transacties per jaar. Elke vertraging in die migratie betekent efficiëntieverliezen voor de bank en voor de samenleving die de omvang van fraude veruit overschaduwen – het gaat om miljarden aan efficiëntiewinsten versus miljoenen aan fraude. Ook in maatschappelijk opzicht is het dus onwenselijk dat fraudebestrijding ten koste gaat van de groei van het transactievolume. De samenleving profiteert overal van goedkoop betalingsverkeer.

Het is echter cruciaal wie de schade draagt die samengaat met het huidige veiligheidsniveau. Daarover bestaat onduidelijkheid. Banken zeggen regelmatig dat ze de schade vergoeden. Maar de regelgeving dwingt dat niet af en gebruikers hebben niet of nauwelijks mogelijkheden om banken aan die toezegging te houden. De regelgeving staat toe dat banken claims afwijzen, omdat ze niet aansluit bij de complexe en veranderlijke aard van internetfraude (Steennot 2008; Spindler 2007). In de praktijk besluit de bank zelf of ze het redelijk vindt om schade te vergoeden. Juridisch verweer tegen zo'n beslissing is lastig. De kosten van de rechtsgang zijn hoog, men kan opdraaien voor de proceskosten en de rechters hebben zich vaak onkritisch opgesteld tegenover de technische beweringen van de banken (Murdoch 2009).

Er is geen extern toezicht op de claim van banken dat ze schade vergoeden. We hebben goede aanwijzingen dat schade wel degelijk deels terechtkomt bij klanten. In december 2008 bracht het televisieprogramma *Kassa* achttien klanten van de Postbank bijeen die samen voor 212.000 euro bestolen waren. De bank had alle claims afgewezen. De makers van het programma stapten eerst naar het Klachteninstituut Financiële Dienstverlening (KiFid), maar het instituut gaf de Postbank gelijk. Dat patroon, klachteninstituten en financiële ombudsmannen die de banken gelijk geven, zien we ook terug in andere Europese landen (Anderson & Bohm 2008). Pas door de publiciteit van het programma werd alsnog de schade vergoed. In werkelijkheid ging het niet om achttien maar om een kleine tweehonderd slachtoffers. En dat bij één aanval op één bank.

Dit incident is geen uitzondering. De historie leert dat banken regelmatig terechte claims afwijzen. In de eerste jaren waarin *skimming* plaatsvond, wezen banken routinematig de schadeclaims af. Ze controleerden of de transactie voorzien was van de pincode. Als de pincode was ingevoerd, ging men ervan uit dat de klant zelf had gefraudeerd of nalatig was geweest door de pincode niet geheim te houden. De rechters volgden doorgaans die redenering. Ten onrechte, want de criminelen hadden methoden om ook de pincodes te achterhalen van de kaarten die ze hadden gekopieerd. Pas toen *skimming* op zo'n grote schaal voorkwam dat de banken het niet langer konden ontkennen, is men schade structureel gaan vergoeden en ook zelf gaan opsporen. Ondertussen was er wel al een groep slachtoffers ontstaan die buiten hun schuld gedupeerd was. De omvang van die groep is niet bekend. In de jaren negentig voerden enkele duizenden Britse slachtoffers een rechtszaak tegen dertien banken, die allen hun claims hadden afgewezen. Die zaak werd door de banken gewonnen (Anderson et al. 2005).

Dit alles suggereert dat er behoorlijk wat schade terechtkomt bij klanten. De Nederlandse banken publiceren geen statistieken over de omvang van internetfraude. Hun Britse collega's doen dat wel. In 2008 vond daar voor ongeveer 360 miljoen euro aan fraude plaats – card-not-present fraude, waarvan de bulk bestaat uit

fraude met online betalingsverkeer. Ter vergelijking: de schade van skimming bedroeg een kleine 190 miljoen euro (APACS 2009). De Nederlandse banken publiceren sinds kort wel, op verzoek van de overheid, de schade van skimming. In 2008 bedroeg deze 31 miljoen euro.[7] Als hier dezelfde verhouding tussen skimming en internetfraude zou bestaan als in het Verenigd Koninkrijk, dan zou in Nederland de fraude zo'n 59 miljoen euro bedragen. In werkelijkheid ligt het waarschijnlijk aanzienlijk lager, maar de vergelijking maakt aannemelijk dat het om een substantieel bedrag gaat. Een deel daarvan zal bij klanten terechtkomen. Een recente Britse enquête stelde dat 20 procent van de mensen die schade hadden geleden, die schade niet vergoed kregen door hun bank (Murdoch 2009).[8]

De banken claimen dat ze de schade vergoeden, maar ze zijn niet bereid die claim in een garantie om te zetten waarop consumenten kunnen vertrouwen. Die discrepantie roept vraagtekens op, mede in het licht van de aanverwante claim van banken dat de totale schade erg meevalt. Als de schade meevalt, deze inderdaad al vergoed zou worden door banken, op grond waarvan kan men dan tegen de codificatie van de bestaande situatie zijn? Die zou de consumenten bescherming bieden die nu geheel ontbreekt. Soms wordt het probleem van *moral hazard* aangehaald als argument: als consumenten niet langer aansprakelijk zijn, dan worden ze laks. Maar voor dat probleem bestaat al lang een oplossing: eigen risico.

Waar de Europese regelgeving weinig bescherming biedt voor consumenten, daar heeft de Amerikaanse overheid al in de jaren zeventig de banken volledig aansprakelijk gesteld, op een eigen risico na van 50 dollar.[9] De financiële instellingen hebben zich eerst met man en macht verzet tegen die wetgeving. Maar al snel beseften ze dat het een zegen was. De banken hoefden hun investeringen in veiligheid niet langer publiekelijk te verantwoorden, omdat ze zelf de schade droegen. Het gevolg was dat ze veel minder gingen uitgeven aan veiligheid dan Europese banken (Anderson & Moore 2006). Die besparingen alleen al waren groter dan de schade die ze moesten vergoeden. Belangrijker nog: het gebruiksgemak voor klanten werd niet belemmerd door veiligheidsmaatregelen, waardoor de migratie naar online betalingsverkeer niet werd geremd. De bescherming van klanten gold niet voor de zakelijke markt. De afgelopen jaren verplaatst de fraude zich dan ook naar de rekeningen van zakelijke gebruikers. Daar is bovendien de potentiële buit veel groter. En dus komen steeds vaker zaken in het nieuws waar het midden- en kleinbedrijf tienduizenden en zelfs honderdduizenden dollars schade oploopt door geplunderde rekeningen.[10] Hoe dit aansprakelijkheidsvraagstuk geregeld moet worden is nog volop inzet van een politieke strijd.

De vraag of de veiligheidskeuzes van banken externaliteiten genereren is niet eensluidend te beantwoorden. De keuzes van verschillende partijen beïnvloeden elkaar en de oorsprong van de fraude ligt uiteraard bij geen van hen, maar bij criminelen. Duidelijk is wel dat de banken afwegingen maken die de risico's voor

hun klanten minder ver terugdringen dan zou kunnen. Ze zeggen de schade te vergoeden, maar dat is vooralsnog weinig meer dan een papieren bewering. Formeel gezien zijn ze doorgaans niet aansprakelijk en er bestaat nagenoeg geen consumentenbescherming op dit terrein.

4.5.3 LEKKEN UIT DATABASES

Overal waar grootschalig data worden opgeslagen ontstaan risico's op het weglekken van die data naar derden, hetzij door onzorgvuldigheid, hetzij door inbraken. Recente voorbeelden omvatten onder meer het lekken van miljoenen creditcardgegevens, van persoonlijke gegevens van burgers uit overheidsbestanden en van gevoelige informatie zoals strafrechtelijke dossiers.[11] In de VS hebben allerlei deelstaten sinds enkele jaren een meldingsplicht. In de afgelopen jaren worden jaarlijks meer dan vijfhonderd datalekken gemeld.[12] De omvang van de lekken is overigens zeer ongelijk verdeeld. Drie procent van de lekken beslaat 88 procent van de gelekte informatie (Mullins 2009). Daarnaast wordt uit de meldingen duidelijk dat er vaak data worden verloren waarvan het slachtoffer niet eens wist dat deze werden opgeslagen en waarvan het onzeker is of deze opgeslagen hadden mogen worden (Verizon Business 2008).

Bijna altijd geldt dat de beheerder van de data niet degene is die de schade draagt van deze lekken. Het is niet zijn informatie die weglekt, maar informatie over anderen, vaak over consumenten. In bijzondere gevallen hebben de getroffenen mogelijkheden om de schade juridisch te verhalen. Bij een computerinbraak bij de Amerikaanse winkelketen TJX werden de gegevens van 94 miljoen creditcards buitgemaakt (Vijayan 2007). Daarop volgden allerlei rechtszaken. Het grootste gedeelte van de getroffen kaarten was van VISA. De schade komt dan terecht bij de banken die de betreffende VISA-kaarten hebben uitgegeven. Die moeten hun klanten schadeloos stellen en nieuwe kaarten uitgeven. De banken begonnen een rechtszaak tegen TJX en wisten uiteindelijk een schikking af te dwingen van 41 miljoen dollar schadevergoeding . De Openbaar Ministeries van 41 Amerikaanse staten spanden ook een rechtszaak aan, onder andere om hun kosten van onderzoek en opsporing te verhalen. Ook die zaak werd geschikt, uiteindelijk voor ongeveer 10 miljoen dollar. Al zijn er in het geval van het lekken van financiële gegevens mogelijkheden tot verhaal, deze zijn beperkt. De dragers van de schade weten nooit de totale kosten te verhalen op degene die het datalek heeft laten gebeuren (Sullivan 2010; MacCarthy 2010).

In de meeste gevallen van datalekken zijn er niet of nauwelijks mogelijkheden tot verhaal. Wel draagt de organisatie met het lek soms gerelateerde kosten. In een recente enquête onder Amerikaanse organisaties die verplicht hun datalek moesten melden, werd de gemiddelde schade geschat op 6,7 miljoen dollar (Ponemon Institute 2009). Het betrof zowel publieke als private organisaties, al is deze

schatting een gemiddelde en hebben publieke organisaties doorgaans niet te maken met het verlies van klanten, hetgeen de grootste kostenpost is, volgens de studie. De overige kostenposten betreffen vooral de kosten van notificatie en van maatregelen om de impact te beperken, zoals publicrelationscampagnes. Andere onderzoeken suggereren dat lekken bij beursgenoteerde bedrijven de aandelenkoers significant kunnen beïnvloeden (Campbell et al. 2003). Een studie vond een effect hiervan op de aandelenkoersen van 225 bedrijven die een datalek hadden ondergaan. Dat effect kwam neer op een gemiddeld verlies van 2,1 procent van de handelswaarde, oftewel 1,65 miljard dollar (Cavusoglu et al. 2004). Het is echter niet bekend of dit effect vluchtig is of ook op de langere termijn standhoudt.

Organisaties die data lekken dragen dus niet of slechts gedeeltelijk de gevolgen van dat lek. Die situatie beloont onderinvestering in veiligheid (Kunreuther & Heal 2003). Systemen voor patiëntendata worden gekocht door ziekenhuisdirecties, die ook de noodzaak voelen van kostenbeheersing, werkbaarheid voor personeel, en de eisen die verzekeraars stellen om een snelle afhandeling van vergoedingen mogelijk te maken. Dat creëert prikkels die in een andere richting werken dan het streven naar veiligheid. De afwezigheid van een meldingsplicht versterkt dit patroon. Organisaties hebben in beginsel prikkels om datalekken te verzwijgen. De honderden meldingen die in de VS worden gedaan sinds de ingevoerde verplichting, tonen aan hoe sterk de prikkel is tot het achterhouden van informatie. Voor de wetgeving was een dergelijk bericht een zeldzaamheid.

Dit illustreert de informatieasymmetrie tussen de organisatie die de data beheert en externe organisaties, zoals toezichthouders, mensen wier gegevens zijn opgeslagen, organisaties die schade ondervinden van lekken en anderen. De externe actoren kunnen de informatie van de beherende organisatie nauwelijks beoordelen. Dat betreft ook claims ten aanzien van de veiligheid van de opgeslagen data. In bepaalde omstandigheden komt er nog informatie vrij door audits en certificeringstrajecten. Maar die hebben vaak een ritualistisch karakter en onderhouden een losse relatie met de daadwerkelijke veiligheidspraktijken.

Deze verdeling van kosten en baten genereert externaliteiten die in hun volle omvang nog zichtbaar moeten worden. De meldingsplicht in de VS heeft ons inzicht gegeven in het routinematige karakter van datalekken.[13] Er is geen enkele reden om aan te nemen dat het in andere landen beter gesteld is. Aan het begin van het essay werd als uitgangspunt geformuleerd dat elke vorm van informatietechnologie intrinsiek onveilig is en in beginsel zal falen. Als falen werkelijk onacceptabel is, dan dienen de data niet opgeslagen te worden. Dat is de conclusie die sommige kleine online winkels hebben getrokken, nadat ze gezien hebben hoe TJX tientallen miljoenen aan schadeclaims te verwerken kreeg. Omdat kleine spelers onvoldoende in staat zijn om de data goed te beveiligen, is het niet opslaan van de data de enige manier om een dergelijke aansprakelijkheid te ontlopen na een lek.

Dit is een gezonde ontwikkeling, omdat het de gevolgen van lekken deels internaliseert bij de actor die ervoor kiest om de data op te slaan. Met het opslaan van data accepteren we de facto ook het optreden van lekken. De vraag is of degene die ervoor kiest om de data op te slaan, ook de gevolgen van het lekken draagt. Het antwoord daarop luidt doorgaans: nee. Een enkele keer, zoals in het geval van TJX, draagt men gedeeltelijk die gevolgen. Actoren die onder de meldingsplicht vallen dragen die gevolgen doorgaans niet en ondergaan alleen tamelijk bescheiden repercussies, zoals reputatieschade en de kosten van het voldoen aan regulering rond de meldingsplicht. Verreweg de meeste actoren dragen echter geen gevolgen van het lekken van hun informatie. Dat geldt zeker in Nederland, waar tot voor kort geen meldingsplicht gold en waar ook de gevallen die toch al aan het licht kwamen niet tot zichtbare repercussies hebben geleid. Daarom zal deze vorm van falen vaker voorkomen dan maatschappelijk wenselijk is. Ook op dit terrein zien we dus de noodzaak tot het terugdringen van zulke afwentelingsmechanismen.

4.6 ROL VAN DE OVERHEID

Tot nu toe hebben we niet expliciet gesproken over overheden als gebruikers van informatietechnologie. Daar was ook geen reden toe. In veel gevallen nemen overheden geen bijzondere positie in. Natuurlijk zijn overheden niet hetzelfde als bedrijven, maar ook zij opereren onder gemengde prikkels. Sommige prikkels die bedrijven voelen, ontbreken – zoals de dreiging dat klanten weglopen na reputatieschade. Daar staat tegenover dat overheden de opslag van data soms met meer waarborgen omgeven, juist omdat het bijzondere gegevens betreffen over de eigen burger. Ook voor overheden geldt echter dat de kosten van onveiligheid vaak bij anderen terechtkomen. Het hoeft dan ook niet te verbazen dat botnets ook machines bevatten die onderdeel uitmaken van overheidsorganisaties en dat data blijven lekken zonder noemenswaardige consequenties.[14] Eventuele antwoorden op deze problemen zullen ook voor overheidsorganisaties moeten gelden.

Welke rol heeft de overheid ten aanzien van het systeem als geheel? In het licht van het voorafgaande betoog, kunnen we twee rollen onderscheiden:

1 Beschermen van decentrale afwegingen rond veiligheid waar actoren zelf de gevolgen dragen van die afwegingen.
2 Ondervangen van afwentelingsmechanismen waar actoren de kosten van falende veiligheid niet zelf dragen.

De eerste rol impliceert vooral terughoudendheid en scepsis. Er zijn allerlei claims dat veiligheid tekortschiet – niet in de laatste plaats van veiligheidsexperts. Deze claims moeten met een gezonde dosis wantrouwen tegemoet getreden worden. Een veiligheidsincident is geen bewijs voor een te laag niveau van veiligheid. Op te veel terreinen wordt veiligheid gegijzeld door *worst case*-denken en risicomijdend gedrag (Furedi 2010). De risicotolerantie die we de facto hebben opgebouwd rondom

internetdiensten is economisch waardevol en moet beschermd worden. Ze is intrinsiek verbonden met de vernieuwingen die deze technologie heeft mogelijk gemaakt. Wel is het binnen deze rol gepast dat de overheid zich inzet voor de toegang van marktpartijen tot informatie waarmee ze hun decentrale veiligheidskeuzes kunnen maken en tot middelen om die keuzes te effectueren. Dit geldt met name voor partijen die zelf weinig expertise kunnen mobiliseren, zoals eindgebruikers en het midden- en kleinbedrijf.

De tweede rol draait om het internaliseren van veiligheidsexternaliteiten. Wanneer er een externaliteit optreedt, is er een aanleiding om de decentrale afwegingen bij te sturen. Dat er een aanleiding is, wil overigens nog niet zeggen dat het ook mogelijk is om externaliteiten efficiënt en zonder al te veel neveneffecten terug te dringen. De instrumenten die hiervoor kunnen worden ingezet zijn, in het geval van informatietechnologie, omstreden. De discussie hierover wordt pas enkele jaren serieus gevoerd. Wel kunnen we enkele contouren schetsen. Het laatste deel van dit essay bespreekt vier dominante opties:

1 ex ante veiligheidsregulering;
2 ex post aansprakelijkheid;
3 verplichte melding van incidenten en ondersteuning van gedupeerden;
4 aansprakelijkheid van intermediaire actoren.[15]

4.6.1 EX ANTE VEILIGHEIDSREGULERING

Het vooraf formuleren van veiligheidseisen waaraan actoren moeten voldoen is een instrument dat op allerlei maatschappelijke terreinen wordt toegepast. Rondom informatietechnologie is dit een minder dominant instrument. We treffen het vooral aan rondom financiële instellingen, die op allerlei terreinen onder verregaande vormen van regulering opereren. Het doel van ex ante veiligheidsnormen is het vooraf garanderen van bepaalde veiligheidsniveaus.

De nadelen zijn ook bekend. Normen richten de aandacht op *compliance*, niet op veiligheid (Forrester Research 2010). Normen maken passief. Normen verstarren een organisatie. Normen belemmeren en verstoren decentrale afwegingen. En normen raken achterhaald, zeker op een terrein dat zo dynamisch is als informatietechnologie. Het is veelzeggend dat de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) zich enige tijd heeft ingezet voor het formuleren van basisnormen voor veiligheid waaraan ISP's zouden moeten voldoen. Dit idee heeft men laten varen, toen bleek dat niet kon worden geïdentificeerd wat dan die basisnormen dienden te zijn.

Ook de normering en certificering op het gebied van software heeft weinig overtuigende resultaten laten zien. In de Angelsaksische wereld wordt veel gebruikgemaakt van de veiligheidsstandaard Common Criteria.[16] Naar verluidt worden

nagenoeg alle aanvragen voor een Common Criteria certificering gehonoreerd. Dat komt door het mechanisme van *adverse selection*. Producenten dragen zelf de kosten voor certificering en kiezen dus de commerciële verstrekker die de minste hordes opwerpt (Anderson & Moore 2006). Overigens werd een vergelijkbaar mechanisme al zichtbaar tijdens de kredietcrisis, toen bleek dat *credit rating agencies* de *subprime* hypotheken op grote schaal van *triple-A* beoordelingen voorzagen. Bijna alle bedrijfsmatig gebruikte software is gecertificeerd, maar wordt even zeer geplaagd door kwetsbaarheden. Daarmee heeft dit instrument dus geen wezenlijk effect op veiligheid.

Een ander adverse selection mechanisme is dat het juist voor dubieuze spelers waardevol is om zich te laten certificeren. Een studie naar veiligheidscertificaten voor websites toonde aan dat de gecertificeerde sites gemiddeld juist onveiliger waren dan de sites zonder certificaat (Edelman 2006). Zulke instrumenten laten dan ook vooral zien dat de producent bereid is om de hordes te nemen op de weg naar certificering, die niet in de laatste plaats bestaat uit het soms hoge prijskaartje van een dergelijk traject. Ze werpen eerder toetredingsbarrières op dan dat ze garanties bieden ten aanzien van kwaliteit.

Zelfs relatief onomstreden normen zijn maar losjes met veiligheid verbonden. Zo wordt over het algemeen het gebruik van encryptie aanbevolen bij het opslaan van privacygevoelige data, zoals patiëntendossiers. Een recente studie heeft een robuuste analyse gemaakt van de effecten van het gebruik van encryptie in de Amerikaanse gezondheidszorg – een praktijk die sterk door de overheid wordt gestimuleerd en in bepaalde staten zelfs per wet wordt afgedwongen. De uitkomsten zijn verrassend. Instellingen die encryptie invoerden bleken daarna een verhoogde kans te hebben op datalekken (Miller & Tucker 2010). De verklaringen hiervoor zijn vooralsnog speculatief. Het kan zijn dat de invoering leidt tot het ruimhartiger toestaan van toegang tot de data, juist omdat deze versleuteld zijn. Wat het wel duidelijk maakt, is dat het vaststellen van normen en best practices door de overheid een hachelijke zaak is.

Normen zullen ongetwijfeld een rol gaan spelen, maar de vraag is of de overheid de aangewezen partij is voor de vaststelling van die normen. De komende jaren zullen waarschijnlijk gaan leiden tot meer privaat ontwikkelde normen, vooral uit de verzekeringssector. Naarmate meer organisaties verzekeringen afsluiten tegen de schade van veiligheidsincidenten die zij zelf veroorzaken, zullen verzekeraars veiligheidsnormen en richtlijnen gaan hanteren om de premiehoogte te bepalen. Actuariële data, die nu nog schaars zijn, zullen in omvang en kwaliteit gaan toenemen, omdat er meer verzekerden en schademeldingen zullen zijn. Daardoor krijgen verzekeraars de mogelijkheid om verbanden te leggen tussen normen en schade. Zonder die basis kan dat niet. Er is geen reden om aan te nemen dat de overheid dit wel zou kunnen.

Dit alles laat onverlet dat normen kunnen helpen bij de inrichting van informatiebeveiliging. Zo hanteerde het College bescherming persoonsgegevens bepaalde generieke principes waaraan volgens het college voldaan moet zijn bij de bescherming van patiëntgegevens. Die principes ondersteunen de oordeelsvorming. Normen kunnen het vertrekpunt zijn van die oordeelsvorming, maar niet het eindpunt. Te vaak is gebleken dat het voldoen aan normen een losse koppeling onderhoudt met daadwerkelijke veiligheid.

4.6.2 EX POST AANSPRAKELIJKHEID

Strikte aansprakelijkheid lijkt op het gebied van informatietechnologie vooralsnog weinig zinvol. De incidenten vinden hun oorsprong vaak in crimineel gedrag, niet in nalatigheid. In dat opzicht is het een volstrekt andere situatie dan een autofabrikant die een onveilig product aflevert. Daarnaast zou strikte aansprakelijkheid waarschijnlijk een fnuikend effect hebben op innovatie.

Wel zouden lichtere vormen van aansprakelijkheid kunnen worden overwogen – die wellicht juridisch gezien niet onder die noemer vallen. Men zou het mogelijk kunnen maken om bij bepaalde incidenten, zoals datalekken, een vergoeding te krijgen. De vergoedingen zouden bijvoorbeeld gestandaardiseerd kunnen worden, zoals het systeem voor elektriciteitsgebruikers die met stroomuitval te maken krijgen.[17] Zo opperden Britse onderzoekers in een rapport voor het Europese agentschap ENISA om ISP's een vast bedrag te laten betalen voor elke melding van *abuse* in hun netwerk die zij niet binnen een bepaalde termijn hadden behandeld (Anderson et al. 2008).

Het gaat dan minder om de werkelijke schade vast te stellen en te compenseren. Dat is kostbaar en ingewikkeld en introduceert onzekerheid in de markt die belemmerend kan werken. Het doel is met name om ervoor te zorgen dat actoren een prikkel hebben om mogelijk falen mee te wegen in hun afwegingen en dat ze gedwongen worden om de gevolgen te dragen als ze verkeerde inschattingen maken. Elk arrangement zal zijn nadelen kennen, maar de status-quo is vaak nog minder aantrekkelijk, namelijk dat falen geen gevolgen heeft voor de betreffende organisatie, afgezien van wellicht wat ongewenste media-aandacht.

4.6.3 VERPLICHTE MELDING VAN INCIDENTEN

In het verlengde van de vorige optie liggen voorstellen om de melding verplicht te stellen van bepaalde categorieën van veiligheidsincidenten. Voor datalekken is deze wetgeving in de VS ingevoerd. In Europa wordt op dit moment een merkwaardig versmalde variant hiervan ingevoerd. In de recent herziene ePrivacyrichtlijn is een meldingsplicht opgenomen voor aanbieders van elektronische communicatie.[18] In Nederland wordt een wijziging in de Telecomwet voorbereid

die de herziene richtlijn moet implementeren. Ook het College bescherming persoonsgegevens heeft het wetsvoorstel en de onderliggende richtlijn bekritiseerd, omdat de meldingsplicht te smal is opgezet om het doel te bereiken, het beschermen van consumenten. Dat vereist een brede meldingsplicht, betoogt men.[19] Die kritiek wordt breed gedeeld. Als een meldingsplicht al helpt, dan zeker niet in de smalle variant.

Of de bredere meldingsplicht in de VS werkelijk tot een verbetering leidt, is nog niet duidelijk. Maar de informatie die vrijkomt door de meldingen is intrinsiek waardevol. Ook hier dient verantwoording georganiseerd te worden en dat vereist het verkleinen van de informatieasymmetrie tussen databankbeheerders en externe partijen. Dat begint met het bekendmaken van incidenten die anders verborgen waren gebleven. Het is niet alleen zinvol om (meer) te weten over financiële dienstverleners of beheerders van privacygevoelige informatie, maar ook van beheerders van kritieke infrastructuren als elektriciteit en luchtverkeer die in belangrijke mate leunen op informatietechnologie bij de aansturing van hun technische systemen.

Bij recentere wetsvoorstellen in de VS wordt de informatieplicht soms gekoppeld aan de plicht om gedupeerden te ondersteunen bij het voorkomen of afhandelen van schade. Dit kan bijvoorbeeld bestaan uit het gratis aanbieden van diensten die identiteitsdiefstal bestrijden en besmeurde kredietregistraties repareren. Er is al een kleine industrietak ontstaan van bedrijven die zulke diensten aanbieden. De organisaties die een datalek hebben gemeld, huren soms dergelijke bedrijven in om hun diensten te kunnen aanbieden aan de gedupeerden.

4.6.4 AANSPRAKELIJKHEID VAN INTERMEDIAIRE ACTOREN

Dit is het terrein waar op korte termijn de meeste dynamiek te verwachten is. Al enige tijd staat het thema in de belangstelling, ook op aanpalende terreinen zoals het bestrijden van inbreuken op auteursrechten. Twee intermediaire partijen staan centraal in de discussie over veiligheid: ISP's en financiële dienstverleners. Over die laatste partij hebben we eerder al gesproken. Als we de banken op hun woord geloven, hebben ze de aansprakelijkheid voor schade van hun klanten al geaccepteerd. Het wordt tijd om dat juridisch te gaan garanderen. In de VS werkt dit regime al jaren uitstekend, al kent het ook daar gaten die gedicht moeten worden, met name voor zakelijke klanten en voor indirecte schade, zoals identiteitsdiefstal. De banken willen nog wel eens suggereren dat het eenzijdig bij hen neerleggen van aansprakelijkheid zal leiden tot onverantwoordelijk gedrag bij hun klanten. Het moral hazard-mechanisme. Er is echter nauwelijks empirische steun voor de claim dat mensen laks worden met hun betaaldiensten als ze niet aansprakelijk zijn. Het blijft een onprettig idee dat iemand zich toegang tot je geld verschaft. Net zoals diefstal van eigendommen op vakantie ook vervelend is,

al heb je een reisverzekering. Als moral hazard grootschalig laksheid zou uitlokken, dan zouden reisverzekeringen al lang onderuit zijn gegaan. En zoals al eerder is betoogd: ook het hanteren van een eigen risico heeft hier nuttige diensten bewezen.

De ISP's zijn de tweede partij. Daar zijn interessante ontwikkelingen te signaleren. Ten aanzien van botnets hebben Nederlandse ISP's recent een convenant getekend om geïnfecteerde klanten te gaan benaderen en, waar nodig, de betreffende verbindingen in quarantaine te gaan plaatsen. Ook in enkele andere landen zien we zulke ontwikkelingen, met name Duitsland en Australië. Niemand beweert dat ISP's de oorzaak zijn van botnets. Het is echter duidelijk dat de eindgebruikers dit probleem zelf niet aankunnen en het vaak zelfs maatschappelijk inefficiënt is als gebruikers werkelijk de veiligheidsadviezen opvolgen die ze krijgen aangereikt. De ISP's verkeren in een cruciale positie om geïnfecteerde machines te identificeren, vaak beter dan de gebruiker zelf. Daarnaast vormen ISP's een natuurlijk controlepunt, zo blijkt uit recent empirisch onderzoek (Van Eeten et al. 2010). De 200 ISP's die de bulk van het marktaandeel hebben in de landen van de organisatie voor economische samenwerking en ontwikkeling (OESO) (30 leden en tien landen die bezig zijn om toe te treden of samen te werken met de OESO) hebben meer dan 60 procent van alle geïnfecteerde machines wereldwijd in hun netwerken. Het patroon is zelfs zo geconcentreerd dat slechts 50 ISP's meer dan de helft van alle besmette machines wereldwijd omvatten (zie figuur 4.4). Ook blijkt dat er grote verschillen bestaan tussen providers. Bij ISP's die onder vergelijkbare condities werken, zien we soms een factor honderd verschil in het aantal geïnfecteerde machines in hun netwerken. Dat betekent dat ze handelingsruimte hebben in de mate waarin ze deze problemen aanpakken.

De overheid zou ISP's kunnen stimuleren hun rol actiever in te vullen. Dat kan bijvoorbeeld door indicatoren te publiceren die de markt signalen geven over de veiligheidsprestaties van ISP's aan consumenten in de zakelijke en thuismarkt. Er zijn allerlei data voorhanden om de relatieve infectiegraden van de netwerken te bepalen. Het publiekelijk maken van de informatie zou waarschijnlijk tot extra inspanningen leiden bij de slechtst presterende providers. In Australië hebben providers een gedragscode opgesteld die lijkt op het Nederlandse convenant. Het verschil is dat er ook een overheidsorganisatie is die actief informatie verzamelt over geïnfecteerde machines bij Australische providers en vervolgens die providers daarvan op de hoogte stelt. Conform de gedragscode moeten deze dan binnen een bepaalde termijn het probleem verhelpen.

Een ander initiatief is recent gestart in Duitsland. Daar financiert de overheid een callcenter waar gebruikers met een besmette machine ondersteuning kunnen krijgen. De providers verwijzen deze mensen door. Dat haalt de grootste kostenpost – en daarmee *disincentive* – weg bij de providers, namelijk contact en ondersteu-

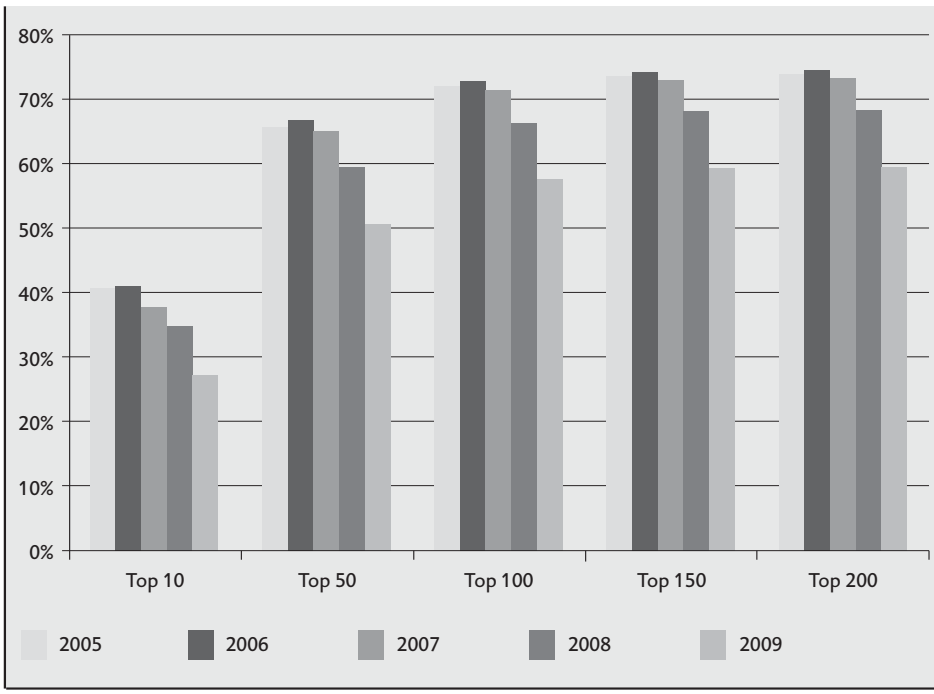
ning van klanten (Van Eeten & Bauer 2008). Het wordt daardoor veel aantrekkelijker om klanten met besmette machines te identificeren en informeren.

Deze initiatieven berusten geen van alle op formele regulering. Mochten de resultaten achterblijven, dan zal de roep om een dwingender regime ongetwijfeld luider klinken. Vooralsnog is er echter geen sprake van inertie. De ISP's vullen zelf hun rol als intermediair in, in het licht van de externaliteiten die door hun klanten worden gegenereerd.

4.7 TOT SLOT

Tot zover de bespreking van de vier opties waarmee de overheid kan proberen om veiligheidsexternaliteiten te internaliseren. Het is uiteraard geen uitputtend overzicht. Ook de vormgeving van elk van deze opties vereist nog veel werk voordat er sprake kan zijn van daadwerkelijke beleidsvoorstellen. Op dit moment is het wellicht belangrijker om helderheid te scheppen over de rol van de overheid. Op die manier kan voorkomen worden dat de onheilsprofeten op het gebied van de risico's van informatietechnologie de politiek tot interventies gaan uitlokken die meer kwaad dan goed doen.

Figuur 4.4 Aandeel van besmette machines wereldwijd in de netwerken van ISP's



Bron: Van Eeten et al. (2010a)

NOTEN

1 Toevalligerwijs werd tijdens de afronding van dit essay de eerste fraudeur gearresteerd. Een dertigjarige Leidse man had een niet op naam gestelde chipkaart verschillende malen opnieuw opgeladen, zonder te betalen. De totale schade werd niet gemeld, maar aangezien het eigen gebruik betrof, moet deze zeer bescheiden zijn. Zie: Openbaar Ministerie, *"Aanhouding voor fraude met OV-chipkaart"*, 17 juni 2010. Online te raadplegen via: http://www.om.nl/actueel/nieuws-_en/@153712/aanhouding_voor/.

2 Zo schreef GOVCERT onlangs: "De risico's groeien.... Cybercrime neemt hand over hand toe." Zie: GOVCERT (2010). *Jaaroverzicht 2009*. GOVCERT. Online te raadplegen via http://www.govcert.nl/render.html?it=177.

3 Lezing van Tracey Vispoli van Chubb Insurance – een van de grootste eigendoms- en schadeverzekeraars ter wereld – tijdens de *Workshop on the Economics of Information Security (WEIS 2010)*, Harvard University, 7 juni 2010.

4 Cormak Herley maakt aannemelijk dat veiligheidsadviezen aan eindgebruikers de samenleving vaak meer schade berokkenen dan goed doen. Een voorbeeld: "Suppose some security advice reduces the risk of becoming a phishing victim by 50 percent. If phishing victimizes 0.37 percent of users per year and each victim wastes 10 hours sorting it out, to be beneficial the daily effort of following the advice should be less than 0:0037 x 0:5 x 10/365 hours or 0:18 seconds per day. Clearly, a user who makes the effort to read URLs to identify phishing sites will spend more time than this. Thus the advice is, in expectation, doing more harm than good."

5 Een van de grootste botnets is Conficker, die wordt geschat op rond de 7 miljoen besmette machines. Zie: http://www.shadowserver.org/wiki/pmwiki.php/Stats/Conficker. Zie voor een studie naar de bredere populatie van botnets: http://www.usenix.org/event/leet08/tech/full_papers/zhuang/zhuang.pdf.

6 Zie ook de recente arrestatie door de FBI van drie mannen die meer dan 100 miljoen dollar hadden verdiend door de verspreiding van valse veiligheidssoftware. Zie: http://chicago.fbi.gov/dojpressrel/pressrel10/cg052710.htm

7 *Schade door skimmen 31 miljoen*, *NRC Handelsblad*, 18 mei 2009. Online te raadplegen via: http://www.nrc.nl/economie/article2244994.ece/Schade_door_skimmen_31_miljoen.

8 Which?, *Fraud victims struggle to get money back*, 2009. Online te raadplegen via: http://www.which.co.uk/news/2009/06/fraud-victims-struggle-to-get-money-back-179150.jsp.

9 Deze regeling staat bekend als *Regulation E* van de *Electronic Fund Transfer Act*. Zie: http://en.wikipedia.org/wiki/Regulation_E.

10 Zie bijvoorbeeld de vele incidenten die journalist Brian Krebs verzamelt: http://krebsonsecurity.com/category/smallbizvictims/.

11 Zie bijvoorbeeld het *Zwartboek Datalekken* dat bijgehouden wordt door Bits of Freedom: https://www.bof.nl/category/zwartboek-datalekken/.

12 Zie: http://datalossdb.org/statistics.

13 Voor een paar aardige Nederlandse voorbeelden, zie het *Zwartboek Datalekken* van Bits of Freedom: https://www.bof.nl/ons-werk/prive-gegevens/zwartboekdatalekken/.

14 Ook hier biedt het *Zwartboek Datalekken* vele illustraties.

15 Deze vier opties zijn mede gebaseerd op een suggestie van Tyler Moore.

16 Zie: http://en.wikipedia.org/wiki/Common_Criteria.

17 Zie de voorlichting over dit arrangement op: http://www.rijksoverheid.nl/ documenten-en-publicaties/vragen-en-antwoorden/krijg-ik-een-vergoeding-bij-een-stroomstoring.html.

18 Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming. Online te raadplegen via: http:// eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:NL: HTML.

19 College bescherming persoonsgegevens (2010) *Wetgevingsadvies CBP inzake wijziging Telecommunicatiewet*, online te raadplegen via: http://www.cbpweb.nl/Pages/med_20100607_telecommunicatiewet.aspx.

LITERATUUR

Aaron, G. & R. Rasmussen (2010) *Global phishing survey: trends and domain name use in 2H2009*, http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf.

Amoroso, E. (2009) *Statement of Edward Amoroso, senior vice president & chief security officer AT&T Inc.* Hearing On Improving Cybersecurity, March 19, 2009. United States Senate, Committee On Commerce, Science And Transportation, http://commerce.senate.gov/public/?a=Files.Serve&File_id=e8d018c6-bf5f-4ea6-9ecc-a990c4b954c4.

Anderson, R. (2007) *Closing the phishing hole – fraud, risk and nonbanks*, http://www.cl.cam.ac.uk/~rja14/Papers/nonbanks.pdf.

Anderson, R. & N. Bohm (2008) *Foundation for Information Policy Research (FIPR) submission to The hunt review of the financial ombudsman service*, http://www.fipr.org/080116huntreview.pdf.

Anderson, R., R. Böhme, R. Clayton & T. Moore (2008) *Security economics and the internal market*, European Network and Information Security Agency (ENISA), http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

Anderson, R. & T. Moore (2006) 'The economics of information security', *Science* 314: 610-613.

APACS (2009). *Fraud – The facts 2009. The definitive overview of payment industry fraud and measures to prevent it*, http://www.theukcardsassociation.org.uk/files/fraud_the_facts_2009.pdf.

Bain, B. (2010) 'Australia taps ISPs to fight 'zombies'', *Federal Computer Week*, http://fcw.com/articles/2010/06/29/web-aussie-isp-code.aspx.

Bakker, J. (2009) 'Botnetbestrijding isp's blijft vrijblijvend', *WebWereld*, http://webwereld.nl/nieuws/63086/botnetbestrijding-isp-s-blijft-vrijblijvend.html

Bauer, J.M., M.J.G. van Eeten & T. Chattopadhyay (2008) *ITU study on the financial aspects of network security: malware and spam*, ITU (International Telecommunication Union), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

Campbell, K., L.A. Gordon, M. P. Loeb & L. Zhou (2003) 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer Security* 11, 3: 431-448, http://brief.weburb.dk/archive/00000130/01/2003-costs-security-on-stock-value-9972866.pdf.

Cavusoglu, H. (2004) 'Economics of IT security management', blz. 71-83 in L. J. Camp and S. Lewis Economics of Information Security, New York: Springer 12: 71-83.

Cavusoglu, H., B. Mishra & S. Raghunathan (2004) 'The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers', *International Journal of Electronic Commerce* 9, 1: 69, http://www.gVSu.edu/business/ijec/v9n1/p069.html.

Clayton, R. (2010) *Might governments clean-up malware?* Ninth Workshop on the Economics of Information Security (WEIS 2010), Cambridge: Harvard University, http://weis2010.econinfosec.org/papers/session4/weis2010_clayton.pdf.

CSI (2008) *CSI survey 2008: the 13th annual computer crime and security survey*, Computer Security Institute, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

Davis, J. (2007) 'Hackers take down the most wired country in europe', *Wired Magazine 15,* http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

Denning, D. (2000) 'Reflections on cyberweapons controls', *Computer Security Journal* 16, 4: 43-53.

Edelman, B. (2006) *Adverse selection in online 'trust' certifications*, Fifth workshop on the economics of information security 2006, http://weis2006.econinfosec.org/docs/10.pdf.

Forrester Research (2010) *The value of corporate secrets*, http://www.rsa.com/products/DLP/ar/10844_5415_The_Value_of_Corporate_Secrets.pdf.

Furedi, F. (2010) *This shutdown is about more than volcanic ash*, Spiked, http://www.frankfuredi.com/index.php/site/article/386/.

GOVCERT (2010) *Jaaroverzicht 2009*, http://www.govcert.nl/render. html?it=177.

Grossman, W. M. (2007) 'Does antivirus have a future? ', *The Guardian,* 20 September 2007, http://www.guardian.co.uk/technology/2007/sep/20/guardianweekly technologysection.spam.

Herley, C. (2009) *So long, and no thanks for the externalities: the rational rejection of security advice by users*, http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf.

Herley, C. (2010) *The plight of the targeted attacker in a world of scale,* Ninth Workshop on the Economics of Information Security (WEIS 2010), Cambridge: Harvard University, http://weis2010.econinfosec.org/papers/session5/weis2010_herley.pdf.

Herley, C. & D. Florencio (2008) *A profitless endeavor: phishing as tragedy of the commons*, http://research.microsoft.com/apps/pubs/?id=74159.

House of Lords (2007) *Science and technology committee, 5th Report of Session 2006–07*, Personal Internet Security, Volume II: Evidence, Authority of the House of Lords, http://www.publications.parliament.uk/pa/ld/ldsctech.htm.

ICANN (2007) *Factsheet: DNS attack,* ICANN Blog, http://blog.icann.org/2007/03/factsheet-dns-attack/.

Internet Crime Complaint Center (2010) *2009 Internet crime report*, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

Krebs, B. (2009) *Avoid Windows malware: bank on a live CD*, Washington Post Security Fix weblog, http://voices.washingtonpost.com/securityfix/2009/10/avoid_windows_malware_bank_on.html.

Kunreuther, H. & G. Heal (2003) 'Interdependent security', *Journal of Risk and Uncertainty* 26, 2: 231.

MacCarthy, M. (2010) *Information security policy in the U.S. retail payments industry,* Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard

University, http://weis2010.econinfosec.org/papers/panel/weis2010_maccarthy.pdf.

Markoff, J. (2008) 'Cyber attack preceded invasion: Georgia's web infrastructure hit, but was it Russia? ', Chicago Tribune website, http://archives.chicagotribune.com/2008/aug/13/business/chi-cyber-war_13aug13.

Miller, A. R. & C. E. Tucker (2010) *Encryption and data loss,* Ninth Workshop on the Economics of Information Security (WEIS 2010), Cambridge: Hardvard University, http://weis2010.econinfosec.org/papers/session1/weis2010_tucker.pdf.

Moore, T., R. Clayton & R. Anderson (2009) 'The economics of online crime', *Journal of Economic Perspectives* 23, 3: 3-20.

Mullins, R. (2009) *Data breach attack trends analyzed*, https://365.rsaconference.com/blogs/articles/2009/04/23/data-breach-attack-trends-analyzed.

OECD (2009) *Computer viruses and other malicious software,* Parijs: Organisation for Economic Co-operation and Development.

Ponemon Institute (2009) *Fourth annual US cost of data breach study. Benchmark study of companies*, http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf.

Protalinski, E. (2009) 'Germany pays to clean malware from Windows PCs', *Ars Technica*, http://arstechnica.com/microsoft/news/2009/12/microsoft-welcomes-germany-ridding-citizen-pcs-of-malware.ars.

Schneier, B. (2007) *Information security and externalities,* NSF/OECD Workshop Social & Economic Factors Shaping The Future Of The Internet: Washington DC, http:// www.oecd.org/dataoecd/60/8/37985707.pdf.

Sullivan, R. J. (2010) *The changing nature of U.S. card payment fraud: issues for industry and public policy*, Ninth Workshop on the Economics of Information Security (WEIS 2010), Harvard University, http://weis2010.econinfosec.org/papers/panel/weis2010_sullivan.pdf.

Symantec (2010) *Norton cybercrime report: the human impact,* http://www.symantec.com/about/news/release/article.jsp?prid=20100908_01.

Symantec (2008) *Internet security threat report, Volume XIII*, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_ internet_security_threat_report_xiii_04-2008.en-us.pdf.

Van Eeten, M., J. Bauer, H. Asghari & S. Tabatabaie (2010) *The role of internet service providers in botnet mitigation: an empirical analysis based on spam data,* Ninth Workshop on the Economics of Information Security (WEIS 2010), Cambridge: Harvard University, http://weis2010.econinfosec.org/papers/session4/weis2010_vaneeten.pdf.

Van Eeten, M., J. Bauer, H. Asghari & S. Tabatabaie (2010a) *The role of internet service providers in botnet mitigation: an empirical analysis based on spam data*, OECD STI Working Paper 2010/5, Parijs: OESO, http://www.oecd.org/officialdocuments/

publicdisplaydocumentpdf/?cote=DSTI/DOC(2010)5&docLanguage=En

Van Eeten, M. & J.M. Bauer (2008) *Economics of malware: security decisions, incentives and externalities, OECD STI Working Paper 2008/1*, OECD, http://www.oecd.org/dataoecd/53/17/40722462.pdf.

Van Eeten, M., H. Asgari, J.M. Bauer & S. Tabatabaie (2011) *Internet service providers and botnet mitigation. A fact-finding study on the Dutch market. Report prepared for the Netherlands Ministry of Economic Affairs, Agriculture and Innovation.* Den Haag: Ministerie van Economische Zaken, Landbouw en Innovatie, http://rijksoverheid.nl/ministeries/eleni/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.nl

Verizon Business (2008) *2008 Data breach investigations report*, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

Vijayan, J. (2009) 'TJX reaches $9.75 million breach settlement with 41 states', *Computerworld*, http://www.computerworld.com/s/article/9134765/TJX_reaches_9.75_million_breach_settlement_with_41_states.

Vijayan, J. (2007) 'Scope of TJX data breach doubles: 94M cards now said to be affected', *Computerworld*, http://www.computerworld.com/s/article/9043944/Scope_of_TJX_data_breach_doubles_94M_cards_now_said_to_be_affected.

Washkuch, F. (2007) 'TJX agrees to $41 million settlement with Visa', *Sc Magazine*, http://www.scmagazineus.com/tjx-agrees-to-41-million-settlement-with-visa/article/99437/.

Weaver, N. & V. Paxson (2004) *A worst-case worm,* Third workshop on the economics of information security: Minneapolis, MN, http://www.dtc.umn.edu/weis2004/weaver.pdf.

Zhuang, L., J. Dunagan, D.R. Simon, H.J. Wang, I. Osipkov, G. Hulten & J.D. Tygar (2008) *Characterizing botnets from email spam records*, LEET '08, first usenix workshop on large-scale exploits and emergent threats: San Francisco, http://www.usenix.org/event/LEET08/tech/full_papers/zhuang/zhuang.pdf.

Zittrain, J. (2008) *The future of the internet: and how to stop it,* Londen: Allen Lane.

5 HET RECHT OP VERGETELHEID. POLITIËLE EN JUSTITIËLE GEGEVENS IN EEN DIGITALE WERELD

Ybo Buruma

PROLOOG

In 1994 ontvangt meneer K., een Nederlandse ondernemer van Surinaamse afkomst, een dagvaarding wegens overtreding van de Opiumwet. Verzoeker gaat naar de politie, omdat hij er niets mee te maken heeft. Dat wordt zowel door de politie als later door de officier van justitie en de rechter geloofd. Het blijkt dat in twee van de inmiddels vijf tegen verzoeker opgemaakte processen-verbaal niet meneer K., maar meneer C. de verdachte was. C. had met hem op de lagere school gezeten. Op 11 juli 2002 maakt de politie Amsterdam weer procesverbaal op tegen C. waarbij deze opnieuw de personalia van meneer K. opgeeft. De volgende dag maakt de politie nogmaals een proces-verbaal dat niet meneer K. maar meneer C. de verdachte is, maar het verbaal van een dag eerder is dan al ingestuurd. Zo kan het gebeuren dat hij voor het eerst bij verstek wordt veroordeeld voor een feit dat door C. is begaan. Dat gebeurt vaker. In 2004 roept het Amsterdamse Hof hem op, in de onjuiste veronderstelling dat hij in detentie verkeert. Dat geeft meneer K. de gelegenheid zijn onschuld te bewijzen. C. was niet aanwezig; die was wel gedetineerd.

De gebeurtenissen worden steeds dramatischer. Meneer K. ondervindt regelmatig hinderlijke verkeerscontroles en wordt op zeker moment klemgereden door een arrestatieteam. En in oktober 2003 verricht de FIOD met 35 man huiszoeking bij hem in aanwezigheid van zijn 7- en 13-jarige kinderen. Hij zou als harddrugsgebruiker betrokken zijn bij het witwassen van drugsgeld en een waslijst aan veroordelingen op zijn naam hebben. Hij wordt voor deze zaak in eerste aanleg veroordeeld in 2006. Hij moet dreigen met een kort geding om zijn administratie van de FIOD terug te krijgen teneinde zijn onschuld te bewijzen, hetgeen dan in 2007 tot vrijspraak bij het Hof leidt. Naar aanleiding van een verzoek om in 2006 zijn bedrijf om te zetten in een holding en een bv meldt het ministerie van Justitie voornemens te zijn de verklaring van geen bezwaar te weigeren, omdat "de ernst en de aard van de strafbare feiten waarvoor betrokkene is veroordeeld dan wel vrijgesproken is van dien aard zijn dat gerede twijfel tegen de morele integriteit van betrokkene gerechtvaardigd was".

Met zijn bedrijf gaat het slechter. In Suriname waar hij een groothandel en een aantal apotheken heeft, krijgt men in 2004 lucht van de geruchten. Meneer K. vindt de contacten met de marechaussee op Schiphol ook steeds vervelender worden. Dat is het gevolg van het feit dat C. onder zijn naam als ongewenst vreemdeling staat

gesignaleerd. Meneer K. heeft weliswaar een geldig paspoort – anders dan een ongewenst vreemdeling – maar dat wordt niet geloofd. Hij wordt meermalen ook in het bijzijn van zakenpartners afgeblaft en diverse keren mist hij zijn vliegtuig. De zaak escaleert een keer en de marechaussee doet dan aangifte van belediging, waarvoor meneer K. bij de politierechter wordt vrijgesproken. Uiteindelijk gaat zijn bedrijf kapot, omdat niemand in Suriname nog zaken met hem wil doen. Als nogmaals een contact met de marechaussee escaleert, wendt hij zich tot de Nationale Ombudsman met de volgende woorden: "Als ik terugkijk op de gebeurtenissen van de afgelopen 13 jaar heb ik moeten concluderen dat het justitiële apparaat in Nederland niet zorgvuldig en naar willekeur met mijn belangen omspringt. Het is mij of mijn advocaat niet gelukt mijn justitiële documentatie te schonen dan wel dat ik geen hinder meer ondervind van justitie of politie omdat een derde misbruik maakt van mijn personalia. De overheidsinstanties die ik in de loop der jaren heb gesproken hieromtrent, of ongevraagd kennis mee heb moeten maken, geven allemaal aan dat het ongelofelijk is en voor mij bijzonder vervelend maar dat zij als betreffende instantie hierin niets kunnen betekenen en zij allen naar een ander doorverwijzen."

De Nationale Ombudsman onderzoekt de zaak en concludeert dat de overheid er niet in slaagt om de negatieve en zeer belastende registraties van verzoeker op de juiste naam, namelijk die van de echte dader, te zetten. Hij neemt er met instemming kennis van dat er een centraal meldpunt wordt ingesteld waar slachtoffers van identiteitsfraude terecht kunnen. Over de eventueel aan meneer K. te betalen schadevergoeding is het laatste woord nog niet gezegd. Intussen overweegt meneer K. ook een proces aan te spannen tegen een hotel dat in 2006 camera's in zijn kamer zou hebben opgehangen, omdat hij kennelijk voor een drugscrimineel werd aangezien (Nationale Ombudsman 2009).[1]

Het meldpunt is er inmiddels.[2] De wetgever heeft met de Wet identiteitsvaststelling verdachten, veroordeelden en getuigen (Stb. 2009, 317) het probleem van de identiteitsfraude ook nader willen aanpakken. Maar meneer K. is anno 2010 nog bezig de scherven op te ruimen, hoewel de werkelijke persoon van zijn virtuele kwelgeest al sinds 2002 in de gevangenis schijnt te zitten.

De problemen die meneer K. had met de overigens onjuiste gegevens in zijn virtuele verleden, overkomen ook anderen. Zo is er de Marokkaanse Nederlander Driss Z. die in 2009 werd opgepakt na een 'mismatch' door de Verwijs Index Personen: een geval van persoonsverwisseling. Of de 16-jarige jongen die ten onrechte van zijn bed wordt gelicht als verdachte van mishandeling, omdat het slachtoffer hem meende te herkennen nadat aan dit slachtoffer schoolfoto's van scholen uit de buurt die op Hyves waren geplaatst waren voorgehouden. Een rechercheur was met de foto naar de betreffende school gegaan om te verifiëren of de jongen inderdaad op school zat en om diens adres te vernemen (Bert Keizer 2010).

Deze problemen illustreren het onderwerp van de onderhavige beschouwing. Als gevolg van de digitalisering van het strafrecht lijkt ieder belast met zijn verleden en gevoelig voor het virtuele beeld dat van hem bestaat. Dat beeld is gebaseerd op gebeurtenissen en mededelingen uit het verleden. Het beeld krijgt door de technologie een scherpte die meer dan ooit een illusie van juistheid oproept, ook als dat niet terecht is. De vraag is of er niet een recht zou moeten bestaan voor burgers om de digitale beelden die van hen zijn opgeslagen te doen vergeten. Een recht op vergetelheid. Een minstens even belangrijke vraag is of de overheid niet een zekere verantwoordelijkheid zou moeten nemen om ervoor te zorgen dat bepaalde – ook buiten het overheidsdomein bestaande – gegevens na verloop van tijd vanzelf verdwijnen.

5.1 BELEID, INFORMATIE EN TECHNOLOGIE: VERANDERINGEN

In het kader van het WRR-project Beleid, Informatie en Technologie wordt nagedacht over de nieuwe dynamiek die het gevolg is van het voortschrijden van de mogelijkheden van de informatietechnologie. De nadruk ligt steeds op de verhouding tussen overheid en burger, alsmede op de samenwerking tussen diverse overheden in tijden van voortschrijdende technologie. In deze bijdrage gaat het om het domein van het strafrecht, of zo u wilt de politie- en justitieketen.

Er zijn de afgelopen twintig jaar enorme veranderingen geweest die dat domein raken. Ik doel dan op het toegenomen belang dat in het beleid aan veiligheid wordt toegekend en op de veranderingen in het inlichtingenwerk. Die veranderingen krijgen extra betekenis in het licht van de technologische ontwikkelingen. Als gevolg daarvan is steeds vanzelfsprekender geworden dat iets wordt opgeslagen in plaats van dat het wordt vergeten.

5.1.1 STRAFRECHT IN DE RISICOSAMENLEVING

De belangrijkste ontwikkeling op het vlak van het strafrechtelijk beleid is het denken in termen van een streven naar veiligheid en risicobeheersing. Waar het denken in de jaren zeventig en tachtig nog werd gekenmerkt door een beduchtheid voor een almachtige overheid – hetgeen bijvoorbeeld is beïnvloed door de eerste veroordeling van Nederland door het Europese Hof voor de Rechten van de Mens (EHRM 23 juni 1976 (*Engel*), NJ 1978: 224) – verandert dit in de jaren negentig. Steeds meer wordt van de overheid verlangd dat zij de burgers beschermt tegen risico's in de samenleving. In het domein van het strafrecht leidt dit tot een paradigmatische verandering – een fundamenteel andere manier van kijken die zowel waarneembaar is in het materiële strafrecht als in het strafprocesrecht.

In het materiële strafrecht ontstaan steeds meer strafbaarstellingen die niet zijn gebaseerd op het idee dat het opzettelijk (en in bijzondere gevallen door onvoor-

zichtigheid) toebrengen van schade moet worden gestraft. Naast de gevaarzettingsdelicten die het Wetboek van Strafrecht al kende (zoals brandstichting) komen meer wetten tot stand volgens welke louter het teweegbrengen van risico of het verrichten van iets wat ons moreel niet onverschillig laat voldoende is voor strafbaarheid.[3] Niet alleen in de sfeer van de strafbaarstelling maar ook in de sfeer van de straffen en maatregelen en zelfs bij de tenuitvoerlegging wordt steeds meer 'proactief' gedacht. Zo is de gemiddelde duur van de maatregel die een tot ter beschikking stelling (tbs) veroordeelde daadwerkelijk ondergaat van 2000-2008 bijna verdubbeld van 5,5 naar 9,7 jaar (Inspectie voor de sanctietoepassing 2009: 21). Daarbij is ook het verlofstelsel drastisch verhard. Het wordt inmiddels aanvaard dat de zedendelinquent alleen op verlof uit zijn tbs-inrichting mag als hij 'vrijwillig' een (onaangenaam) libidoremmend middel aanvaardt.

In het strafprocesrecht zien we een vergelijkbare verandering (Buruma 2005: 81-83). Het vroegere paradigma was dat er ergens een lijk lag met een mes tussen de ribben en de politie zocht bij dat vermoedelijk strafbare feit een verdachte. Tegenwoordig is er een persoon die riskant is vanuit het oogpunt van terrorisme, georganiseerde misdaad, of veelplegen of die als klant van de psychiatrie of de jeugdzorg dan wel anderszins als bekende van de politie speciale aandacht krijgt. Dergelijke personen worden in het oog gehouden om bij hun beweerdelijk riskante profiel een daad te vinden. Men zoekt niet de dader van een bekende inbraak, maar de daden van een bekende inbreker. Hoewel aldus iets te stellig geformuleerd – er wordt natuurlijk nog steeds klassiek gespeurd om gepleegde moorden op te lossen – is het verschil in benadering fundamenteel veranderd.

In de risicosamenleving zijn twee richtsnoeren van belang (Buruma 2007). Of men nu risico's wil reduceren of de waarde van de rechtsstaat wil uitdragen, men zal van deze twee kernpunten moeten uitgaan:

1 Het kan in een rechtsstaat niet zo zijn dat de overheid een mensenleven verwoest louter op grond van toekomstvoorspelling.
2 Het kan in een moderne democratie niet zo zijn dat de overheid niet ingrijpt als een mensenleven dreigt te worden verwoest, omdat ze de ogen sluit voor wetenschappelijk onderbouwde mogelijkheden van risicotaxatie, diagnose en interventie.

Dat we op grond van toekomstvoorspelling geen levens mogen verwoesten betekent dat de rechter hooguit bereid zal zijn een leven te verwoesten als zijn beslissing niet louter is gebaseerd op toekomstvoorspelling, maar ook kan worden beschouwd als een consequentie van het eigen gedrag van betrokkene. Levenslang voor een zevenvoudige moord is aanvaardbaar als betrokkene het gedaan heeft. Levenslang louter vanwege het risico dat iemand zo'n delict zal gaan plegen is niet aanvaardbaar. Dat wordt pas anders als er aanleiding is om zo'n drastische maatregel te rechtvaardigen, bijvoorbeeld bestaand in het feit dat betrokkene reeds een

moord heeft gepleegd in combinatie met aanwijzingen dat hij het weer gaat doen. Het uitgangspunt blijft echter dat uiterste gevolgen niet gebaseerd mogen zijn louter op toekomstvoorspelling als we mensen een vrije wil toedichten. Ook het kind van een seriemoordenaar uit een anomische buurt met een veel te lage angstdrempel kan brandweerman of politieagent worden. De kans is misschien klein, maar als we aan die mogelijkheid voorbijgaan, is dat het einde van de rechtsstaat. Anderzijds wordt niet langer aanvaard dat de overheid geen gebruik zou maken van wetenschappelijke inschattingen. Goede taxaties kunnen zeker helpen bij het nemen van maatregelen. Zij zijn er niet om levens te verwoesten maar om levens onder dwang te verbeteren. De kinderpsychiater Th. Dorelijers zei ooit dat ADHD-kinderen er recht op hebben dat wordt voorkomen dat ze in de criminaliteit terechtkomen. Die benadering om criminaliteit of een criminele predispositie als ziekte te beschouwen is onder meer gekozen door de World Health Organization (WHO). Mensen hebben er in dat perspectief recht op dat hun risico serieus wordt genomen. Als we mensen de kans geven hun aanleg tot borstkanker snel op te sporen en aan te pakken, moeten we ook mensen die de aanleg hebben in de criminaliteit terecht te komen snel helpen – daar heeft zo iemand niet alleen zelf wat aan, zoals de borstkankerpatiënt, maar ook de omgeving.

De aldus geschetste tegenstelling impliceert dat we niet de ogen moeten willen sluiten voor de mogelijkheden die de nieuwe technieken bieden. Anderzijds kan de enkele mogelijkheid van gevaar die uit de opgeslagen gegevens blijkt niet genoeg zijn om voor mensen ingrijpende activiteiten te verrichten. Het is een evident spanningsveld zodra we denken aan de ervaring die inmiddels bestaat met de inschatting van risico's. Zowel bij de advisering aan de rechter over de vraag of iemand misschien een tbs zou moeten krijgen, als bij de beslissingen over de verlenging van de tbs wordt al van oudsher een inschatting van gedragsdeskundigen vereist. Inmiddels zijn er risicotaxatie-instrumenten ontwikkeld om deze adviezen een grotere graad van (interbeoordelaars)betrouwbaarheid te geven.[4]

Bijna altijd spelen historische factoren daarbij een rol (zoals de justitiële voorgeschiedenis, eigen slachtofferschap, eerder middelengebruik en psychiatrische ziektegeschiedenis). Maar bijvoorbeeld in de zogenaamde HC.R-20 en de HKT-30 schalen – waarmee algemene recidivekansen worden getaxeerd – wordt ook gelet op klinische gegevens (zoals impulsiviteit, huidig middelengebruik en probleeminzicht) en met toekomstgerichte of op risicomanagement gerichte factoren (zoals de begeleidbaarheid van betrokkene en zijn sociaal netwerk). In een meta-evaluatie gaan Harte en Breukink op maar liefst 26 van dergelijke instrumenten in (Harte & Breukink 2010; Emmerik 2008). Hun kritisch oordeel houdt onder meer in dat de predictieve validiteit – oftewel het vermogen om recidive te voorspellen – van de zojuist genoemde taxatie-instrumenten (en veel andere) wellicht hoger is dan een niet gestandaardiseerd klinisch oordeel, maar dat deze validiteit nog steeds niet geweldig is. Zelfs de beste instrumenten geven foutkansen. Mensen kunnen

ten onrechte als riskant worden beoordeeld (fout positief) en ten onrechte als ongevaarlijk (fout negatief); zie ook hierna paragraaf 5.2.3. Vooral over die zogenaamde fout-positieven is weinig bekend, terwijl die mensen dus mogelijk ten onrechte in de tbs terechtkomen of blijven. In een onderzoek van Hildebrand c.s. werden dossiers van ex-tbs-gestelden van wie de maatregel inmiddels enkele jaren geleden was beëindigd retrospectief gescoord. Het blijkt dat ongeveer 45 procent van degenen die volgens de risicotaxatie hoog recidive-gevaarlijk leken, niet opnieuw was veroordeeld (Hildebrand et al. 2005; Lodewijks 2008: 99).[5] Ten aanzien van hen moeten we de vraag onder ogen zien of hun leven is verwoest vanwege de eisen van de risicosamenleving.

5.1.2 INLICHTINGENWERK

Vanaf het midden van de jaren tachtig is de politie meer 'informatiegestuurd' gaan werken. Inmiddels beschikken alle regionale korpsen evenals de nationale recherche over speciale criminele inlichtingen eenheden (CIE's) om informatie over personen te verzamelen. Die ontwikkeling hangt samen met de zojuist gesignaleerde beleidsverandering, maar ook met de veranderde technologische mogelijkheden. In het klassieke inlichtingenwerk gaat het vooral om gegevens die via al dan niet heimelijke methoden zijn verkregen van menselijke bronnen. Bij die menselijke bronnen is te denken aan informatie van informanten en infiltranten en gegevens van getuigen en deskundige organisaties (zoals jeugdzorg of reclassering). Steeds meer zien we evenwel dat de politie beschikt over gegevens die afkomstig zijn van technische bronnen.

Zeker na de Wet bijzondere opsporingsbevoegdheden (Stb. 1999: 245) heeft het gebruik van camera's in verband met observatie, het tappen van telecommunicatie, het opvragen van verkeersgegevens over telecommunicatie en het gebruik van afluisterapparatuur een grote vlucht genomen. In 2008 heeft justitie 26.425 telefoonnummers afgeluisterd met als gevolg dat gemiddeld 1946 taps per dag lopen.[6] En dan te bedenken dat er ongeveer 8000 rechercheurs bij de politie werken (Klerx 2008), of – om een ander perspectief te geven – er worden jaarlijks tegen 25.000 verdachten (al dan niet deels) onvoorwaardelijke gevangenisstraffen opgelegd en daaronder zitten ook veelplegers, dronken rijders en incestplegers waarbij geen enkele tap plaatsvindt. Wanneer we dan ook nog bedenken, hoeveel gesprekken er via een afgeluisterd toestel worden gevoerd, dan is het duidelijk hoe gigantisch het voorhanden werk is.

Een andere indicatie van de omvang van de voor de politie beschikbare digitale bronnen is het cameratoezicht in 22 van de 25 steden met meer dan 100.000 inwoners (Hissel & Dekkers 2008).[7] Hoewel volgens onderzoekers van het Sociaal en Cultureel Planbureau (SCP) het vertrouwen in de preventieve werking van cameratoezicht dat veel (lokale) overheden hebben vooralsnog niet wordt waarge-

maakt, kan de politie sneller ingrijpen wanneer een incident dreigt te escaleren. Maar bovenal kunnen de cameragegevens achteraf worden gebruikt ten behoeve van de opsporing (Van Noije & Wittebrood 2009: 66; HR 20 april 2004, LJN: AL8449). Ook de kentekenlezende zogenaamde CatchKen of ANPR-camera's boven de snelwegen worden feitelijk gebruikt ten behoeve van de opsporing van andere zaken dan het rijden zonder de kentekenbelasting te hebben betaald, hoewel ze daar formeel niet voor zijn aangelegd. Ik kom er in paragraaf 5.3.4 op terug. En dan kunnen we ook nog denken aan de DNA-bank, waarin DNA-materiaal van 98.000 burgers is opgeslagen.[8] Waar DNA-materiaal in het verleden vooral als bewijsmateriaal werd beschouwd (om te controleren of de gevonden sporen pasten bij de reeds als verdachte aangemerkte bekende persoon), is de betekenis van die bank steeds nadrukkelijker dat daarmee een indicatie wordt gegeven wie de tot dan toe onbekende verdachte zou kunnen zijn.

Aparte vermelding verdient het opvragen van gegevens bij derden. In de vroege eenentwintigste eeuw wordt er zowel in het bedrijfsleven als via de zogenaamde sociale netwerken nog meer opgeslagen dan in officiële registers. Daar wordt immers informatie bewaard over financiële transacties, communicatie, reizen, *web searches*, juridische procedures, consumentenvoorkeuren, en geleidelijk aan ook gedragsmatige en biologische gegevens. Dergelijke informatie is zowel te verkrijgen via open bronnen (zoals sociale netwerken) als door op voet van de Wet vorderen gegevens (Stb. 2005, 390) gebaseerde verzoeken tot uitlevering aan de houder van de gegevens. Spectaculair is dat 2,8 miljoen keer per jaar telefoongegevens – inclusief zogenaamde verkeers- en locatiegegevens – worden opgevraagd.[9] Deze gegevens leveren zelden bewijs van rechtstreekse betrokkenheid bij een delict. Vaker zijn ze van belang als start- of sturingsinformatie. Dat kan zijn om te achterhalen met wie een reeds bekende verdachte nog meer contact had. Ook worden locatiegegevens veiliggesteld in de buurt van een plaats delict teneinde verdachten te identificeren en in steeds meer zaken ook om ontkenningen en alibiverweren te ontkrachten. Een bekend voorbeeld van dergelijk gebruik is de Deventer moordzaak.

De technologische veranderingen van informatiegaring droegen bij aan een andere benadering van het inlichtingenwerk. Het gebeurt minder heimelijk dan vroeger toen de inlichtingendiensten zelf nogal geheimzinnig opereerden (Mottram 2007). Zelfs de AIVD en de CIA hebben nu een eigen website. Dat neemt niet weg dat de afscherming van informanten en dergelijke nog evenveel nadruk krijgt als vroeger. Sterker nog, tegenwoordig wordt openlijk opgeroepen tot het doen van anonieme meldingen met het oog op strafrechtelijke doelen. Men kan anoniem terecht bij de politie (CIE's) en bij de publiek-private Stichting M die anonieme meldingen doorspeelt aan de politie. Er is discussie gaande over het doen van anonieme aangifte. Zelfs geheimhouders worden in staat gesteld hun waarnemingen en vermoedens discreet te melden, bijvoorbeeld bij het Meldpunt Kindermishandeling, hetgeen soms leidt tot inlichtingen in de richting van de politie.

Al met al heeft het inlichtingenwerk gigantische ontwikkelingen doorgemaakt. De hoeveelheden gegevens die worden vergaard en bewaard zijn haast ontelbaar. En de gedachte *select before you collect* is nog geen gemeengoed (Jacobs 2007).

5.1.3 TECHNOLOGISCHE ONTWIKKELING

Het streven naar veiligheid in de risicosamenleving en de ontwikkeling van de informatiegestuurde opsporing moet begrepen worden tegen de achtergrond van de digitale revolutie aan het eind van de twintigste eeuw.[10] Deze heeft het in hoog tempo gemakkelijker gemaakt te bewaren wat aan gegevens is vergaard en te zoeken in wat is opgeslagen.[11]

Op het eerste gezicht lijkt het web een superbibliotheek. We lezen er kranten en artikelen en we downloaden films en muziek. Maar vanaf ongeveer 2001 realiseren gebruikers zich dat internet er niet alleen is om informatie te ontvangen, maar ook om informatie te scheppen en te delen. Men spreekt wel van Web 2.0. Of dat nu gebeurt via Facebook en Hyves, via blogs of twitter, via chatfora en dating sites, steeds meer mensen nemen deel aan inhoud scheppende activiteiten op het web. Met onze digitale camera's, e-mail, mobiele telefoons en elektronische agenda's slaan we zelf steeds meer data digitaal op. Het is uitgerekend dat Wal-Mart, een supermarktketen, per uur 1 miljoen transacties verwerkt en daarmee databases vult van meer dan 2.5 petabytes.[12] Ook anderen plaatsen informatie over ons in een digitale omgeving: de dokter plaatst medische gegevens, de disco leuke foto's van dansende klanten, en de winkelier afschrikwekkende foto's van winkeldieven – soms zijn de gegevens beveiligd, soms niet.

Het bestaan van dergelijke bestanden roept de vraag op in hoeverre de overheid een taak dienaangaande heeft. Aan de ene kant is er de vraag in hoeverre autoriteiten bevoegd zijn de gegevens te gebruiken. Aan de andere kant is er de vraag in hoeverre de overheid een taak heeft sommige bestanden tegen te gaan en andere met waarborgen te omgeven. We zitten op dit moment midden in de discussie daarover: men hoeft maar te denken aan het Elektronisch Patiëntendossier (EPD). Art. 126nf Sv maakt het mogelijk dat de officier van justitie met machtiging van de rechter-commissaris informatie daaruit opvraagt om deze voor de opsporing te gebruiken, maar dat wordt in de discussies over het EPD doorgaans niet benadrukt. Anderzijds zijn er zorgen over de mate waarin verzekeraars ondanks alle toezeggingen toch inzage kunnen krijgen, hierbij kan men denken aan het gevaar van misbruik (door pillenshoppers) via identiteitsfraude en dergelijke.

En we gaan alweer een stap verder met internet-der-dingen: ook apparaten worden steeds meer uitgerust met geheugen als gevolg waarvan we in ons moderne leven steeds meer digitale sporen achterlaten: betaaltelevisie, de OV-chipkaart, de ANPR- (of CatchKen) camera's die onze bewegingen op de snelweg fotograferen,

de mobiele telefonievoorzieningen waarmee geïndiceerd wordt waar wij (althans onze telefoons) waren. Intelligente autonome omgevingen – waar men op naam herkend wordt bij binnenkomst van een winkel dankzij de Rfid-chip in de klantenkaart – zullen weer nieuwe problemen en vraagstukken opleveren: identiteitsverwisselingen en stigmatisering liggen op de loer (Hildebrandt & Koops 2010).

De groei van de digitale opslagruimte verloopt sneller dan die van ons vermogen om informatie na te slaan (op te halen) en nuttig te gebruiken. Niettemin wordt de technologie steeds verfijnder om in grote verzamelingen gegevens te zoeken, ze te analyseren en er patronen in te vinden. Dat gebeurt met scherpzinnige kwantitatieve technieken: data management en analyse worden inmiddels beschouwd als cruciale onderdelen in de software-industrie. Het duurde tien jaar om de drie miljard basisparen van het menselijk genoom te analyseren eer dat in 2003 gebeurd was; in 2010 had dat een week gekost. Het lijkt erop dat data-intensief onderzoek een nieuwe revolutie in de wetenschappen zal bewerkstelligen (Hey et al. 2009; Lazer et al. 2009). Bovendien is er steeds meer aandacht voor het bewerkstelligen van zinvolle verwerkingsmogelijkheden. Steeds meer wordt opgeslagen in geïntegreerde bestanden en er is steeds meer aandacht voor standaardisering in de opslag (Bell & Gemmell 2008; Allen 2008). Niettemin is veel digitale opslag nog niet aan elkaar gekoppeld: menige mobiele telefoon bevat informatie die de eigenaar vergeten is te downloaden op zijn pc, zoals dat ook geldt voor informatie van zijn ziektekostenverzekeraar en zijn kabelbedrijf. Het is bovendien verrassend moeilijk om diverse databestanden te koppelen. Een gebrek aan daadwerkelijke standaardisatie zorgt voorts voor moeilijkheden om in grote – of gekoppelde – bestanden verstandig om te gaan met deels afwezige gegevens, of net anders gedefinieerde gegevens (is het ben laden of bin laden?), of ook kwalitatief weinig betrouwbare gegevens.

Een basisnoodzaak om alle opgeslagen gegevens te kunnen verwerken bestaat in het toevoegen van zogenaamde metadata en indexering, zoals vroeger catalogi op auteursnaam, titelnaam, onderwerp, taal en dergelijke konden worden aangelegd. Deze metadata (of 'tags') helpen de opgeslagen data terug te vinden en te verwerken. Steeds vaker worden tags min of meer automatisch toegevoegd zoals de datum en tijd waarop een foto is gemaakt, gegevens over de ontvangers en de bellers van telecommunicatie, en geolocatie in mobiele telefoons. Die tags maken het mogelijk bestanden te doorzoeken en (relatief anoniem) te bewerken. Sterker nog, iedereen die zoekt op internet schept alleen al daardoor metadata ('klanten die hierin waren geïnteresseerd, waren ook geïnteresseerd in XYZ'). Bij de bewerkingen is te denken aan de lotgevallen van de postcode. Die was ooit bedoeld om de post sneller te kunnen sorteren, maar wordt tegenwoordig gebruikt door marketingmensen om wijken te kunnen bestoken met min of meer gepersonaliseerde reclame. Ietwat technisch gezegd: de postcode is gedecontextualiseerd (uit de context van de postbezorging gehaald) en gerecontextualiseerd door deze te

koppelen met demografische gegevens (rijk/arm, stad/land, enz.).
De technologie heeft een massale gegevensopslag mogelijk gemaakt en we staan aan de vooravond van een revolutie in het intelligente gebruik van de uit bewerkingen van die gegevens te trekken conclusies.

5.2 HET GEHEUGEN IN HET DIGITALE TIJDVAK

Tegen de achtergrond van de in de vorige paragraaf beschreven veranderingen op het vlak van beleid, inlichtingenwerk en technologie moet de vraag onder ogen worden gezien hoe we de kwaliteit van gegevens die worden vergaard, opgeslagen en bewerkt, moeten beoordelen. Daartoe moeten we beseffen dat de digitale opslag van gegevens fundamenteel anders is dan de gewone, biologische manier van herinneren. Viktor Mayer-Schönberger heeft dat pregnant verwoord met de stelling dat vergetelheid is veranderd van een *default* – iets wat overblijft als je niets doet – in iets wat inspanning vergt (Mayer-Schönberger 2009). Volgens hem hebben de technologische innovaties en de daarmee gepaard gaande maatschappelijke en juridische ontwikkelingen een eind gemaakt aan de vanzelfsprekendheid van het vergeten.

In een bespreking van het werk van Mayer-Schönberger relativeert Blanchette diens stelling. Hij wijst erop hoe snel de marktontwikkelingen gaan, hetgeen tot gevolg heeft dat er wel degelijk databestanden zijn die nauwelijks meer te openen zijn: plain text is niet XML is niet Word is niet PDF is niet TIFF (Blanchette, in voorbereiding). Inderdaad: wat ik ooit heb opgeslagen op grote slappe floppies is de facto verloren. Ik weet dan ook niet zeker of het papieren archief van de rechtenfaculteit uit de jaren zeventig, tachtig niet de facto beter is te ontsluiten dan het archief van de digitale decaan van het eerste decennium van de eenentwintigste eeuw.

Niettemin moet worden erkend dat een deel van hetgeen digitaal is opgeslagen sneller en preciezer aan de vergetelheid is te ontrukken dan hetgeen is toevertrouwd aan het papieren archief van de negentiende en twintigste eeuw. Zo bezien lijkt het digitale geheugen veel voor te hebben op het biologische. Het is de moeite waard te onderzoeken waarin de wezenlijke verschillen schuilen.

5.2.1 BIOLOGISCH EN DIGITAAL VERGETEN

Herinnering is doorgaans de wenselijke toestand: daardoor leren we wat waardevol en nuttig is. We kunnen dankzij ons geheugen onze hoogstpersoonlijke ontwikkeling bijhouden en onze sociale contacten versterken. Dankzij de taal kunnen we onze herinnering delen met anderen. Door ons talig vermogen te generaliseren en te abstraheren is het minder relevant alle details uit het verleden te onthouden. Dankzij dat vermogen heeft de mensheid het verschil geleerd

tussen de subjectieve belevingen van het verstrijken van de tijd en de objectieve voortgang van de geschiedenis. We kunnen over het verleden spreken in volgordelijkheid: eerst dit, toen dat. En dat maakt het mogelijk zelfs causaliteit te veronderstellen (Pinker 2007: 188-208).

De kern van het biologische geheugen is de koppeling van de ene gedachte aan de andere. We relateren een nieuw gegeven aan wat al is opgeslagen. Geavanceerd laboratoriumonderzoek toont steeds weer aan dat ons brein – met de werking van de neuronen en synapsen – uiteindelijk zo is samengesteld dat het coherente verbanden kan herkennen en leggen. De herinnering werkt niet als een videoapparaat of een harddisk waarmee gegevens worden opgeslagen, maar lijkt eerder op een web van verbanden tussen mensen en dingen (Greene 2010). Met het opslaan wordt het verband al gelegd: zonder verband geen opslag. Dat verschil met de computer zal voor ons belangrijk blijken. Het verklaart niet alleen de geringere betrouwbaarheid van het biologisch geheugen, maar dwingt er ook toe na te denken over het kenmerk dat digitale opslag van een gegeven niet vanzelf gepaard gaat met de opslag van contextuele gegevens.

Biologisch vergeten kan verschillende vormen aannemen.[13] Het volgende overzicht ontleen ik aan de psycholoog Schacter (Schacter 2001; Dodge & Kitchin 2007):[14]

- *Transience:* Met het ouder worden verdwijnen details.
- *Absent-mindedness:* Niet alles wordt opgeslagen op het moment dat dit kan. Onder meer onze emoties en vooroordelen beïnvloeden de waarneming en daarmee ook wat wordt opgeslagen.
- *Blocking:* Soms zijn er voorvallen na de opslag die het moeilijk maken de herinnering terug te halen.
- *Misattribution:* Een gebeurtenis wordt toegeschreven aan de verkeerde persoon of in verband gebracht met een andere gebeurtenis, hoewel dat verband niet correct is.
- *Suggestibility:* Het kan zijn dat door een ander de suggestie ontstaat van een gebeurtenis die helemaal niet heeft plaatsgevonden. Dit is een belangrijk onderwerp in de rechtspsychologische literatuur over verhoormethoden.
- *Bias:* Retrospectieve distorsies vinden plaats als betrokkene zelf het achteraf logisch vindt dat iets wel zal zijn gebeurd, terwijl dat niet zo is. Onbewust 'corrigeert' hij dan zijn geheugen. Ook is er de *fading effect bias* waardoor veel mensen emotioneel indringende narigheid in de loop van de tijd minder intens voelen, terwijl ze prettige dingen en handelingen waar ze trots op zijn juist goed onthouden.

Deze verschillende verschijnselen beïnvloeden elkaar. Zo merken we de laatstgenoemde zelfcorrecties niet altijd op als gevolg van het blokkeermechanisme. Elke keer dat we een gegeven oproepen in ons geheugen wordt het daarna heropgesla-

gen als nieuwe herinnering en daardoor wordt de oude, oorspronkelijke opslag moeilijker toegankelijk (LeDoux 2008). Daardoor 'herinnert' een ooggetuige zich wat hij in de krant heeft gelezen over een gebeurtenis waar hij zelf bij was in plaats van wat hij zag.

De mensheid heeft eerst via liederen, later via schrift, boekdrukkunst en de laatste eeuw via grammofoonplaten, fotografie en film haar biologische beperkingen weten te ondervangen. Met de digitalisering is een geheugen ontstaan dat op enkele cruciale punten afwijkt van het biologische en/of het collectieve geheugen van weleer. In de eerste plaats zijn computers veel beter in staat om getrouw enorme massa's details op te slaan (en deze later weer na te slaan) dan mensen. In de tweede plaats maakt een digitaal geheugen het mogelijk op grond van die authentieke details nieuwe verbanden te leggen, die op zich betrouwbaarder zijn dan de patronen die je geheugen vormt.

Hiervoor noemde ik de gebruikelijke biologische zwakten van mensen als gevolg waarvan ze vergeten. Bezien we de digitale geheugens, dan zijn deze zwakten afwezig of enigszins anders van aard. Ik loop ze achtereenvolgens na:
- Het digitale geheugen vervliegt niet, tenzij je het instelt dat het zichzelf na verloop van tijd vernietigt.
- Op zich kan alles worden opgeslagen, ook allerlei details die je op het moment van de gebeurtenis (bijvoorbeeld door je emotionele betrokkenheid) had gemist; denk aan een foto waarop een bekende op de achtergrond blijkt te staan.
- Het terughalen van digitaal opgeslagen gegevens is geen probleem, tenzij er een beveiliging op het bestand zit. Die beveiliging kan van wettelijke, technische of organisatorische aard zijn.
- Verbanden en correlaties kunnen naderhand worden gelegd, maar dat gebeurt dan welbewust en in beginsel toetsbaar – denk aan de adviezen van amazon.com over wat je waarschijnlijk ook leuk vindt om te lezen op grond van wat je eerder had besteld.
- Ook technologische suggestibiliteit is mogelijk, omdat valse gegevens kunnen worden teweeggebracht door onopzettelijke of opzettelijke foutieve invoer (al dan niet door een ander) en/of aanpassing.
- Retrospectieve distorsie zal niet plaatsvinden, maar het omgekeerde wel. Valse gegevens ontstaan door het achterwege blijven van actualisering. De gedachte ontstaat dat het opgeslagen materiaal nog wel zal kloppen.

In de woorden van Gordon Bell is dit als volgt samen te vatten: "Biological memory is subjective, patchy, emotion-tinged, ego-filtered, impressionistic, and mutable. Digital memory is objective, dispassionate, prosaic, and unforgivingly accurate." (Bell & Gemmell 2009: 56) Misschien gaat Bell in zijn enthousiasme voorbij aan enkele reële problemen. Die worden onder meer aangestipt in de laatste twee bullets. Maar belangrijker nog is een derde cruciaal punt waarop het digi-

tale geheugen afwijkt van het biologische – en dit keer valt het verschil niet automatisch in het voordeel van de technologie uit. Dit is hetgeen onder de vierde bullet stond vermeld – dat digitale opslag een specifieke beslissing vergt over de vraag welk gegeven met welke andere gegevens in verband wordt gebracht: de context wordt niet automatisch geassocieerd.

5.2.2 IJKPUNTEN: ACCURATESSE, BETROUWBAARHEID EN CONTROLE

Het digitale geheugen maakt de toegang tot opgeslagen data sneller en gemakkelijker. Deze versnelling heeft diverse gevolgen voor het beoordelen van de impact van de technologie op de kwaliteit van de data. Ik beperk me tot problemen met betrekking tot drie ijkpunten: accuratesse, betrouwbaarheid en controle. Accuratesse van een tekst bestaat onafhankelijk van de wil van de spreker of die van zijn publiek. "Reality is that which, when you don't believe it, doesn't go away", weten journalisten die niet alleen geïnteresseerd zijn in opinies (Kovach & Rosenstiel 2007: 48).[15] Verificatie van feiten ter bevordering van de accuratesse van een tekst of een bestand blijft op het digitale web vaak achterwege. De snelle mogelijkheid van plaatsing van data op internet of in niet-direct toegankelijke bestanden draagt bij aan het nalaten van verificatie. Niettemin wekken bepaalde feiten het gevoel op dat je de waarheid dan wel kent. Manjoo spreekt in dit verband van de *post-fact society* waarbij *truthiness* belangrijker is geworden dan *truth* – 'weten met het hart' is belangrijker geworden dan 'denken met het hoofd' (Manjoo 2008: 188-189).

De waarheid van een bewering hangt niet alleen af van de accuratesse ervan in termen van de verifieerbare correspondentie met een werkelijke stand van zaken. De Britse filosoof Sir Bernard Williams beschouwt als de twee belangrijkste deugden van waarheid naast accuratesse de ernst (*accuracy and sincerity*) (Williams 2002). Beweringen worden ook gedaan in gevallen waarin kennis niet eigen is, maar wordt doorgegeven. Wij verlangen dan van de spreker dat hij zelf gelooft dat het waar is wat hij zegt. Juist de massaliteit en de snelheid van het digitale doorgeven van gegevens onderstreept het belang hiervan. In het bijzonder geldt in dit verband het belang van wat ik zou willen noemen de (contextuele) betrouwbaarheid. Deze betrouwbaarheid – in de specifieke betekenis van Williams – heeft betrekking op de omstandigheid dat feiten betekenis krijgen door ze een plaats te geven zowel in hun historische (diachrone) als in hun gelijktijdige (synchrone) context op een wijze die niet alleen de spreker maar ook anderen binnen diezelfde context voor juist houden. Ter illustratie: de mededeling van de politicus Wilders dat de voorzitter van het CDA maar vakantie moest nemen was bedoeld als blijk van afkeuring (synchrone context), maar werd opgevat als een milde uitlating in het licht van eerdere uitspraken (historische context). Een bewering zal in de context waarin ze 'aankomt' moeten worden ingepast op een wijze die ook anderen die zich in de oorspronkelijke details hebben verdiept correct zouden hebben gevonden (wat wetenschappers 'interbeoordelaarsbetrouwbaarheid' noemen).

Hier wordt in de volgende subparagraaf uitgebreider (in 5.2.3) op ingegaan. Ik herinner er nu alvast aan dat voor het terughalen van opgeslagen gegevens tags of metadata aan de gegevens moeten worden gehangen. Dat levert een bijzondere vorm van contextafhankelijkheid op. De politie kan iemand bijvoorbeeld registreren als iemand die vier keer met de politie in aanraking is geweest. Degene die conclusies trekt uit het gegeven 'vier politiecontacten' moet in staat zijn dit (al dan niet accurate) getal te duiden in het licht van de context – bijvoorbeeld in verband met een voortslepende burenruzie. In dat voorbeeld is de gebruikelijke connotatie van de tag 'bekende van de politie' niet helemaal juist.

Een derde ijkpunt betreft niet een factor die de waarheid van gegevens betreft als wel de zeggenschap (controle) van personen over op hen betrekking hebbende gegevens (Sen 2009: 236-238). Ook op dit punt wordt hierna uitgebreid teruggekomen (in subpar. 5.4.3). Hier wordt erop gewezen dat het er niet eens toe doet wie het gegeven heeft opgeslagen: een ander of uzelf. Feit is dat u na de opslag de controle erover verliest. Het hangt van technische, organisatorische en wettelijke omstandigheden af wie tot die opgeslagen gegevens toegang hebben. Het antwoord op de vraag wat er met de over ons bestaande gegevens gebeurt, is afhankelijk van anderen – ongeacht of die gegevens waar zijn of niet en ongeacht of uzelf de keuze hebt ook andere gegevens bekend te maken. Dit gebrek aan controle heeft met onze vrijheid te maken. Terecht schreef Bernard Williams immers: "To lack freedom is paradigmatically not simply to be short of choices but to be subject to the will of others"(Williams 1993: 154).

5.2.3 SPECIFIEKE BETROUWBAARHEIDSPROBLEMEN: FOUT POSITIEF EN FOUT NEGATIEF

De digitale technologie maakt het – zoals gezegd – mogelijk getrouw massa's gegevens op te slaan en tussen die gegevens nieuwe verbanden te leggen. Als we nu even afzien van problemen van accuratesse en controle, dan zijn er twee specifieke vraagstukken die door deze nieuwe mogelijkheden prangender zijn geworden en die de betrouwbaarheid van de gegevens betreffen. Het eerste probleem ziet op de zogenaamde fout-negatieven: men miskent het belang van een gegeven binnen een bepaalde context en beschouwt het daardoor ten onrechte als niet betrouwbaar (of niet relevant). Ik spreek dan van ruis. Het tweede probleem ziet op de zogenaamde fout-positieven: men denkt ten onrechte dat een bepaald gegeven in de relevante context belangrijk is.

Eerst iets over de 'ruis'. In de Amerikaanse terreurbestrijding spreekt men van *drowning in data but starving for knowledge* (Committee on Technical and Privacy Dimensions 2008: appendix Datamining). Het is lastig belangrijke van onbelangrijke informatie te onderscheiden. Dat geldt in het algemeen, maar zeker met het oog op de inschatting van toekomstige gebeurtenissen. Ten onrechte wordt

gemeend dat het verzamelen van steeds meer data per definitie de relevante kennis doet toenemen, maar dan wordt vergeten dat relevantie een verhouding is tussen wat ertoe doet en wat er niet toe doet. Bij de poging van Umar Farouk Abdul Mutallab om een bom in zijn onderbroek tot ontploffing te brengen op een vlucht van Amsterdam naar Detroit op 25 december 2009 was bekend dat er plannen waren vanuit Jemen (waar Umar was gerekruteerd) en waren er gegevens over de vermoedens van zijn vader binnengekomen, maar niet doorgegeven en was deze zelfs niet op de no-flylist geplaatst. Achteraf lijkt het gevaar evident en wijt men het feit dat de man met een bom in het vliegtuig kwam aan gebrekkige samenwerking van functionarissen en organisaties (*connecting the dots*). In feite kan men dit ook beschouwen als illustratie van de moeilijkheid om belangrijke van onbelangrijke gegevens te onderscheiden. In dit geval was er sprake van een fout negatief – het relevante signaal werd voor ruis aangezien. 'Meer data' leidde tot 'meer ruis'. Juist een overheid die verantwoordelijk is voor het systeem als geheel moet beseffen dat ongeselecteerde opslag van gegevens hooguit helpt die overheid meer in verlegenheid te brengen: achteraf is het verwijt dan eenvoudig te maken dat 'ze het toch had kunnen weten', terwijl op het moment van binnenkomst de mogelijkheid van correcte interpretatie van de overmatig aanwezige informatie eigenlijk afwezig is.

Het tweede probleem is de keerzijde van het voorgaande en betreft gevallen waarin men aan een gegeven ten onrechte te veel waarde hecht. Uiteraard speelt accuratesse hierbij een rol. Maar bij gebrek aan toetsingsmogelijkheden kan het gebeuren dat een gegeven onvoldoende wordt getoetst, omdat het zo waarheidsgetrouw lijkt (de *truthiness* waar ik eerder van sprak). In zo'n geval kan een gegeven een rol gaan spelen in een proces van selectieve waarneming waarmee naar een bredere context wordt gekeken (tunnelvisie). Is wat je hebt gefilmd wel wat het lijkt en is de menselijke – al dan niet anonieme – bron wel betrouwbaar?

Illustratief is de aanleiding van de Irak-oorlog die ten minste deels gevonden moet worden in het zogenaamde *stove-piping*. Daarmee wordt bedoeld dat ruwe inlichtingen direct worden doorgegeven aan de beleidsmakers met voorbijgaan van de procedures die dienen om interpretaties te controleren en gegevens in context te plaatsen (Hersh 2005: 207-224).[16] In die procedures bepalen gedistantieerde experts wat opmerkelijk is en bijvoorbeeld verder onderzoek (of drastischer maatregelen) verdient. De voorlopige aard van veel gegevens en de kwetsbaarheid voor onbetrouwbare of onjuiste invoer leidt doorgaans terecht tot voorzichtigheid bij de interpretatie – een voorzichtigheid bij de interpretatie die doorgaans van wijs beleid getuigt, omdat er anders te veel fout-positieven zouden zijn. Een overheid die alleen maar waarschuwt, wordt als de verveelde herdersjongen uit de fabel van Aesopos die het dorp herhaaldelijk waarschuwde voor een 'een wolf!' die er niet was en niet geloofd werd toen deze daadwerkelijk de schapen bedreigde.

Zowel het probleem van de fout-negatieven als dat van de fout-positieven kan afschuwelijke gevolgen hebben. De mensenhandelaar wordt voortijdig vrijgelaten en meneer K. wordt ten onrechte vastgezet. Het probleem van de fout-positieven klemt te meer, omdat de gegevensopslag iedereen betreft. Fouten worden al lang niet meer alleen jegens 'the usual suspects' gemaakt.

5.3 OPSLAG EN GEBRUIK VAN GEGEVENS IN DE STRAFRECHTSKETEN

De term 'strafrechtsketen' lijkt welhaast gemaakt met het oog op de beoordeling van de werking van de informatietechnologie in het justitiële veld. In deze keten van politie, Openbaar Ministerie, rechter en ten uitvoer leggende instanties wordt als het ware voortdurend een pakketje gegevens doorgeschoven en verrijkt. De politie levert immers een stamproces-verbaal met allerlei bijlagen over de zaak en de persoon (deels ook weer bestaande uit processen-verbaal, bijvoorbeeld van aangifte, van getuigenverhoor, enz.), het Openbaar Ministerie organiseert daarbij rapporten van reclassering en/of gedragsdeskundigen en stelt het strafdossier in de betreffende zaak samen, de rechter schrijft een vonnis, waar dan het gevangeniswezen of het Centraal Justitieel Incassobureau mee aan de slag gaan.

Nu zijn er ook veel gegevens die niet direct in de keten worden opgenomen. Hiervoor bleek in subparagraaf 5.1.2 reeds dat de politie sinds de laatste jaren van de twintigste eeuw zowel beschikt over een keur aan eigen onderzoeksbevoegdheden als over de mogelijkheid om gegevens bij derden te vorderen.

In een arrest van 23 maart 2010 gaat de Hoge Raad op die laatstbedoelde materie nader in (NJ 2010: 326 met noot Mevis). Het Openbaar Ministerie had van het bedrijf Trans Link Systems (TLS), het bedrijf dat de OV-chipkaart levert, de foto's gevorderd van reizigers die in de buurt waren geweest van een aanranding in de metro. Toen het bedrijf bezwaar maakte tegen de vordering kreeg het uiteindelijk gelijk. De redengeving – het opvragen van de foto's zou gevoelige gegevens betreffen en daarom een beslissing conform art. 126nf Sv van de rechter-commissaris vergen – leidde tot enige commotie. Het arrest kan toch niet betekenen dat geen enkele foto meer kon worden gevraagd zonder voorafgaande machtiging van de rechter-commissaris. Een stevig aantal nadere zaken volgde (onder meer Hof Den Haag 6 mei 2010, LJN: BM8433; zie verder Buruma 2010).

De kern is evenwel dat de rechter de juiste maat trachtte te vinden om een al te gemakkelijk opvragen van gegevens bij derden tegen te gaan. Dergelijke verzoeken brengen kosten met zich mee voor degene bij wie de gegevens zijn opgeslagen: het opvragen van de 2,8 miljoen telefoongegevens heeft zelfs de instelling van een speciale dienst, de CIOT, gevergd aan de kant van de telecomproviders. Belangrijker nog is dat dergelijke gegevens afkomstig zijn uit bestanden die dikwijls een

zekere vertrouwelijkheid hebben (hetgeen evident is bij medische bestanden), en in elk geval doorgaans een doel dienen, wat de betrokken subjecten begrijpen, zonder dat ze het op prijs stellen dat iedereen van die gegevens kennisneemt (men denke aan bibliotheek-, videoverhuur- en reisgegevens). De bestandhouders gaan er dan logischerwijs van uit dat ze een zorg voor de privacy van hun klant hebben.

Buiten het opvragen van gegevens bij derden bestaat er gaandeweg steeds meer belangstelling voor het gebruik van open bronnen, zoals sociale netwerksites. Er is op dit moment geen enkele strafrechtelijke reden waarom de politie geen gebruik zou mogen maken van dergelijke voor iedereen toegankelijke bronnen. In het strafrecht geldt nu eenmaal niet de bestuursrechtelijke gedachte dat de overheid slechts mag doen waartoe ze een bevoegdheid heeft gekregen. Dat is slechts anders als er bijvoorbeeld inbreuk wordt gemaakt op een mensenrecht, aangezien dergelijke inbreuken een wettelijke rechtvaardiging vergen. Maar op het eerste gezicht lijkt het erop dat iemand die iets op Hyves of Facebook zet daarmee zijn/haar recht op privacy dienaangaande opgeeft waar het de openbaarmaking van het betreffende gegeven betreft (waarmee nog niet gezegd is dat het deze sociale netwerksites daarmee vrijstaat alle verwerkingen te verrichten die hun goeddunkt).

De resultaten van het opsporingsonderzoek worden opgeslagen. Technisch is het uiteraard mogelijk om het gebruik van deze gegevens niet te beperken tot het specifieke onderzoek waarvoor ze zijn vergaard, maar ze in later onderzoek opnieuw te gebruiken. Het denken over de opslag en de verwerking van gegevens bij de Nederlandse politie staat evenwel nog in de kinderschoenen. Wel zijn er tal van wettelijke regels dienaangaande.

In 2004 werd vastgesteld dat de informatiestromen binnen de politie in omvang en aantal sterk toenemen, maar de informatie werd ook toen nog gescheiden opgeslagen, waardoor landelijk, regionaal en lokaal inzicht in de voorhanden kennis gebrekkig was (Inspectie Openbare Orde en Veiligheid 2004). In het Nationaal Intelligence Model (NIM) is inmiddels als doel gesteld dat alle korpsen uiterlijk eind 2012 informatiegestuurd werken, maar het ziet ernaar uit dat nog steeds niet alle agenten voldoende 'informatiebewustzijn' hebben (Inspectie Openbare Orde en Veiligheid 2008). Toch lijkt dit een kwestie van tijd. De structuur begint zo langzamerhand te komen met diverse databases en zoeksystemen met namen als Blueview, BPS, Genesys, HKS, BVO, VROS die voor het beter hanteren van de gegevens gebruikt zullen worden.

5.3.1 OPSLAG EN VERWERKING VAN POLITIE- EN JUSTITIEGEGEVENS: WETGEVING

De belangrijkste wetgeving in het justitieel domein zijn de Wet politiegegevens (per 1-1-2008) en de Wet justitiële en strafvorderlijke gegevens (Wjg, 2002 en gewijzigd per 2004).[17] Deze wetgeving is dus speciaal ten opzichte van de Wet

bescherming persoonsgegevens. Ze is sterk beïnvloed door het gedachtegoed van de EG-Privacyrichtlijnen uit 1995, 2002 en 2006, en door de opvattingen van het Europese Hof voor de Rechten van de Mens.

Deze wetten zijn extreem fijnmazig en kennen een overvloed aan administratieve verplichtingen. Dat draagt eraan bij dat slechts superspecialisten de weg erin weten te vinden. Ongetwijfeld geldt voor dit regelstelsel hetzelfde als bleek bij een evaluatie van de Wet bescherming persoonsgegevens. Het is wetgeving die in de rechtspraktijk nog niet erg leeft, betrekkelijk lastig hanteerbaar wordt geacht en ten aanzien waarvan de kennis in den breedte ook niet overhoudt (Winter et al. 2008).

In de kern is het wettelijk stelsel opgebouwd om de opslag, de verwerking en het gebruik van gegevens in de strafrechtsketen van de nodige waarborgen te voorzien. De Wet politiegegevens (Wpol) kent een systeem van autorisatie, interne controle en onder omstandigheden instemming van het OM en toezicht door het College bescherming persoonsgegevens (CPB) op wat er bijvoorbeeld door Criminele Inlichtingen Eenheden wordt opgeslagen. Het systeem kent verschillende vormen van autorisatie al naar gelang het concrete doel van de opslag en als gevolg daarvan bestaan diverse registers met verschillende doelen naast elkaar. Naast de uitvoering van de dagelijkse politietaak (art. 8 Wpol; meldingen, noodhulp, kleine diefstallen en dergelijke) is er de verwerking ten behoeve van een concreet opsporingsonderzoek (art. 9 Wpol), de verwerking om beter inzicht te krijgen in de betrokkenheid van personen bij zware criminaliteit – themaverwerking, CIE- en RID-verwerking (art. 10 Wpol) , de informantenregisters (art. 12 Wpol) en de ondersteunende verwerking ten aanzien van specialistische onderwerpen of verschillende meldingen ten aanzien van een persoon (art. 13 Wpol). Gevolg van deze differentiatie is bijvoorbeeld dat er een speciale regeling is om een gegeven dat eerst in een register voor een concreet opsporingsonderzoek is opgenomen, nadien te verplaatsen naar het register zware criminaliteit.

De ondoorzichtigheid wordt versterkt doordat de Wpol de term 'verwerken' zowel gebruikt voor het verzamelen, het vastleggen, het wijzigen, het opvragen, het raadplegen, het doorzenden, het met elkaar in verband brengen als het vernietigen (en heel veel meer werkwoorden) van gegevens. Het gevolg is dat bijvoorbeeld zowel voor het raadplegen door een agent als voor het verstrekken aan een schoolhoofd van een politiegegeven voldaan moet zijn aan het systeem van autorisaties, waarbij verschillende eisen aan het ene en het andere geval worden gesteld. Zowel het vullen van nationale systemen als het raadplegen ervan spreekt niet altijd vanzelf. Zo bleek in de Schiedammer parkmoord (een zaak waarin de betreffende politieambtenaren heel veel energie staken) dat het zogenaamde systeem VICLAS – bedoeld om verbanden tussen zedendelicten te kunnen leggen – niet was gevuld met het zedendelict dat de werkelijke dader had gepleegd voor deze moord, hoewel hij daarvoor was aangehouden en veroordeeld (Posthumus 2005: 67-68).

Anderzijds is het systeem van de Meldingen Ongebruikelijke Transacties (MOT) van de Financial Intelligence Unit (FIU) eigenlijk een goudmijn. Het lukt de beheerders van dat systeem echter moeilijk om MOT-informatie door de opsporing te laten gebruiken: slechts terzake van 9600 op het totaal van 82.454 doorgemelde verdachte transacties is in 2008 een proces-verbaal of een rapport opgemaakt (FIU jaaroverzicht 2008: 32, 93 en 141).

Politiegegevens worden volgens de wet rechtstreeks aan het OM verstrekt (art. 16 jo 23 Wpol) – en enkele andere opsporingsambtenaren, maar niet aan de rechter – terwijl justitiële gegevens aan de rechter en aan de minister worden verstrekt (art. 8 Wjg). Maar vervolgens wordt in de Wpol en in de Wjg de sluis opengezet via een soort blanketregeling: aan derden kan ook structureel of incidenteel worden verstrekt.[18] We hebben het dan wat de politiegegevens betreft onder veel meer over de reclassering, Bureau Jeugdzorg, de kinderbescherming, de woningbouwverenigingen, slachtoffers die willen procederen, de IND, BIBOB, AFM, luchtvaartmaatschappijen, de sociale dienst en buitenlandse autoriteiten. De politie en het OM werken steeds meer samen met derden in de sfeer van preventie en nazorg en de Wet politiegegevens staat dan niet in de weg aan de zogeheten programmatische aanpak – de brede aanpak van misdaad en overlast, ook met behulp van bestuursrechtelijk optreden.[19] Met justitiële gegevens wordt iets terughoudender omgegaan, maar hier kan worden gedacht aan het zogenaamde cliënt-volgsysteem, de reclassering, de kinderbescherming, terwijl de minister ook van de gegevens kan kennisnemen bij het afgeven van verklaringen omtrent het gedrag. Voor zover voor het nemen van in artikel 1:3 Awb bedoelde besluiten justitiële gegevens noodzakelijk zijn, worden ze desgevraagd verstrekt aan de betreffende personen of colleges.

Uiteindelijk zal altijd rekening moeten worden gehouden met de mogelijkheid van een output van niet-accurate gegevens ondanks het gedetailleerde systeem van autorisatie bij opslag en verwerking. De gegevens kunnen in eerste instantie al niet accuraat zijn geweest op het moment van invoeren, ze kunnen tijdens de opslag onterecht zijn gemanipuleerd (door hackers of onderhoudspersoneel die om wat voor redenen dan ook daarbij belang hebben), maar ze kunnen inmiddels ook verouderd (achterhaald) zijn. Bij uitstek ten aanzien van gegevens die aan derden zijn doorgegeven bestaat het risico dat ze onvoldoende worden bijgehouden.

5.3.2 KENNISNEMING, VERBETERING EN VERWIJDERING VAN POLITIE- EN JUSTITIEGEGEVENS

De wet kent de mogelijkheid om betrokkenen enige controle te geven op hetgeen omtrent henzelf is opgeslagen in de strafrechtsketen. Daartoe bestaat een recht van kennisneming (in de Wpol) en een recht van kennisneming en verbetering (in de Wjg). Verzoeken daartoe worden in de praktijk echter vrijwel altijd afgewezen

(Kielman 2010: 157; Schreuders & Van der Wel 2004: 153 e.v.). Let wel: het gaat dan natuurlijk niet om stukken die in een strafdossier zijn opgenomen en waarvan de verdachte kan kennisnemen. Het gaat om stukken die nooit in een strafdossier terechtkomen (journaals, aantekeningen van interviews met mensen die niets bruikbaars te vertellen hadden, processen-verbaal van activiteiten die geen resultaat opleverden e.d.), om stukken die in het dossier van een ander zitten en bovenal om gegevens zoals opgenomen in registers.

Dat gegevens doorgaans niet worden verstrekt is ook niet verwonderlijk als we lezen dat volgens art. 27 Wpol een verzoek kan worden afgewezen als dat noodzakelijk is in het belang van: a) de goede uitvoering van de politietaak, b) de gewichtige belangen van derden en c) de veiligheid van de staat. In artikel 39l Wjg worden in vergelijkbare zin genoemd: a) de veiligheid van de staat, b) het voorkomen, opsporen en vervolgen van strafbare feiten, c) het toezicht op de naleving van wettelijke voorschriften (…) en d) de bescherming van de betrokkene of van de rechten en vrijheden van anderen. Op zich is het logisch dat weigering tot kennisneming bijvoorbeeld moet afstuiten op de bescherming van de anonimiteit van de oorspronkelijke bron, maar het is opmerkelijk dat de politie het kennelijk als een succes beschouwt dat men meestal bij verzoeken 'de deur dicht weet te houden'.

Het ontbreken van een werkelijk recht van kennisneming over wat is opgeslagen wordt niet gecompenseerd door de zogenaamde notificatieplicht ten aanzien van manieren van vergaren van gegevens (art. 126bb Sv). Volgens deze plicht moeten mensen worden geïnformeerd als tijdens het vergaren van gegevens door inzet van bijzondere opsporingsmethoden inbreuk op de privacy is gemaakt.[20] Let wel: vergaren is een stap eerder dan opslaan en verwerken en er worden ongetwijfeld zaken geregistreerd die niet door bijzondere methoden bekend zijn geworden. Maar vanuit het oogpunt van gegevensvergaring en -verwerking door de overheid is er een verband. In een fraai rapport over de notificatieplicht van de AIVD legt de Commissie van Toezicht uit dat notificatie door het EHRM wordt gezien als een van de middelen die kunnen bijdragen aan een geheel van daadwerkelijke en effectieve waarborgen tegen misbruik van bijzondere bevoegdheden. Ook in zaken waarin Duitsland en Bulgarije in dit verband werden veroordeeld werd erkend dat notificatie niet de langetermijndoelstellingen van het geheime bijzondere onderzoek in gevaar mag brengen. Ook mag notificatie niet de rechtmatige belangen van de inlichtingendienst in gevaar brengen zoals daar zijn de geheimhouding van bronnen, werkwijze en het actuele kennisniveau. De notificatieplicht kan volgens de commissie daarom niet zonder meer als een uit het EVRM voortvloeiende verplichting worden gezien.[21]

Deze overwegingen lijken evenzeer gelding te hebben voor de politie en lijken zelfs in hoofdlijn van toepassing voor de weigering om burgers te laten kennisnemen van wat er over hen is opgeslagen. Uitgangspunt is dat er daadwerkelijke en effectieve waarborgen moeten zijn. Het verdient aandacht dat er wel een wettelijk,

maar geen daadwerkelijk en effectief systeem is om op de hoogte te worden gebracht van de methoden die tegen een burger zijn ingezet, terwijl er ook geen reëel systeem is waaruit die burger kan vernemen wat er eigenlijk over hem is opgeslagen.

Waar het recht op kennisneming en notificatie problematisch blijken, geldt dat evenzeer voor het recht op verbetering. Ik neem het eenvoudige voorbeeld van de opslag van een sepot onder code 01 of code 02. Code 01 betekent dat iemand *achteraf* ten onrechte als verdachte blijkt te zijn aangemerkt als gevolg van (administratieve) fouten van politie of parket, dan wel omdat op het moment van inboeking nog niet vaststond wie als verdachte moest worden beschouwd, dan wel omdat later blijkt dat de betreffende persoon ten onrechte als verdacht is aangemerkt, bijvoorbeeld na valse aangifte. Onder code 02 valt onvoldoende of niet overtuigend bewijs. De ervaring leert dat in het merendeel van de gevallen vrijwel automatisch code 02 (gebrek aan bewijs) wordt gegeven in plaats van code 01 (ten onrechte verdacht). Dat laatste gebeurt alleen als de onschuld is gebleken, hetgeen – volgens politie en justitie – niet het geval is door de enkele omstandigheid dat geen bewijs is aangetroffen. Terecht legt de Nationale Ombudsman de lat hoger door te toetsen of er in het onderzoek feiten of omstandigheden zijn gebleken op grond waarvan het redelijk vermoeden van schuld in de zin van artikel 27 lid 1 Sv is komen te vervallen.[22] Over de codering – en daarmee over de notatie in de overheidsregisters – bestaat geen beroepsgang, ook niet bij de Raad van State (ABRvs 12 maart 2008, LJN: BC6408).[23] Dat neemt niet weg dat code 02 bijvoorbeeld met het oog op het verkrijgen van bepaalde vergunningen (of met het oog op een BIBOB-advies) bezwaarlijk is en – hoewel volgens het OM niet uitgesloten – ook de kans op schadevergoeding geringer is (Hof Den Bosch 4 augustus 2009, LJN: BJ7250).

Na de kennisneming en de verbetering brengt dat ons bij de verwijdering van gegevens. Politiegegevens moeten worden verwijderd zodra ze niet langer noodzakelijk zijn voor het doel waarvoor ze zijn opgeslagen en daartoe worden ze (althans volgens de wet) elk half jaar gecontroleerd. Overigens worden ze verwijderd uiterlijk vijf jaar na de laatste verwerking, zij het dat ze daarna nog vijf jaar 'achter een schot' worden bewaard voor beperkt gebruik.

Justitiële gegevens worden na twintig jaar of na het overlijden van betrokkene verwijderd, (art. 4 Wjg). De twintig jaar is eventueel te verlengen met de duur van de onvoorwaardelijke gevangenisstraf die is opgelegd en met nog eens tien jaar als het om een zwaar delict gaat (art. 5 Wjg). Justitiële gegevens van overtredingen blijven vijf jaar bewaard.

De tijdige verwijdering van opgeslagen dagelijkse gegevens volgens de vijf-jaren eis wordt met zogenaamde multi-agenttechnieken bevorderd. Het gaat daarbij om digitale softwareagenten die complexe taken uitvoeren (Koelewijn 2009: 192-193).

Schoning vanwege het noodzakelijkheidsbeginsel is problematischer. Dat is ook wel begrijpelijk. Een belangrijke reden van de terughoudendheid met het verwijderen is dat data die zijn vergaard voor het ene doel voor een ander kunnen worden gebruikt. Een onderzoek kan bijvoorbeeld deel uitmaken van een project waaruit diverse strafzaken tegen diverse personen voortvloeien – waarbij dan bijvoorbeeld de tapgegevens die zijn opgenomen in het kader van zaak A via een tap op meneer B, ook worden gebruikt in zaak C, waarbij de machtiging om B te tappen dikwijls niet is te vinden in het dossier C, omdat deze zich bevindt in dossier A. Zo is ook te begrijpen dat – hoewel dit wordt beheerst door een totaal ander juridisch regime – in 18 procent van de gemeenten, opgenomen videobeelden van cameratoezicht langer dan zeven dagen worden bewaard (Hissel & Dekkers 2008: IV). Niettemin zijn er wel degelijk gevallen waarin gegevens *moeten* worden verwijderd, bijvoorbeeld na een vrijspraak.

Nu worden verzoeken tot verwijdering bepaald niet automatisch gehonoreerd (Hof Den Haag 24 maart 2009, LJN: BJ2459). Niettemin bestaan er juist na vrijspraak voorbeelden dat de rechter bereid is dat recht te doen effectueren. Zo werd met succes een beroep op de rechter gedaan om gegevens uit politieregisters te laten verwijderen na vrijspraken van ontucht (Rechtbank Den Bosch 25 februari 2010, LJN: BM0090), stalking (Voorzieningenrechter Rechtbank Dordrecht 24 maart 2009 LJN: BH7597) en openlijke geweldpleging (Rechtbank Rotterdam 26 januari 2010, LJN: BL4462). Dat rechterlijke interventie nodig was betekent evenwel ook dat het niet vanzelfsprekend is dat onjuiste (althans niet hard gemaakte) vermoedens uit het geheugen van de politie worden verwijderd.

Bij uitzondering heeft het juridische gevolgen als gegevens ten onrechte niet zijn geschoond. In HR 7 juli 2009, NJ 2009, 399, ging het om de foto van verdachte, die buiten zijn wil was gemaakt in een andere zaak waarvoor hij is vrijgesproken. Die foto is gebruikt ten behoeve van een fotoconfrontatie. Het Hof had – mede gelet op artikel 5a Wet politieregisters (de voorganger van de Wet politiegegevens) – niet zonder meer voorbij mogen gaan aan het verweer dat verdachtes foto niet in 'politieadministraties' had mogen worden opgenomen, althans daaruit verwijderd had moeten zijn, omdat de foto is gemaakt in het opsporingsonderzoek in een andere zaak tegen verdachte die tot vrijspraak heeft geleid.[24] Ook de hierna onder subparagraaf 5.3.3 te behandelen problematiek van het gebruik van kentekengegevens die zijn vergaard met ANPR-camera's is terug te voeren op deze redenering. Als een gefotografeerd kenteken geen 'hit' oplevert, omdat er wel wegenbelasting is betaald, zou het gegeven eigenlijk vernietigd moeten worden. In de praktijk wordt het echter op diverse manieren gebruikt voor de opsporing (of voor het ter controle op bijvoorbeeld de naleving van de Opiumwet staande houden van auto's). Een laatste voorbeeld – meer uit het justitiële dan het politiële domein – is het niet verwijderen van zogenaamde geheimhoudersgesprekken uit de strafdossiers.

Kennisneming, verbetering en verwijdering stuiten op dit moment steeds op enorme problemen en zo bezien ontbreekt deze mogelijke waarborg ten aanzien van de correctheid van door de politie aangedragen gegevens.

5.3.3 HET GEBRUIK VAN POLITIËLE EN JUSTITIËLE GEGEVENS

Er zijn op dit moment mijns inziens drie vormen van gebruik van opgeslagen gegevens in de strafrechtsketen te onderscheiden.

De eerste vorm betreft de situatie waarin een verdachte bekend is geworden (in rechercheterm: 'is geïdentificeerd') en nu bewijs tegen hem moet worden verzameld. Een voorbeeld is te ontlenen aan het gebruik van DNA-gegevens. Er is een spoor gevonden waaraan een DNA-profiel kan worden ontleend van de vermoedelijke dader. Er is een verdachte. En er wordt vergeleken of het opgeslagen DNA-profiel van het spoor een match heeft met het DNA-profiel van de verdachte. Een vergelijkbaar verhaal is te verzinnen in verband met beelden van een ANPR-camera of met telefoonlocatiegegevens. Er is een verdachte en gekeken wordt of zijn auto dan wel zijn telefoon op of omstreeks het moment van plegen in de nabijheid van de plaats delict was. In deze voorbeelden worden de opgeslagen gegevens gebruikt als belastend (of ontlastend) bewijsmateriaal.

De tweede vorm van gebruik van gegevens ziet op de identificatie van een verdachte van een gepleegd feit met behulp van de opgeslagen gegevens. Het subject dat in het bestand wordt gezocht is dan nog geen bekende verdachte. Hier is te denken aan het geval waarin een spoor is gevonden waaraan een DNA-profiel kan worden ontleend en dat profiel wordt vergeleken met alle opgeslagen persoonsprofielen in een databank. Eveneens identificerend werken de meldingen van ongebruikelijke transacties als gevolg waarvan ook verdachte meldingen naar voren komen (en daarmee de namen van te verdenken personen), en men kan natuurlijk feitelijk ook de locatiegegevens (van personen die blijkens gegevens van de telefoonmasten hun mobiel hadden aanstaan) rondom een plaats delict gebruiken om een lijst met potentiële verdachten aan te leggen. De identificatie van de verdachte door de bestandsvergelijking kan uiteindelijk onder omstandigheden als bewijsmiddel worden gebruikt en valt dan samen met de eerste vorm, maar de techniek kan in andere omstandigheden worden aangewend om bijvoorbeeld een prioritering van te controleren personen op te stellen.

Het derde gebruik van gegevens is die van grondstof voor risico-inschatting. Soms dragen niet-politiële en niet-justitiële gegevens bij aan een risico-inschatting in het justitiële domein; in andere gevallen beïnvloeden politiële en justitiële gegevens een maatschappelijke risico-inschatting. Een voorbeeld van niet-justitiële invloed is aan te treffen bij de bestrijding van jeugdcriminaliteit.

Belangrijke voorspellers van jeugdcriminaliteit (die ook meerdere oorzaken benaderen) zijn bijvoorbeeld hyperactiviteit en/of *thrill-seeking*, slechte (conflictueuze) opvoeding door de ouders, ouderlijke misdaad, gedragsproblemen op school, ganglidmaatschap en een zwakke buurtorganisatie. Belangrijke beschermende factoren zijn eerstgeborenen, 'lieve kinderen' in kleine gezinnen, vader in het huishouden, geen uitkering, geen wapens of drugs in huis, middelbare schoolonderwijs en goede ouderlijke opvoedingsstijlen (Loeber & Farrington 2001; Hawkins et al. 2000). Er bestaat een vrijwel lineair verband tussen het aantal risico's (met aftrek van het aantal protectieve factoren) en de kans op crimineel gedrag (Loeber et al. 2001: 350-351). Het is logisch dat de politie kinderen met veel risicofactoren en weinig protectieve factoren 'proactief' in de gaten houdt, maar in de praktijk valt dit niet mee. Veel professionals houden met risicofactoren rekening die hen het meest vertrouwd zijn. De schoolarts vraagt aandacht voor hyperactieve kinderen, de politie voor de bekende 'gang'-leden en de kinderbescherming voor het slechte gezin. Men realiseert zich inmiddels ook in de praktijk dat diverse factoren tezamen – en in het bijzonder factoren die onderling weinig met elkaar van doen hebben – een betere voorspellende waarde hebben. Niet voor niets wordt multidisciplinair overleg nu belangrijk gevonden.

Illustratief voor het belang van justitiële gegevens voor niet-justitiële instellingen – maar ook een mooi voorbeeld van de wederkerige werking – is de Verwijsindex Risicojongeren.[25] In het besluit terzake worden functionarissen genoemd die worden aangewezen om een jeugdige aan de verwijsindex te melden. In een eerdere versie werd daarbij vooral gedacht aan de zogenaamde Antillianencoördinator. Dat werd problematisch geacht in verband met het verbod van artikel 16 Wet bescherming persoonsgegevens om persoonsgegevens betreffende iemands ras te verwerken. Belangrijker op deze plaats was de discussie over de mogelijkheid van de politie om aan het Bureau Jeugdzorg door te geven dat de politie zich zorgen maakt over een jeugdige. Een meldingsbevoegde kan een jeugdige namelijk melden indien hij een 'redelijk vermoeden' heeft van een situatie die nu al een schadelijk of belemmerend effect heeft op de ontwikkeling van de jeugdige en/of dat de ontwikkeling van de jeugdige bedreigd wordt. Dat kan te maken hebben met materiële omstandigheden, gezondheid, opvoeding en gezinsrelaties, onderwijs en werk, alsook met de sociale omgeving buiten het gezin en de school.[26]

Door de mogelijke rol van de politie is – volgens het College bescherming persoonsgegevens – niet duidelijk hoe de doelstelling die de jeugdhulpverlening betreft zich verhoudt tot de doelstelling openbare orde. Gaat het nu in de kern om minderjarige slachtoffers of ook om het probleem van de delinquente pubers. Zijn de 5000 voor wie een taakstraf eigenlijk te licht is immers niet allemaal risicojongeren? En los daarvan: gaat het om alle 40.000 die bij de Meldpunten kindermishandeling genoemd zijn of alleen om de potentiële Savanna's en Maasmeisjes? Wat betekent het eigenlijk voor iemands verdere leven als hij op de index heeft

gestaan? Wordt iemand daardoor ook voor de politie 'gevaarlijk'? Slachtoffers zijn immers dikwijls ook potentiële daders.

Een andere illustratie van de maatschappelijke risico-inschatting op voet van gegevens uit het justitieel domein is het systeem van de Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (BIBOB). Volgens deze wet wordt een beschikking (een vergunning, subsidie of aanbesteding) geweigerd of ingetrokken, indien er ernstig gevaar bestaat dat deze mede zal worden gebruikt om strafbare feiten te plegen, of geldelijk voordeel uit strafbare feiten te benutten. Dat oordeel kan worden gebaseerd op een departementaal uitgevoerde analyse van het verleden van betrokkene – zoals onder meer blijkt uit politie- en justitiegegevens – die dan tot een advies aan de beschikkingverlener leidt. Daarbij hoeft volgens de memorie van toelichting niet onomstotelijk vast te staan dat strafbare feiten zijn gepleegd, terwijl men evenmin van de onschuldpresumptie hoeft uit te gaan (ABRvS 22 november 2006, LJN: AZ2786). Wel is zorgvuldigheid bij de totstandkoming van het advies nodig en moet de bestuursrechter oordelen of de feiten de conclusies kunnen dragen (ABRvS 27 februari 2008, LJN: BC5265). Zo zal informatie uit het register zware criminaliteit (het CIE-register) slechts in combinatie met andere feiten die in dezelfde richting wijzen voldoende grond opleveren voor eerder bedoeld ernstig vermoeden (Muijen 2008). Hoewel het in deze wet om veel meer beschikkingen en aanbestedingen gaat, zien we in de praktijk dat vooral het rijk en grote gemeenten deze wet gebruiken om via het weigeren van vergunningen horecaondernemingen (inclusief gokhallen, prostitutie-inrichtingen en coffeeshops) te kunnen afstoppen. Maar er zijn ook voorbeelden van taxibedrijven, partycentra en zelfs een biomassa verwerkend bedrijf dat wegens het verleden geen toekomst kreeg. Het kan daarbij gaan om gegevens over een relatief ver verleden (ABRvS 8 juli 2009, LJN: BJ1892, Yab Yum). BIBOB stelt met andere woorden geen paal en perk aan de gedachtelijn 'waar rook is, is vuur' en volgt de gedachtelijn *better safe than sorry*. Dergelijke niet altijd voorziene praktische consequenties die zojuist over BIBOB werden beschreven kunnen worden herhaald in verband met de verklaringen omtrent het gedrag (VOG), die individuele personen steeds vaker moeten aanbieden aan een mogelijke werkgever of een bedrijf dat een stageplaats aanbiedt. Naar verluidt gaat het om honderdduizenden VOG's per jaar. Ook daarover wordt steeds vaker geprocedeerd, zoals door de man die buschauffeur wilde worden, maar die desgevraagd geen VOG kreeg omdat hij tien jaar geleden 20 uur taakstraf had gekregen wegens het als jeugdige enkele malen feitelijke aanranden van de eerbaarheid (RvS 1 december 2010, LJN BO5695).

Het traditionele gebruik van gegevens ten behoeve van het bewijs is inmiddels aangevuld met gebruik ter identificatie van verdachten naar aanleiding van gepleegde delicten en gebruik ten behoeve van risico-inschatting.

De gedachte dat een ruwe uitkomst – al dan niet na automatische bewerking – van een gegevensonderzoek een menselijke verificatie zou vergen als de gevolgen groot zijn, is niet vastgelegd. Gelukkig vindt die verificatie in de sfeer van de opsporing wel vaak plaats: de politie zal doorgaans controleren of de vuurwapengevaarlijke X echt in de woning woont (waar hij volgens de computer zou moeten wonen) voordat de deur wordt ingetrapt. Dat is belangrijk, niet omdat het verwerkingssysteem niet goed zou werken, maar omdat sommige van de ingevoerde en verwerkte data achteraf bezien toch niet accuraat of onbetrouwbaar kunnen zijn.

5.3.4 BESTANDSVERGELIJKING EN DATAMINING

In de praktijk wordt het voornaamste gebruik van politiële en justitiële gegevens met het oog op risico-inschatting gemaakt door instellingen buiten politie en justitie – zoals de jeugdzorg en BIBOB. Dat is opmerkelijk, omdat er nieuwe technieken bestaan om aan opgeslagen gegevens tamelijk concrete voorspellingen te ontlenen.

Het is goed om eerst aan te geven waar het eigenlijk over gaat. Datamining is een notoir lastig begrip, omdat er verschillende technieken van data-analyse onder worden verstaan. Bij datamining in ruime zin gaat het om het leggen van verbanden tussen en het trekken van conclusies uit in de loop van de tijd opgeslagen gegevens (Sietsma 2006: 370-371). Grofweg kan datamining op twee verschillende manieren worden uitgevoerd. De eerste komt erop neer dat men bijvoorbeeld vijf – bijvoorbeeld door wetenschappers aangevoerde – attributen kiest waarnaar men op zoek gaat in een groot (al dan niet door koppeling tot stand gebracht) databestand: wie voldoet aan alle vijf, wie aan geen enzovoorts. Dat lijkt op de aanpak van de bestandsvergelijking die de FIU toepast als ze beoordeelt of ongebruikelijke transacties al dan niet moeten worden aangemerkt als verdachte transacties. Een bijvoorbeeld door een bank als ongebruikelijk doorgegeven transactie wordt als verdacht gekwalificeerd als de automatische vergelijking met de Verwijzingsindex Recherche Onderzoeken & Subjecten (VROS) een match oplevert. Er wordt met andere woorden gekeken of iemand zowel voorkomt op de lijst 'ongebruikelijke transacties' als op de lijst 'bekenden van de politie'.

De andere – interessantere – benadering komt erop neer dat trends, patronen of profielen – kortom statistische waarschijnlijkheden – worden gezocht in een groot databestand. Op deze manier kan een bank zien wanneer een bepaald gebruik van een creditcard of pinpas voor deze klant ongebruikelijk is en afwijkt van zijn profiel. Degene die zelden reist en normaliter kleine bedragen pint, zal worden gebeld als hij plotseling in twee dagen tijd veel geld lijkt op te nemen in Napels, Milaan en New York. De bank extrapoleert dus uit gegevens uit het verleden verwachtingen over het gedrag. De kennis die is verkregen door te kijken naar eerdere data wordt dus gebruikt om een relatie te leggen tussen nieuwe data en die

oudere data. Een stap verder gaat deze techniek als men recente gegevens van individuen met een soort *feedreader* vergelijkt met profielen die zijn aangelegd (en/of voortdurend worden aangepast) over mogelijk vergelijkbare individuen. Een voorbeeld levert het internetbedrijf amazon.com dat goede adviezen geeft over een mogelijk te kopen boek aan de hand van de zoekgeschiedenis van de klant en die van andere kopers die vergelijkbare aankopen deden.

In de sfeer van het strafrecht lijken deze ontwikkelingen iets trager te gaan dan in het particuliere bedrijfsleven. Men kampt nog met het praktische probleem dat over bepaalde data soms wel en soms niet informatie wordt gegeven, dat niet gestandaardiseerd wordt opgeslagen of dat verschillende definities worden gebruikt. Maar de eerste voorbeelden zijn er. Bekend werden Amerikaanse voorbeelden in verband met terrorismebestrijding, zoals in het programma met de veelzeggende titel *non-obvious relationship awareness* (NORA) (Baker 2008: 133-135; O'Harrow 2006: 146-148). NORA bestaat uit software die het eerst werd gebruikt in casino's. De gebruiker ziet dat Krista die als verdachte klant staat gesignaleerd hetzelfde huistelefoonnummer heeft als Tammy die solliciteert voor de functie van croupier. NORA wijst correlaties aan, hetgeen niet wegneemt dat mensen vervolgens moeten controleren of er echt iets mis is. Analysetechnieken als NORA hebben in de commerciële sector opmerkelijke resultaten gehad, maar de National Research Council (2008: 4) waarschuwt voor overspannen verwachtingen dienaangaande bijvoorbeeld met betrekking tot terreurbestrijding: "Because data of questionable quality are likely to be the norm in counterterrorism, analysts must be cognizant of their effects, especially in fused or linked databases." Een verschil tussen het bedrijfsleven en de politie is bijvoorbeeld dat de datamining van banken en internetbedrijven kan plaatsvinden in enorme gegevensbestanden, waarin niet alleen relevante subjecten zijn verwerkt maar ook anderen. In politiebestanden zijn logischerwijs niet-verdachte, gewone mensen ondervertegenwoordigd, maar daardoor kan met minder zekerheid worden beoordeeld wat bijzonder is aan de verdachten! Toch is te verwachten dat in de toekomst datamining steeds nadrukkelijker zal leiden tot gebruik in de politiële sfeer, zij het ter identificatie van mensen of organisaties die riskant zijn of om targets aan te wijzen waartegen proactief moet worden opgetreden (Guttman & Stern 2007). Daarbij kan gebruik worden gemaakt van nieuwe technieken om door combinaties van gegevens van sociale netwerken als Facebook, Twitter en Hyves met *click tracking data* automatisch de identiteit te achterhalen van bezoekers van de eigen website en meer algemeen om de identiteit van mensen uit grote datasets te halen (Narayanan & Shmatikov 2008: 111-125; Narayanan & Shmatikov 2009; Patel 2010).

De Wet politiegegevens biedt de mogelijkheid voor het geautomatiseerd vergelijken van gegevens, inclusief gegevens van onverdachte burgers (art. 11 Wpol). Of daarmee ook datamining als patroononderzoek een juridisch kader heeft is zacht gezegd betwistbaar. Inmiddels zijn er grofweg twee categorieën zaken in Neder-

land geweest. Bekend is in de eerste plaats de – niet op de WPol, maar op de Wbp gebaseerde – datamining in de zogenoemde Waterproof-zaken. Daarbij ging het om niet-politiële fraudebestrijding, waarbij de gemeente bij het waterbedrijf de verbruiksgegevens heeft opgevraagd. Vervolgens is op adressen van uitkeringsgerechtigden met een extreem hoog of laag verbruik onderzoek gedaan vanuit de gedachte dat dergelijk gebruik is te beschouwen als aanwijzing dat er meer of minder personen op dat adres verblijven dan is aangegeven. Bestuursrechters oordeelden aanvankelijk dat de gegevensverstrekking door het waterleidingbedrijf strijdig was met de Wet bescherming persoonsgegevens, maar de Centrale Raad van Beroep aanvaardde deze werkwijze (CRvB 27 april 2010, LJN: BM 3881).

Een van de eerste voorbeelden van datamining in het strafrecht (buiten de eerdergenoemde bestandsvergelijking door de Financial Intelligence Unit) is het gebruik van de zogenaamde ANPR-database – het bestand met kentekens dat tot stand komt na A(utomatic) N(umber) P(late) R(ecognition). ANPR is een methode om via boven de weg hangende of langs de weg opgestelde camera's gescande kentekens op automatische wijze te vergelijken met een verzamelbestand waarin een selectie van kentekens is opgenomen (College bescherming persoonsgegevens 2009). Eigenlijk gaat het dus ook om bestandsvergelijking. Deze vergelijking kan een hit opleveren: een signaal dat een kenteken wordt herkend. Concreet betekent dit dat gecontroleerd wordt op gestolen auto's of kentekenplaten, of op achterstallige betalingen van boetes. Het CBP gaat daarbij uit van een beeld van de computer als een efficiënt notitieblok. Ik citeer: "Geautomatiseerde gegevensvergelijking is immers vele malen sneller dan de vergelijking die een politieagent kan maken tussen de kentekens in de verkeersstroom en de kentekens in zijn notitieboekje. De zoekvraag is geen andere dan voorheen werd gesteld aan de individuele agent; in principe komen alleen de gegevens die de politie verwerkt in het kader van de uitvoering van de dagelijkse politietaak in aanmerking voor toepassing van ANPR."

Ook als de bewerking heeft plaatsgevonden – en ook als geen hit met het oog op de verkeersregelgeving is gebleken – worden de gegevens in de praktijk nog enige dagen bewaard. De opgeslagen, gefotografeerde kentekens kunnen dan – zoals in een Zwolse zaak (Hof Leeuwarden 16 juni 2010, LJN: BM8111) – worden geraadpleegd met het oog op een specifiek kenteken (namelijk van de van autodiefstallen verdachte persoon), of ze worden vergeleken met een nieuw referentiebestand – zoals de lijst met potentiële drugsverkopers in een Maastrichtse zaak (Rechtbank Maastricht 17 februari 2010, LJN: BL4080).

De Leeuwardense en Maastrichtse rechters hebben er (evenals enkele andere) voor gekozen om deze werkwijze niet toe te laten. Alleen de Rechtbank Zwolle 2 juli 2009, LJN: BJ2119 – de rechtbank in eerste aanleg in de zaak van het Leeuwardense arrest – achtte het optreden rechtmatig. In dat geval ging het om twee met naam en

toenaam bekende verdachten van diefstallen (van auto's van parkeerterreinen van autohandelaren en garages) van wie bekend was dat zij in twee bij kenteken, merk en type bekende auto's reden. Bezien werd of zij in bepaalde nachten op bepaalde plaatsen hadden gereden. Dat het Leeuwardense Hof de methode in hoger beroep afkeurde heeft wellicht te maken met het feit dat de minister heeft aangekondigd een regeling te maken. Dat is een gemiste kans. Zelfs het CBP heeft in diens richtlijnen die ruimte eigenlijk gelaten aan de politie – juist in gevallen waarin iemand daadwerkelijk verdachte is. In het Zwolse geval werd het ANPR-bestand immers gebruikt om de verkeersbewegingen van de in concreto verdachte bestuurders van twee tevoren geselecteerde auto's te achterhalen, waarmee die zaak zich principieel onderscheidt van het Maastrichtse geval waarin het ging om het controleren van een lijst met 'potentiële verdachten'.

De keuze om tot bewijsuitsluiting over te gaan is bepaald niet vanzelfsprekend. Betwijfeld kan worden of hier – om het daarvoor relevante criterium aan te halen – sprake is van schending van een belangrijk strafvorderlijk voorschrift (HR 30 maart 2004, NJ 2004: 376). Maar voor ons onderwerp nog belangrijker is waarom we die bewijsuitsluiting zouden toejuichen. Uiteraard gaat het om het recht op privacy. In het daarover handelende belangrijke arrest EHRM 4 december 2008 (S. and Marper v. UK) kwam het Hof tot een streng oordeel met het oog op de privacybescherming tegen voortdurende opname in een register vanwege het (impliciete) verband dat door opneming in het register werd gelegd met het strafrechtelijk verleden (van de andere subjecten). Zelfs waar het de op zichzelf beschouwd onbenullige registratie van vingerafdrukken betrof. Maar opname van een kenteken in een ANPR-register (met allemaal andere automobilisten) is precies in dit perspectief iets anders dan opname in het DNA-register van verdachte en veroordeelde personen. Vanwege het verband met de eerdere verdenking of veroordeling is de mate van inbreuk door onterecht voortdurende opname in het ANPR-bestand natuurlijk veel geringer dan bij gegevens die rechtstreeks verband houden met wat het EHRM noemt 'the individual's effective enjoyment of intimate or key rights'. Overigens: zelfs fouten met betrekking tot de DNA-bestanden hoeven niet tot bewijsuitsluiting te leiden (HR 27 januari 2009, NJ 2009: 86), al gebeurt dat terecht soms wel (Hof Arnhem 18 maart 2009, NJFS 2009: 100). In dit perspectief was de Maastrichtse ANPR-zaak principieel anders. Daar was immers een incriminerend referentiebestand aangelegd van mogelijke drugshandelaren, maar bestond er geen concrete verdenking tegen de mensen die – anders dan andere automobilisten – werden gecontroleerd. Zelfs in die zaak kan men de vraag stellen of bewijsuitsluiting wel op haar plaats was, maar dat is dan nog te begrijpen vanuit de in sommige gevallen door S. and Marper geëiste strenge aanpak. In dat licht is het van belang onderscheid te blijven maken tussen mensen die reeds verdacht zijn en ten aanzien van wie bij wijze van spreken 'naslag' in een register wordt gedaan en mensen die nog geen verdachte zijn, maar die worden geselecteerd op basis van hetgeen in het register over hen is opgenomen. In zekere zin lijkt dit evident, maar

het roept wel de vraag op of het dan nog wel aanvaardbaar is een lijst met niet-verdachte ex-veroordeelden ('bekenden van de politie') louter vanwege die status te vergelijken met een andere lijst. Ik kom er in subparagraaf 5.4.3 op terug.

5.4 WAAROM ZOU VERGETELHEID WENSELIJK ZIJN?

Op dit punt van het betoog aangekomen is het goed een moment te recapituleren. In paragraaf 1 is geschetst hoe het strafrecht in de risicosamenleving zich ontwikkelde met intensiever gebruik van wetenschappelijke inzichten en geavanceerd inlichtingenwerk, waarbij een en ander mogelijk werd door technologische ontwikkelingen. In paragraaf 5.2 is vervolgens naar voren gebracht dat het digitale geheugen op drie belangrijke punten afwijkt van het biologische geheugen: het is nauwkeuriger en in staat onverwachte verbanden bloot te leggen, maar het vergt specifieke beslissingen aangaande de context. In paragraaf 5.3 is aan de orde gekomen dat de regelgeving met betrekking tot politiegegevens en strafvorderlijke gegevens ingewikkeld is. Het is niet zo dat een rechtssubject de facto het recht heeft op de hoogte te geraken van wat over hem is opgeslagen en het is bepaald niet zeker dat de politie onjuiste gegevens verwijdert, ondanks het feit dat in beginsel de wettelijke plicht daartoe lijkt te bestaan. Die gegevens kunnen zowel voor het bewijs, als voor de identificatie van verdachten als voor risicotaxatie worden gebruikt en het ziet er – ondanks aarzelingen in de jurisprudentie – naar uit dat ook datamining in die gegevens steeds belangrijker zal worden.

Zowel vanuit een maatschappelijk als vanuit een individueel gezichtspunt is deze stand van zaken niet ideaal. Er is geleidelijk aan feitelijk van alles met betrekking tot de gegevensverwerking veranderd. Het is evident dat men er – zoals meneer K. uit de proloog – enorm door benadeeld kan worden als de opgeslagen gegevens niet accuraat zijn of verkeerd worden geïnterpreteerd bij gebrek aan kennis van de relevante context. Betekent dit nu dat de overheid maar niets moet bewaren en dat burgers een volledig recht op vergetelheid zouden moeten hebben? Natuurlijk niet. Zinvolle suggesties voor verbetering vergen evenwel de introductie van een begripsmatig onderscheid. Dat onderscheid heeft te maken met het verschil tussen de manier waarop mensen zich van oudsher een herinnering vormen van gebeurtenissen die in de maatschappij plaatsvinden en de manier van herinneren die bestaat in de administratieve rationaliteit van de overheid.

5.4.1 EEN FUNDAMENTEEL ANDERE HERINNERING: OVERHEID EN SAMENLEVING

Het onderscheid tussen overheid en maatschappij (of *civil society)* lijkt door hun verregaande verwevenheid in de vroege eenentwintigste eeuw welhaast vergeten. Toch is het zinvol het onderscheid voor ogen te blijven houden. De civil society is dan "het geheel van dynamische netwerken van onderling verbonden niet-gouvernementele instellingen" (Keane 1998). Het gaat om die netwerken waarbinnen een

individu zich gebonden weet, zoals het gezin, de wijk, een club of een kerkgemeenschap. Het gaat om netwerken waarin of met behulp waarvan een individu zich ontwikkelt, zoals de school, de media, *high* en *low culture*. En het gaat om netwerken (waarbinnen) een individu zijn hoogstpersoonlijke identiteit ontwikkelt die te maken heeft met zijn etnische groep, zijn professie of zijn leefstijl. Het lijdt geen twijfel dat deze netwerken in de loop van de tijd zijn veranderd, maar het verschil tussen staat en samenleving bestaat nog steeds. Dat verschil gaat in de kern gepaard met verschillende manieren waarop mensen zich tot elkaar verhouden. Die verschillende relatievorming werkt op haar beurt door in de verschillende eisen die aan de herinnering worden gesteld. We zullen zien dat het digitale geheugen beter past bij de administratieve rationaliteit van de overheid, terwijl het biologische geheugen kenmerken heeft die belangrijk waren in het maatschappelijk leven tot nu toe. Maar laat ik niet op de zaken vooruitlopen.

Avishai Margalit onderscheidt in *The Ethics of Memory* (Margalit 2002) vette en magere relaties (zie ook Williams 1985). De vette relaties zijn de relaties binnen de burgerlijke samenleving. Ze zijn gebaseerd op kenmerken als ouder, vriend, club- of landgenoot – op een gedeeld verleden en verweven met gezamenlijke (eerstehands) herinnering. In die vette relaties wordt gestreefd naar cohesie en vertrouwen. Dat streven wordt gevoed door onze identiteit – dat wil zeggen door datgene dat wij delen met anderen. Identiteit is het verhaal waar ik aan deelneem, schrijft Jonathan Sacks (Sacks 2007: 116). Tegenwoordig zijn dat wel verhalen in veelvoud. Iemand kan immers zowel moeder van Aicha, advocaat in Nijmegen als frequent bezoeker van de Abibakr moskee zijn. Terwijl anderen ons in een specifieke context labelen met één identiteit, moeten we zelf gegeven onze veelheid aan identiteiten het relatieve gewicht toekennen van onze diverse associaties in een specifieke context (Sen 2006: XIII). Sterker nog: die identiteiten willen wij tegenwoordig (vermoedelijk meer dan bijvoorbeeld in de jaren vijftig van de vorige eeuw) soms in die zin graag scherp gescheiden houden. Met de kinderen gedeelde herinneringen willen we niet met onze cliënt of met elk van onze geloofsgenoten delen. Aan incidentele gebeurtenissen schrijven we in onze herinnering betekenis toe door de vette context, terwijl we aan veel details voorbijgaan: soms kiezen we er zelfs bewust voor te vergeten en vergeven. We maken verschil tussen anderen, niet alleen al naar gelang de context maar ook binnen een specifieke context. In de burgerlijke samenleving onderscheidt de leraar immers de 5 van de 7 van de 9; de sporter die wint onderscheidt zich van degene die na hem kwam; en zelfs in het café is de een populairder dan de ander. Zo staat hier het woord 'mens' of 'persoon' of 'individu' voor een prestatie – iets wat is bereikt en waardoor men zich onderscheidt (Margalit 2002: 46).

Magere relaties zijn anders. Ze zijn gebaseerd op individuele maar gemeenschappelijke kenmerken, bijvoorbeeld dat we Nederlandse burger zijn of vrouw of jurist. Het gaat niet om de intrinsieke waarde van de band of om de geschiedenis van de

relatie. In de moraal van de magere relaties gaat het net als in het recht eerder om algemene regels en wederzijds respect. Vanuit de magere overheidslogica bezien we separate gedragingen en prestaties en worden conflicten opgelost en liever nog voorkomen. Hier staat het woord 'mens' voor een uitgangspunt, de persoon wiens individualiteit en de daarbij horende rechten erkend moeten worden – en van wie we diens persoonlijke geschiedenis in beginsel kunnen negeren. Magere relaties zijn volgens Margalit kenmerkend voor de moderne administratieve rationaliteit. Daarbij ligt het institutionele wantrouwen van 'vertrouwen is goed, controle is beter' meer voor de hand dan het noodzakelijke vertrouwen dat de patiënt doorgaans aan de huisarts geeft (het wordt minder) en de caféhouder aan de man die hij zijn zevende biertje tapt. In de overheidslogica staat ook niet het verschil van het sportveld voorop, maar de gedachte van gelijke rechten en gelijk respect.

In de samenleving houden mensen er dus een andere basisverhouding tot elkaar op na dan in de administratieve rationaliteit van de overheid. Het verschil in onderlinge verhoudingen vanuit het perspectief van de samenleving en de overheid is met de volgende tegenstelling weer te geven: vertrouwen en onderscheid versus controle en gelijkheid (Buruma 2008: 321-330). Een illustratie is eenvoudig te geven. Dat iemand altijd zijn familie wil helpen is nauwelijks een argument bij de beoordeling van een verdachte die zich heeft gemengd in een ruzie tussen zijn broer en een derde: vanuit de overheidslogica is hij een mededader, maar vanuit de maatschappelijke logica handelt hij integer.

Bezien vanuit deze magere overheidslogica is het belangrijk dat de techniek het steeds gemakkelijker heeft gemaakt om gebeurtenissen – buiten enige vette context – te onthouden. Die vette context wordt liever buiten beschouwing gelaten. Daarmee lijkt de magere overheidslogica bijzonder compatibel met de digitale herinneringen. Daar is niets mee mis, zolang we onder ogen zien dat de traditionele vette maatschappelijke herinnering door het digitale herinneren op de achtergrond raakt. Ik zal dat toelichten aan de hand van de 'slimme' watermeter. Zo'n meter is handig voor de klant, omdat er dan geen fysieke controles meer nodig zijn en de klant evenals de waterleidingmaatschappij weet wanneer hij veel water verbruikt. Dankzij de meter is het echter ook eenvoudig om vrome moslims op te sporen. Als immers per kwartier wordt bijgehouden hoeveel water wordt verbruikt, kan men die huishoudens opzoeken waar om 05.00 uur in de morgen water wordt verbruikt – kennelijk om je te wassen. Mensen die zich op dat moment wassen bereiden zich vermoedelijk voor op het ochtendgebed, zeker als we een marginale check op de naam uitvoeren. Het simpele feit dat de betreffende bewoner ook vanwege vroege ochtenddiensten dan de kraan laat lopen is voor het labelen als 'vrome moslim' irrelevant.[27]

Met andere woorden de data-analyse heeft een 'magere' logica. Algemeen gesproken wordt er niet veel mee gezegd – even weinig als met de aanduiding 'vrome

christen' – maar in de vette maatschappelijke logica kan het leiden tot een onaangename truthiness: het risico bestaat dat de lezer van dit gegeven 'met zijn hart wel weet' wat voor type de bewoner is.

Het per definitie magere digitale gegeven onthoudt aan het subject de integriteit die hem vanuit de vette maatschappelijke relaties bezien toekomt. Daarbij blijken de onder subparagraaf 5.2.2 geformuleerde ijkpunten elk akelige vragen op te roepen: 1) Is de conclusie dat de man uit het voorbeeld een vrome moslim is, even accuraat als de waarneming van zijn watergebruik? 2) Wordt hij vervolgens gereduceerd tot iemand die louter een vrome moslim is (en wordt daarmee miskend dat mensen in de vette maatschappelijke logica meer identiteiten hebben)? 3) Als hij zichzelf al primair zou willen labelen als vrome moslim, wordt hem dan de vrijheid gegeven om zich als zodanig te labelen of ontbreekt hem die controle, omdat anderen dat voor hem doen? (Sen 2009: 236-238)

Met andere woorden: het onderscheid tussen vette en magere relaties toont aan dat de overheid haast wel voorbij moet gaan aan maatschappelijk relevante contexten. Dat kan echter afbreuk doen aan de accuratesse en zeker aan de betrouwbaarheid van de interpretatie van de gegevens. Bovendien is er een verschil met betrekking tot de controle op het beeld dat van betrokkene naar buiten komt door hemzelf. Zowel in de maatschappij als ten aanzien van de overheid is die controle niet altijd ideaal (vanuit betrokkene geredeneerd), maar doorgaans kan het subject in de samenleving ervan op de hoogte zijn hoe er over hem wordt gedacht, terwijl dat bij de overheid niet zo is. Een en ander is nog pregnanter, gegeven dat de overheid anders dan de samenleving niet uitgaat van het vertrouwen op eerdere ervaringen, maar van de noodzaak van steeds herhaalde controle. Van hun context geabstraheerde details kunnen dan reden worden voor overheidsoptreden, terwijl ze binnen de maatschappelijke verbanden begrepen of vergeten waren.

5.4.2 PRIVACY: EEN MENSENRECHT EN EEN MAATSCHAPPELIJK BEGRIP

In de beschouwing over het verschil tussen biologische en digitale herinnering bleek de kracht van de digitale herinnering gelegen in de accuratesse van hetgeen wordt teruggehaald uit het verleden. Die kracht en het daarmee gepaard gaande vertrouwen is zo groot dat in een geval van identiteitsfraude de kans bestaat dat men een slachtoffer als meneer K. niet gelooft. In de beschouwing over het verschil tussen magere en vette relaties bleek dat incorrecte conclusies uit op zich correcte herinneringen kunnen worden getrokken en dat aspecten die in de meeste van de vette relaties van betrokkene relevant zijn niet worden meegenomen. Dat onderstreept het belang van de vraag welke controle het subject moet of zou moeten hebben over hetgeen van hem wordt herinnerd. Daarmee zijn we aangekomen bij enkele belangrijke aspecten van het leerstuk van het recht op privacy.

Privacy is een weerbarstig begrip. In de literatuur over het recht op privacy wordt steevast begonnen met de aanduiding van Warren en Brandeis in hun artikel in de *Harvard Law Review* van 1890. Zij noemden dit recht (naar aanleiding van de uitvinding van de instant fotocamera en het gebruik van foto's in de pers) 'het recht om met rust gelaten te worden'. Privacy leverde voor hen – respectabele heren die leefden aan het eind van de negentiende eeuw – een sluier van geheimhouding op die essentieel was voor de menselijke waardigheid en voor de bescherming van hun reputatie (Friedman 2007: 213-216). Privacy als sfeer van immuniteit is echter, zoals D. Solove heeft beschreven, te breed, omdat elke beperking van de autonomie en elk beledigend of schadelijk optreden jegens een ander dan een inbreuk op de privacy oplevert (Solove 2008). Deze hedendaagse jurist beschouwt privacy veeleer als een groep beschermende maatregelen tegen verschillende maar met elkaar verband houdende problemen. Hij concentreert zich op het verzamelen, verwerken en verspreiden van informatie en het binnendringen en interveniëren in iemands privéleven. Die aanpak kon vanuit de overheidsbenadering van magere relaties wel eens de meest zinvolle zijn. Het is in elk geval een aanpak die verklaart hoe het komt dat het recht op privacy onder veel meer zowel het huisrecht en de bescherming van (tele)communicatie, als de opslag van persoonlijke gegevens omvat.

Maar ook vanuit de maatschappelijke benadering van vette relaties is een invalshoek te kiezen die preciezer is dan de aanpak van Warren en Brandeis. De filosoof Thomas Nagel beschouwt privacy vanuit de gedachte dat we bepaalde dingen aan het zicht willen kunnen onttrekken teneinde controle te hebben over de manier waarop we ons aan anderen presenteren (Nagel 2002). Het gaat hierbij niet alleen om het recht om ongunstige feiten over onszelf geheim te houden, aangezien we sommige dingen best met sommige anderen willen delen, maar niet met iedereen. Ik doel hier op de omstandigheid dat mensen – in de onder subparagraaf 5.4.1 genoemde terminologie – over meer identiteiten beschikken en aan meer verhalen deelnemen. Een goed voorbeeld biedt de vertrouwelijkheid van lotgenoten-patiënten, of die van lotgenoten-slachtoffers. De accurate detailgegevens over de eigen ziekte wil de lotgenoot best inbrengen in de groep en het kan zijn dat de groep in het geheel daarmee een les leert die op de website van de groep komt, maar de patiënt in kwestie zou niet willen dat dit gegeven (herkenbaar) aan derden werd doorgegeven. Het gaat dus niet louter om het idee dat informatie een soort eigendom oplevert, aangezien vaak anderen over dezelfde informatie beschikken (denk ook aan de manier van optreden tijdens het liefdesspel – gedeelde kennis, maar zonder twijfel privé).

In de benadering van Sen (2009) en Nagel (2002) die ik hier volg, gaat het bij het denken over de maatschappelijke betekenis van privacy om de autonome keuze die een aspect is van de wens te controleren welk beeld er van ons naar buiten wordt gebracht. Voor het voortbestaan van de vette relaties van de burgerlijke samenleving – en voor de identiteit die we onszelf toedichten – is dat beeld van

belang. Terughoudendheid om te vertellen dat je zo nu en dan naar pornoplaatjes kijkt, dat je je baas weerzinwekkend vindt, of kreupele gedichtjes schrijft, is in een beschaafde samenleving functioneel. Een gebrek aan controle over het moment waarop en het adressaat aan wie dit soort dingen bekend worden, leidt tot genante situaties en conflicten. Het leidt trouwens ook tot een vermindering van mogelijkheden een vertrouwensrelatie op te bouwen en tot verarming van het intieme leven (dat immers extra waarde krijgt door de exclusiviteit van hetgeen je met een ander deelt). Voor de maatschappelijke privacy is het van belang dat we verschil maken tussen wat we in de context van het ene of het andere deel van onze identiteit willen openbaren. Als niets vertrouwelijk blijft is niets schandelijk. Gebrek aan schaamte, beleefdheid en zelfbeheersing zijn de keerzijde van gebrek aan privacy. Wat er eerder was – het tegenwoordig wijdverbreide exhibitionisme of de invasies in de privacy – laat ik in het midden, maar er bestaat een relatie tussen. Als we mensen weer willen leren onderscheid te maken tussen hun sociale en hun innerlijke zelf, zullen we moeten beginnen hun een zekere mate van controle te gunnen over hetgeen ze in hun diverse 'vette' maatschappelijke relaties bekend willen maken of niet.

Waar in het magere overheidsdenken de privacydiscussie vooral lijkt te worden gevoerd vanuit het (eigenlijk achterhaalde) idee dat privacy gaat over een sfeer van immuniteit en het achterhouden van dingen die je te verbergen hebt, heeft de privacy in de maatschappij als bundeling van diverse 'vette relaties' een directe betekenis voor de kwaliteit van die relaties en de kwaliteit van het samenleven. En soms – zoals in het voorbeeld van de lotgenoten – blijkt geaggregeerde maar in vertrouwen gedeelde kennis maatschappelijk voordeel te kunnen opleveren.

5.4.3 PRIVACY EN OPGESLAGEN GEGEVENS IN HET RECHT

Dankzij de technologische ontwikkelingen is het mogelijk accurate gegevens uit het verleden terug te halen. De huidige wet- en regelgeving over de opslag en het gebruik van die gegevens bleek hiervoor ondoorzichtig (zie subpar. 5.3.1) en controle op de juistheid van hetgeen is opgeslagen bleek moeilijker te realiseren dan de wetgeving suggereert (onder subpar. 5.3.2). Niettemin wordt er steeds creatiever gebruikgemaakt van gegevensverzamelingen, waarbij het zowel gaat om (door hun context) gevoelige gegevens als heel platte gegevens en waarbij het zowel gaat om onderzoek naar verdachten als om onderzoek naar mensen die in het geheel niet verdacht zijn (subpar. 5.3.4). Die ontwikkelingen roepen ondanks het bestaan van de regelgeving terzake steeds opnieuw vragen met betrekking tot de privacy op. Het lijkt erop alsof de geldende wetgeving een belangrijk punt mist. Ik denk dat het dan gaat om hetgeen zojuist werd besproken over privacy in zijn vette maatschappelijke context en het vraagstuk van de controle over hetgeen over iemand wordt teruggehaald uit het verleden.

Voor die gedachte is een aanknopingspunt te vinden in een uitspraak van het Europese Hof voor de Rechten van de Mens van 4 december 2008 (S. and Marper v. UK). Daarin heeft het Hof uitgebreid stilgestaan bij de vraag wat allemaal onder het begrip 'private life' valt. Na diverse bekende punten te hebben genoemd schrijft het: "Article 8 protects in addition a right to personal development, and the right to establish and develop relationships with other human beings and the outside. The concept of private life moreover includes elements relating to a person's right to their image."

The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8. … The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article. The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data was efficiently protected from misuse and abuse…

Het ging in deze zaak om de opslag van vingerafdrukken, celmateriaal en DNA-profielen, maar de redengeving is van algemener belang. De bescherming in verband met automatische verwerking van gegevens in het bijzonder door de politie wordt geëist. De positie van mensen die niet zijn veroordeeld – met het oog op de onschuldpresumptie – en van kinderen vergt daarbij volgens het arrest extra aandacht.

Het Hof noemt het recht op persoonlijke ontwikkeling nadrukkelijk en terecht. Mensen veranderen onder invloed van de context waarbinnen zij verkeren. Registraties dragen het gevaar in zich dat met op zich accurate gegevens een beeld wordt geschapen van iemand dat, doordat die gegevens van de context zijn geabstraheerd, niet juist is. Of niet langer juist is. Digitale herinnering kan onrecht doen aan de groei van mensen.

Ook bij het denken in termen van privacy over het gebruik van opgeslagen gegevens is terug te grijpen op de parameters accuratesse, betrouwbaarheid en controle. Een eenvoudig voorbeeld van het belang van accuratesse is het binnenvallen van een arrestatieteam in een woning waarin de door het team te arresteren verdachte niet meer woont. Het probleem zit maatschappelijk echter nog wat dieper. Maatschappelijk verlangen we een accuraat beeld van onszelf dat niet geba-

seerd is op het verleden. Hoe droevig was het voor de conservatieve dr. Laura Schlessinger dat 23-jaar oude naaktfoto's van haar op het web verschenen (Solove 2007: 164). Toen haar vriend ze maakte, zat ze er niet mee, maar na al die jaren lag dat anders. De Nederlandse strafrechter heeft overigens in een vergelijkbaar geval een veroordeling wegens belediging en schending van het (auteursrechtelijke) portretrecht uitgesproken (Rechtbank Leeuwarden 9 april 2009, LJN: BI0666). In het traditionele, 'vette' maatschappelijk leven houden we iemands ontwikkeling door de tijd heen voor ogen. We zijn ook bereid achter bepaalde gebeurtenissen een punt te zetten en (te doen alsof we) ze vergeten. Dankzij de moderne technologie dreigt van mij evenwel een *immutable me* te worden gemaakt alsof ik mij niet ontwikkel (O'Harrow 2006: 157-189).

Een voorbeeld van contextuele betrouwbaarheid blijkt als we ons realiseren dat we in bijzondere relaties een ander beeld van onszelf toestaan dan in willekeurig andere relaties (met inbegrip van relaties met de overheid). Denken we aan een kring personen waarbinnen de deelnemers een redelijke verwachting van privacy hebben, zoals de eerdergenoemde groep lotgenoten. Een actueel voorbeeld vormen de slachtoffers van seksuele handelingen van priesters die over hun ervaringen met elkaar van gedachten wisselen. De meeste mensen zullen het misplaatst vinden de confidenties die werden meegedeeld in een slachtoffercontext zonder hun toestemming te betrekken in een opsporingsonderzoek. Maar binnen de administratieve rationaliteit van de overheid ligt dit minder voor de hand (al was het maar omdat het niet gaat om de wel erkende beperkte kring van het familieleven). Dankzij de technologie dreigen gegevensuitwisselingen die bijdragen aan het vormen van relaties met anderen in al hun gedetailleerdheid eerder (of gemakkelijker of grootschaliger) te worden doorgegeven aan anderen buiten die persoonlijke relaties.

Ten slotte is een voorbeeld van het belang van controle over het eigen beeld – naast het voorbeeld van de oude naaktfoto's – het geval dat anderen een beeld van ons scheppen door gegevens te catalogiseren en te combineren. Daarbij kan het gaan om gedragingen die normaliter niet met elkaar verbonden en anoniem zijn. Het is één ding als wordt waargenomen dat je een fles whisky koopt, maar het is vervelend als men op het werk verneemt dat je deze week reeds vijf flessen hebt aangeschaft. Hier wordt een beeld door een ander geschapen, waar je geen controle op hebt. Hoewel we natuurlijk ook in het vette maatschappelijk leven voorwerp van roddel en achterdocht kunnen zijn, is het dankzij de digitale technologieën mogelijk opgeslagen gegevens te categoriseren tot een 'wetenschappelijk verantwoord' beeld dat een meer getrouwe weergave van onszelf lijkt op te leveren dan het beeld dat we van onszelf hebben.

Deze uitwerkingen illustreren dat het juridische begrip privacy zich goed verdraagt met het verlangen dat een accuraat, contextueel betrouwbaar beeld van

ons bestaat waarbij wij greep hebben op nieuwe beelden die tot stand worden gebracht door bewerking van bestaande, opgeslagen gegevens. Met het oog op het accurate (niet verouderde) beeld en de contextuele betrouwbaarheid die wij in onze vette relaties belangrijk vinden en trouwens ook gewoonweg vanuit onze wens controle te hebben op het beeld dat van ons naar buiten komt, willen we dat bepaalde zaken vergeten worden. We willen van andere gegevens niet dat ze worden doorgegeven aan anderen voor wie ze niet bestemd zijn en dat mogelijke conclusies die uit verbanden tussen gegevens over ons bestaan zijn te trekken, niet worden getrokken. Zo vanuit het individu geredeneerd lijkt een recht op vergetelheid een mooie gedachte.

5.5 BEZWAREN TEGEN EEN RECHT OP VERGETELHEID

De op het functioneren van de biologische herinnering gestoelde gedachte dat het beter zou zijn om op individuen betrekking hebbende gegevens te vergeten, ze niet digitaal door te geven en tussen die gegevens geen verbanden te leggen, duid ik nu aan als de wenselijkheid van het recht op vergetelheid. In de vorige paragraaf zagen we de positieve kanten ervan. Nog afgezien van de persoonlijke voordelen is er immers geen enkel maatschappelijk voordeel als de uitkomsten van een risico-inschatting of proactief optreden onjuist blijken. Binding en vertrouwelijkheid binnen een bepaalde kring kan maatschappelijk voordeel opleveren – men denke aan de ervaringskennis die slachtoffers van ziekten of andere narigheid met elkaar delen als gevolg waarvan onze gemeenschappelijke kennis en inzicht dienaangaande toenemen. Tenslotte is het een maatschappelijk voordeel als mensen het besef van gêne, beleefdheid en vertrouwen individueel blijven behouden. Het idee dat mensen zelf controle hebben op hetgeen over hen wordt gedacht draagt bij aan de beschaving van de samenleving.

In Frankrijk hebben de senatoren Détraigne en Escoffier een Proposition de loi (2009-2010) ingediend aangaande het 'Droit a l'Oubli'. Het voorstel beoogt online en mobiele firma's te dwingen e-mails en sms-berichten na een bepaalde tijd of op verzoek van het betreffende individu te verwijderen. Uiteindelijk wordt beoogd te verhinderen dat toekomstige werkgevers of familieleden incriminerende gegevens van het web kunnen downloaden als men dat niet wil. Het voorstel is alleen gericht op private partijen en mist de vergetelheid van de zijde van de overheid. Het heeft bovendien in zoverre een beperkte werking dat het niet gemakkelijk grensoverschrijdend zal werken, terwijl internet natuurlijk bij uitstek grensoverschrijdend is. Maar het is een begin. Inmiddels heeft ook de Europese Commissie op 4 november 2010 aangekondigd in het kader van een strategie ter versterking van de gegevensbeschermingsregels dat "iedereen het recht heeft te worden vergeten wanneer gegevens niet langer nodig zijn of wanneer iemand zijn gegevens wil laten wissen".[28]

Toch rijst juist vanwege de concreetheid van het voorstel de vraag of er dan geen argumenten bestaan tegen zo'n recht op vergetelheid. Is het immers niet zo dat dankzij de digitale technologie massa's gegevens veel accurater kunnen worden bewaard, dat de contextuele betrouwbaarheid misschien wel een probleem is, maar dat banken en internetbedrijven juist door dubbel te checken daar wel mee hebben leren omgaan en dat we ook weer niet te sentimenteel over de controle op ons eigen beeld moeten doen?

5.5.1 BEZWAREN TEGEN VERWIJDERING DOOR DE OVERHEID ALS SYSTEEMVERANTWOORDELIJKE

De gedachte dat een recht op vergetelheid zou moeten worden ingevoerd suggereert in elk geval dat de overheid een systeemverantwoordelijkheid heeft voor wat er in de digitale wereld gebeurt. Het Franse voorstel is primair gericht op verantwoordelijkheid van de overheid voor verwijdering van individuele gegevens uit particuliere bestanden. Laten we eerst onderscheid maken tussen verwijdering op verzoek en spontane verwijdering. Dat een burger er recht op heeft dat gegevens over hem op zijn verzoek worden verwijderd, is een uitgangspunt dat me – vanuit de gedachte dat voor het recht op privacy controle essentieel is (zie subpar. 5.4.2) – wel aanspreekt. Er schuilt natuurlijk wel een probleem dat het dikwijls zo zal zijn dat meer dan één burger in dezen rechten heeft. Als een stripper en een minister samen op een website van een krant staan zal de minister de foto willen laten verwijderen, maar de stripper vindt het misschien goede reclame dat ze voor de minister heeft opgetreden. Wiens recht gaat dan voor? Het is evident dat er dan met een beroep op een belangenafweging een beslissing moet worden genomen, maar het gaat me nu om het punt dat het bij de beoordeling van de vraag wat de gegevensbeheerder (dat wil zeggen de krant) moet doen niet altijd om slechts twee belangen gaat. Met andere woorden, als we het recht op verwijdering na een verzoek daartoe als uitgangspunt nemen en de overheid een taak dienaangaande geven, zullen er nog lastige vragen rijzen, maar principieel is dat uitgangspunt helder. Terzijde: misschien is het dankzij de computer steeds bekendere woord *default* in dit verband beter dan uitgangspunt. Dat geeft beter aan dat er allerlei redenen of omstandigheden kunnen worden verzonnen waaronder de verwijdering niet plaatsvindt (zoals de op het eerste gezicht zinnige uitzonderingen met betrekking tot politieregisters; hiervoor subpar. 5.3.2), maar als zo'n uitzondering zich niet voordoet, dan moet er worden verwijderd. Dat de overheid de rechthebbende dan eventueel te hulp komt en in zoverre een taak heeft, lijkt verdedigbaar.

Of de overheid ook de verantwoordelijkheid heeft om spontane verwijdering – bijvoorbeeld zoals in het Franse voorstel na tijdsverloop – te stimuleren is een andere kwestie. Uitgangspunt van deze benadering (of liever: de default) impliceert dat een ander geen gegevens van mij mag opslaan. Ook daar zijn natuurlijk allerlei uitzonderingen op te maken – bijvoorbeeld langs de lijnen van de doelbin-

ding of voor een beperkte tijdsduur – maar de default is dat het niet mag. Het is mij niet duidelijk waarop dit uitgangspunt kan zijn gebaseerd. Het is historisch begrijpelijk als men specifieke verboden dienaangaande voorstaat ter bescherming van de reputatie van mensen, maar als algemeen uitgangspunt is een verbod om gegevens over anderen te noteren vermoedelijk gebaseerd op een te brede invulling van het begrip privacy. Ik zie dan ook niet goed waarom de overheid in beginsel een taak zou moeten hebben om er in de samenleving op aan te dringen dat lijsten met gegevens worden geschoond. Het is hooguit zo dat specifieke soorten bestanden te belangrijk zijn om zonder controle te laten voortbestaan. Laat ik het krachtigste voorbeeld nemen dat ik kan verzinnen: de ledenlijst van de vereniging van pedoseksuelen 'Martijn'. Het lijkt me afschuwelijk om ten onrechte op die lijst te staan.

Maar wat doen we, als we stellen dat de overheid de verantwoordelijkheid heeft te bewerkstelligen dat die lijst na zekere tijd wordt geschoond? Waarom zou de overheid daarin een taak hebben? Mijns inziens gaat de daarmee impliciet gegeven opvatting over systeemverantwoordelijkheid voorbij aan de relevantie van het fundamentele verschil tussen het domein van de overheid en dat van de burgerlijke samenleving. Uiteraard zijn er domeinen waar de overheid om andere redenen wel een eigen verantwoordelijkheid heeft. Het is denkbaar dat de overheid een zekere systeemverantwoordelijkheid voelt (of zal gaan voelen) voor de kwaliteit van wat op het Elektronisch Patiëntendossier wordt geplaatst. Maar dat is dan vanuit de taak om de gezondheidszorg te bevorderen en niet vanuit de verantwoordelijkheid voor wat wordt opgeslagen.

Als men met mij uitgaat van de gedachte dat de vrijheid van informatieverwerving vooropstaat en daarmee de vrijheid gegevens over anderen te verzamelen, kan men natuurlijk nog zeggen dat de overheid desalniettemin een taak toekomt, omdat er op collectieve schaal praktische bezwaren opduiken. Wie zou anders iets moeten doen aan het voortbestaan van verouderde gegevens waar niemand iets aan heeft? Dat verdedigbare standpunt suggereert wat mij betreft dat de overheid hooguit een coördinerende rol kan spelen bij verbeteringen ten aanzien van het systeem. Die rol zou gezocht kunnen worden in het faciliteren van verbetering van de technologische architectuur. We zouden immers kunnen proberen om verwijdering en/of actualisering van gegevens als het ware langs automatische weg te bevorderen. Men kan er bijvoorbeeld aan denken dat gegevens zichzelf vernietigen na een bepaalde tijd of na enkele malen kopiëren. Mayer-Schönberger (2009: 169-195) stelt voor om de default om te zetten en een expiratiedatum standaard te maken als metagegeven bij elk opgeslagen file, waarop dan uitzonderingen mogelijk zijn. Het is immers in sommige systemen heel lastig als er bepaalde gegevens automatisch verdwijnen, omdat bepaalde functies van elkaar afhangen.

Wat daar van zij, er zou gestreefd kunnen worden naar een systeem waarin aan elk bestand niet alleen een naam, maar ook een retentietijd wordt toegevoegd door de

maker. Mayer-Schönberger ziet zelf een keur aan problemen onder ogen en het is de vraag of zijn voorstel zal werken (skeptisch is Blanchette, in voorbereiding). In het kader van het tegengaan van het illegaal kopiëren van auteursrechtelijk beschermde werken (Digital Rights Management) heeft men ook aan dergelijke ideeën gedacht. Echt succesvol bleken die niet te zijn, onder meer als gevolg van de vele technische mogelijkheden om dergelijke maatregelen te omzeilen.

5.5.2 BEZWAREN TEGEN VERWIJDERING DOOR DE OVERHEID ALS GEBRUIKER

In de vorige subparagraaf stonden we stil bij de rol van de overheid met betrekking tot vergetelheid in de samenleving. De vraag naar de wenselijkheid van vergetelheid ligt wellicht anders als we niet spreken over de overheid als systeemverantwoordelijke, maar als gebruiker.

Het gaat dan dus om het voortbestaan van gegevens, waarbij de vraag is of dat voortbestaan in de relatie overheid-burger een andere moet zijn dan in relaties tussen twee of meer burgers. Zojuist beargumenteerde ik naar aanleiding van het Franse wetsvoorstel dat de introductie van het recht op vergetelheid in de maatschappij wat mij betreft te ver gaat. De vervolgvraag is of we zo'n recht ten aanzien van de overheid wel zouden willen introduceren. In het systeem van de mensenrechten is dat misschien logisch. Maar maken we door de introductie van een recht op vergetelheid de overheid dan vleugellam, terwijl we andere machtige spelers in het maatschappelijk veld ongemoeid laten?

Laten we beginnen deze problematiek te bezien vanuit de vraag wat er eigenlijk op tegen is als gegevens van een burger in een overheidsbestand zijn opgeslagen. Opnieuw is de default interessant, maar in deze context is het antwoord op de vraag wat de juiste default is lastiger dan in de maatschappelijke context. Waar we in de samenleving uitgaan van de vrijheid van burgers, zijn er rechtsdomeinen waarin men uitgaat van de gedachte dat de overheid alleen mag doen wat uitdrukkelijk is toegelaten. En zelfs als men niet van dat strenge uitgangspunt uitgaat, maar van de gedachte dat de overheid alleen inbreuk mag maken op fundamentele rechten als dat is toegelaten, zal dat in de onderhavige materie al snel betekenen dat opslag en verwerking van gegevens door de overheid (vanwege het recht op privacy; art. 8 EVRM) een wettelijke basis behoeft. Ik vind dat vreemd. In tijden waarin iedereen via de sociale netwerken de meest bizarre details over mensen bij elkaar kan sprokkelen, lijkt het mij achterhaald om dienaangaande specifieke wetgeving voor de overheid als gebruiker te verlangen. Ik heb er geen enkele twijfel over dat het voor een burger legaal is om zich via internet te informeren over alle dames met blond haar, een specifieke voorkeur aangaande films en vaardigheid in de Chinese taal. Het zou van achterhaald bestuursrechtelijk legalisme getuigen als de politie voor diezelfde activiteit een wettelijke basis nodig zou hebben. Het is dit (achterhaalde) uitgangspunt dat de geldende wetgeving zo

ondoorzichtig doet zijn. Ik vind het dus ook niet nodig dat in een wet wordt vastgelegd dat de politie – in het in het begin gegeven voorbeeld van Bert Keizer – een getuige op Hyves mag laten kijken.

Toch heeft de overheid een andere positie dan maatschappelijke 'spelers'. Het lijkt verdedigbaar dat een burger er recht op heeft dat de overheid een accuraat en zo betrouwbaar mogelijk beeld van hem/haar heeft. De informatie kan verouderd of anderszins niet (meer) accuraat zijn. Indringend is natuurlijk de bevinding van de Inspector-General van het Amerikaanse Justice Department dat 35 procent van de 68.669 terroristische 'identiteiten' van de *terrorist watchlist* van de FBI erop stonden zonder geldende terrorismeaanduiding; nader onderzoek leerde dat na het sluiten van het onderzoek ze niet van de lijst waren verwijderd (Inspector General Audit Division 2009). En de informatie kan te mager zijn, in die zin dat een factor die niet uit de bestanden naar voren komt een totaal ander beeld op de man/daad in kwestie kan werpen. Men herinnere zich de vrome moslim (subpar. 5.4.1) die misschien iets minder vroom was, maar vroeg moet opstaan voor zijn werk in de bouw.

Betekent dit dan dat de politie (of in de opsporing het Openbaar Ministerie) als gebruiker de eindverantwoordelijkheid heeft voor de juistheid van wat is opgeslagen? Ik denk dat dit te veel is gevraagd. Bedenk dat de politie in belangrijke mate wordt gevoed met beweringen en geruchten waarvan aantekening wordt gemaakt, maar waarvan de juistheid niet steeds onmiddellijk kan worden gecontroleerd en gecorrigeerd. Wel heeft de politie als gebruiker de eindverantwoordelijkheid voor het gebruik van die gegevens. Het is wellicht niet meer genoeg om – zoals nu gebeurt – te redeneren dat een melding dat iemand een pistool heeft na drie weken wordt geverifieerd door bij hem op basis van die melding een doorzoeking in zijn woning te doen (in sommige regio's wordt er overigens sneller opgetreden). Ik voel er zelf wel voor dat duidelijk wordt gemaakt welke nadere controle van de juistheid van de melding er heeft plaatsgevonden vooraleer tot zoeking werd beslist. Het door Bert Keizer gegeven voorbeeld illustreert dat we daarbij eisen mogen stellen aan de kwaliteit van de nadere controle: in dat voorbeeld was de controle of de jongen op de school die een foto op het web had geplaatst irrelevant voor de vraag of hij terecht als verdachte was aangemerkt. Ook als men mij in de wens tot aanscherping van de eisen met betrekking tot digitaal ondersteunde verdenkingen niet volgt, betekent die eindverantwoordelijkheid voor het gebruik mijns inziens dat het gebruik van verouderde, onvoldoende geverifieerde of anderzijds niet-correcte gegevens – zoals in de zaak K. – een juridisch stevig verankerde en verder dan nu gaande herstelplicht met zich meebrengt. Daarvoor is des te meer aanleiding omdat – zoals in subparagraaf 5.3.2 aan de orde kwam – het recht op kennisneming en aanpassing van hetgeen is opgeslagen niet goed werkt. Ik zou met andere woorden de nadruk van het stelsel willen verschuiven van de verantwoordelijkheden met betrekking tot de opslag naar extra verantwoordelijkheden met betrekking tot gebruik jegens een persoon.

In subparagraaf 5.3.4 gaf ik aan dat het voor de hand ligt dat er bij de opsporing meer zal worden gewerkt met datamining en bestandsvergelijking. Wat betekent het recht op vergetelheid daarvoor? Vaststaat dat we het voor de datamining – waarbij het gaat om het vinden van patronen in een groot bestand – moeilijker maken als we de bestanden verkleinen: er moeten juist veel onschuldigen in zo'n bestand zitten, zoals er veel eerlijke mensen in de bestanden van banken bijdragen aan de ontdekking – via datamining – van de kenmerken van een fraudeur. Vanuit de accuratesse van de gegevens is datamining in beginsel voordelig. Ik geef een voorbeeld. Op dit moment kan het gebeuren dat de politie een haar bekende jongen die rijdt in een voor zijn leeftijd te dure auto vanwege 'ongebruikelijk bezit' natrekt (vgl. de casus van HR 15 december 2009, LJN: BK0679). Ook een anonieme tip kan het begin zijn van zo'n actie. Men zoekt een en ander na en besluit tot doorzoeking van zijn woning op verdenking van witwassen, waarbij er wat drugs boven water komen. Een problematische werkwijze – juridisch problematisch vanuit de presumptie van onschuld, maar praktisch ook problematisch omdat op deze manier vrij baan wordt gegeven aan agenten die met iemand een appeltje te schillen hebben. Stel nu dat niet de waarneming van de individuele agent of de anonieme tip, maar de uitkomst van een statistische analyse – datamining in een reusachtig databestand waarin men naar onverwachte patronen zoekt – oplevert dat iemand ongebruikelijke transacties doet, ongebruikelijke routes rijdt enzovoorts. Er is dan in elk geval sprake van een objectieve aanleiding voor verdergaand onderzoek. Het gevaar van de bevooroordeelde agent en de valse aangifte worden dan teruggedrongen, al is de aanleiding niet langs de vertrouwde (maar subjectieve) lijnen van de verdenking beredeneerd. Datamining getuigt zo bezien van dezelfde voordelen als die de digitale herinnering ten opzichte van de biologische herinnering heeft en de administratieve rationaliteit van de bureaucratie ten opzichte van de willekeur van de individuele ambtenaar. Natuurlijk bestaat het gevaar dat ook de datamining is gebaseerd op foute gegevens (denk aan de 35 procent fout-positieve terroristische entiteiten van de FBI). Dat is een belangrijk praktisch probleem, maar geen principieel bezwaar. Het onderstreept alleen het belang van controle van de uitkomst van datamining – niet alleen vanwege vragen terzake de accuraatheid van de oorspronkelijke bestanden, maar ook omdat de uitkomsten 'mager' zijn en context ontberen.

Bij de bestandsvergelijking kunnen er wel principiële vragen rijzen. Bij die werkwijze wordt er immers niet gekeken naar willekeurig naar voren komende bijzonderheden (zoals in het geval van NORA; hiervoor subpar. 5.3.4). Hier worden van tevoren referentiebestanden aangelegd. Dat kunnen relatief onschuldige bestanden zijn. Maar wat te denken van vergelijking van de (onschuldige) kentekens die via de ANPR zijn gefilmd met (beladen) lijsten van personen die gezien hun verleden speciale politieaandacht vragen (zoals in de Maastrichtse casus in subpar. 5.3.4)? Dan betekent dit dat bepaalde groepen burgers als te controleren potentiële verdachten worden beschouwd. Dat is iets nieuws, wat erop neerkomt dat een

strafrechtelijk verleden als discriminatiegrond wordt aanvaard. Zeker, er is criminologische aanleiding om een eerdere veroordeling te beschouwen als een risicofactor; er is daarentegen een morele reden om degene die zijn straf heeft uitgezeten gelijk te behandelen als anderen teneinde hem daadwerkelijk de kans te geven een beter leven te gaan leiden. Geldt voor de ex-gedetineerde immers de presumptie van onschuld niet evenzeer als voor ieder ander? Degene die deze principiële benadering verwerpt (bijvoorbeeld met een beroep op de beweerde effectiviteit van de bestandsvergelijking) zal opmerken dat er toch nauwelijks een verschil bestaat met politiewerk dat gebaseerd is op de biologische herinnering: de wijkagent die zijn pappenheimers kent, houdt ook bepaalde lieden meer in het oog dan andere. Daar staat tegenover dat die wijkagent onmiddellijk over 'vette' informatie beschikt. Hij weet dat de ex-veroordeelde Piet nu een vrouw en een kind en werk heeft, hetgeen reden is hem enigszins anders te bekijken dan ex-veroordeelde Jan die niet beschikt over 'werk, woning of wijf'. Met andere woorden de urgentie van de principiële vraag of bepaalde vergelijkingsbestanden wel mogen worden aangelegd en/of gebruikt, is toch nog steeds op zijn plaats (en dan hoef ik niet eens naar S. and Marper te verwijzen, welk arrest aan deze gedachte steun geeft). Ik recapituleer. Het lijkt misschien bezwaarlijk om bestandsvergelijking te bemoeilijken door het recht op vergetelheid te erkennen. Maar dan rijst toch wel als zwaarwegend punt de vraag welke keuze men maakt bij het formuleren van de referentiebestanden. Het recht op vergetelheid wordt in dat soort gevallen ondersteund door het discriminatieverbod en de presumptie van onschuld. Toch is hiermee niet het laatste woord gezegd. Het probleem blijkt onmiddellijk als we bedenken of deze redenering dan niet opgaat bij de meldingen van ongebruikelijke transacties: is het eigenlijk wel juist dat een ongebruikelijke transactie als verdacht wordt bestempeld louter omdat betrokkene een bekende van de politie is?

5.6 CONCLUSIE

De belangrijkste ontwikkeling op het vlak van het strafrechtelijk beleid van de laatste twintig jaar is het denken in termen van een streven naar veiligheid en risicobeheersing. Die ontwikkeling kwam gelijk op met het 'informatiegestuurd' werken door de politie. Voortschrijdende technologie maakte opslag van en snelle naslag in zeer grote bestanden gemakkelijker. Elk van deze ontwikkelingen heeft zijn keerzijde. De risicomaatschappij heeft zijn fout-positieven, mensen die ten onrechte of overmatig voor gevaarlijk worden gehouden. Het inlichtingenwerk wordt niet meer geremd door de onmogelijkheid om gegevens te vergaren en op te slaan, wat tot een feitelijk ongebreideld vergaren en bewaren leidt. Door de technologische veranderingen is vergetelheid veranderd van een default – iets wat overblijft als je niets doet – in iets wat inspanning vergt.

Deze ontwikkelingen zijn gepaard gegaan met de komst en de verbreiding van het digitale geheugen. In het maatschappelijk leven kan de sollicitant worden gecon-

fronteerd met een uitspraak die hij drie jaar eerder op Hyves plaatste en de ex-echtgenote met intieme foto's van haarzelf die haar vriend jaren geleden heeft gemaakt. Intussen beschikt ook de overheid over een digitaal geheugen. Politie- en justitiebestanden maken het mogelijk een klasse van permanent gestigmatiseerde personen te scheppen (Friedman 2007: 265). Je hoeft echt niet veroordeeld te zijn om op grond van een analyse van bureau BIBOB geen vergunning te krijgen.

In deze beschouwing is onderzocht of de digitalisering van het geheugen een fundamenteel nieuwe situatie heeft bewerkstelligd. Het ouderwetse biologische geheugen had zijn positieve kanten. Maar het is ongetwijfeld zo dat computers veel beter in staat zijn om accuraat massa's details over separate gebeurtenissen op te slaan. Bovendien maakt een digitaal geheugen het mogelijk op grond van die authentieke details verbanden te leggen, die met het blote oog nauwelijks waarneembaar zijn.

Feit is dat steeds meer gegevens worden verwerkt, zowel buiten als binnen de overheid. In wetgeving zijn vooral de opslag en de verstrekking van de gegevens met nauwgezette administratieve verplichtingen omgeven, maar dit garandeert bepaald geen correcte output. Met betrekking tot de kennisneming en verbetering van de inhoud van bestanden door betrokkenen en het verwijderen (het schonen) van die bestanden is de juridische regeling op het eerste gezicht adequaat, maar er kan toch niet worden gezegd dat wij – zoals het Europese Hof voor de Rechten van de Mens eist – beschikken over daadwerkelijke en effectieve waarborgen tegen misbruik en fouten.

Zijn dat nu redenen om te pleiten voor de introductie van een recht op vergetelheid? Niet direct, maar de gedachte moet ook niet onmiddellijk terzijde worden gelegd. Het is van belang daarbij te bedenken dat er belangrijke verschillen bestaan tussen de vette manier waarop mensen zich in de samenleving gegevens over andere mensen herinneren en de manier waarop de overheid dat doet. Ze selecteren (dikwijls onbewust) details en kleuren deze met veronderstelde bedoelingen en de context van eerdere ervaringen en gelijktijdige gebeurtenissen. In het overheidsdenken wordt het individu niet bezien als een in een maatschappelijke context opererende uitkomst van een persoonlijke historische ontwikkeling, maar als een gelijk aan anderen te respecteren individu en diens harde gedragingen. In de maatschappij staan onderscheid en vertrouwen voorop; in de relatie tussen overheid en burger gelijkheid en controle. Het een is niet beter dan het ander, maar er is een verschil en dat verschil lijkt welhaast een echo van het verschil tussen het biologische en het digitale geheugen.

Het fundamentele verschil tussen overheid en maatschappij brengt mij ertoe terughoudend te reageren op voorstellen een daadwerkelijk recht op vergetelheid te introduceren. Zo'n recht zou erop neerkomen dat onze digitale sporen na

verloop van tijd vervagen, dat oude gegevens (vanwege het gevaar dat ze niet langer accuraat zijn) worden verwijderd en dat andere gegevens waarvan de vette context belangrijk is niet separaat kunnen worden bezien. In rechtspraak van het EHRM is erkend dat het recht op privacy ook inhoudt het recht op persoonlijke ontwikkeling en het recht om zelf greep te hebben op het imago dat men in de samenleving heeft. Zo bezien heeft men er recht op dat accurate gegevens worden opgeslagen, dat die gegevens op betrouwbare wijze worden geplaatst in de relevante context en dat men tot op zekere hoogte van wijzigingen van de opslag van die gegevens moet kunnen kennisnemen en wijzigingen moet kunnen aanbrengen. Het is logisch dat iemand zich wil beschermen tegen vervelende echo's uit het verleden, maar het is toch de vraag in hoeverre de overheid hierbij een taak heeft. Het ligt immers niet voor de hand dat een particuliere derde geen gegevens over een ander zou mogen verzamelen. In het maatschappelijk verkeer kan een detail uit het verleden wel degelijk van belang zijn. Als 'Verbrande Herman' voor de zoveelste keer problemen met justitie heeft, weten zijn kennissen nog steeds dat hij lang geleden twee mensen uit een brandend huis redde. Dat maakt hem toch anders dan de eerste de beste veelpleger, maar in de overheidslogica doet dit er niet toe en dat hoeft ook niet. Niettemin zou het raar zijn als die heldendaad zou moeten worden gewist.

Een en ander brengt me tot een niet eenvoudige conclusie. De overheid kan niet zomaar – vanuit een zekere systeemverantwoordelijkheid – verlangen dat in particuliere bestanden oude gegevens worden verwijderd (dan zou heldendom ook vergeten worden!). De overheid heeft onder omstandigheden hooguit soms een taak als aan oude gegevens gevolgen worden verbonden die schade voor de betrokkene opleveren. We kunnen dan echter niet van de overheid verlangen dat deze een systeemverantwoordelijkheid aan zich trekt om de accuratesse en betrouwbaarheid van de gegevens te bewaken. Als de overheid al een verdergaande systeemverantwoordelijkheid op dit vlak heeft, dan zou deze erin schuilen dat zij burgers zou moeten faciliteren bij het uitoefenen van controle op wat anderen over hen hebben opgeslagen.

Voor wat betreft de overheid als gebruiker van gegevens is het mijns inziens noodzakelijk om de uitgangspunten van de gegevensbescherming van dit moment te heroverwegen. Het feit dat de overheid gebruikmaakt van gegevens is zo vanzelfsprekend dat een deel van de wetgeving dienaangaande overbodig is. De overheid dreigt in de huidige juridische situatie op achterstand te komen ten opzichte van het bedrijfsleven dat terecht allerlei ruime bewerkingsmogelijkheden heeft. Ook doelbinding en beperking van retentietijd spreken niet vanzelf, als men uitgaat van het standpunt dat het verzamelen van gegevens toelaatbaar is.

Dat betekent niet dat ik een ultra-libertair standpunt hanteer. Punt is dat de regulering van opslag en verwerking van gegevens mijns inziens van minder belang

zijn dan de regulering van het handelen *of line* dat is gebaseerd op digitale gegevens. Bij een inval in een woning op grond van een virtueel beeld van verdachte is de strafrechter minder geïnteresseerd in de vraag of het virtuele beeld wel mocht worden samengesteld dan of het klopte. De overheid dient wat mij betreft te worden aangesproken op de accuratesse van gegevens die reële gevolgen hadden. Er moeten daarom nadere eisen worden gesteld aan de mate van verificatie. Om met Slavoj Zizek in een documentaire uit 2004 te spreken: *Virtual reality is not the problem, but the reality of the virtual.*

Het gaat trouwens niet alleen om de accuratesse van de feiten, al is dat in de administratieve rationaliteit van de overheid wel het belangrijkste criterium. De overheid zal zich soms rekenschap moeten geven van de per definitie 'magere' aard van digitale gegevens en de vraag stellen of er nog andere relevante gegevens zijn die de harde, accurate feiten vanuit maatschappelijk oogpunt in een ander licht plaatsen. Juist ten aanzien van oude gegevens dient de overheid bij gebruik van die gegevens te beseffen dat de in maatschappelijke context – vanwege het belang van vertrouwen – vaak eerder voor betrokkene gunstige kwesties worden meegenomen die – vanwege het belang van controle aan de hand van risicofactoren – in de administratieve overheidslogica niet relevant zijn. Toch wordt de overheid in het bijzonder geacht rekening te houden met de context bij de afwegingen van opportuniteit en juist in dat licht is wat ik hiervoor als de kwestie van betrouwbaarheid aanduidde geen kwestie ten overvloede. En ten slotte zal de overheid als gebruiker wegen moeten vinden om meer dan nu het geval is de burger enige feitelijke controle te geven door reële (in plaats van louter formele) mogelijkheden tot inzage, verbetering en verwijdering te bewerkstelligen.

Ook voor de overheid hebben de nieuwe digitale technieken – bestandsvergelijking en datamining – potentie. Die technieken vergen dat niet alleen kan worden gezocht in zeer beperkte bestanden met betrekking tot nauwkeurig aangewezen subjecten. Met andere woorden: die technieken vergen dat er ook gebruik wordt gemaakt van gegevens over evident onschuldige mensen. Dat is een prijs die we zouden moeten willen betalen. Datamining kan vormen aannemen die objectiever en minder willekeurig zijn dan de huidige politiepraktijk waar het vooroordeel van de agent of het ressentiment van de aangever een rol kunnen spelen. Daaraan wordt niet afgedaan door het feit dat de nieuwe digitale technieken nieuwe fundamentele vragen opwerpen. Denk maar aan de vraag of bij bestandsvergelijking gebruik mag worden gemaakt van een referentiebestand dat bestaat uit een lijst met vrijgelaten veroordeelden.

Het digitale geheugen en de daarmee tot wasdom komende nieuwe technieken vergen een verdere doordenking van de vraag wat het data-intensieve onderzoek betekent voor onze samenleving en dus ook voor politie- en justitiewerk. We doen er goed aan daarbij ook de uitgangspunten die in de jaren tachtig zijn geko-

zen voor de omgang met gegevens met open blik ter discussie te stellen. Een recht op vergetelheid zou ik niet willen introduceren. Maar doordenking van de mogelijkheid van zo'n recht geeft wel aan dat er reden is de overheid en andere gegevensverzamelaars de gevolgen van de digitale herinneringsarbeid te doen beseffen.

Ook elders heeft men er al voor gepleit beperkingen te stellen aan dataverzameling en oude gegevens te wissen, beperkingen te stellen aan de toegang tot data, maatregelen te nemen tegen intern misbruik, de betrokkenen te notificeren en de gelegenheid te geven tot corrigeren (Committee on Privacy in the Information Age 2007: 6-7). Zowel bij die fundamentele herbezinning als bij die mogelijke praktische zelfbeperking zal rekening moeten worden gehouden met het feit dat de digitale werkelijkheid een magere werkelijkheid is. Het is een werkelijkheid waarin anders dan in het echte maatschappelijke leven accuratesse van gegevens niet automatisch impliceert dat de gegevens nog actueel zijn, omdat ze doorgaans niet zelf zijn waargenomen, maar na massale digitale verschuivingen anoniem op een bureau belanden. Het is een werkelijkheid waarin anders dan in de maatschappelijke werkelijkheid context en ontwikkeling niet bij voorbaat gegeven zijn, maar interpretatie en verrijking door analisten vergen. En het is een werkelijkheid die als we niet opletten subjecten het gevoel geeft van het verlies van de greep op het imago dat de wereld van hen heeft. De burger die zich gesteld ziet ten overstaan van een overheid die beter dan hijzelf weet wie hij is, heeft geen behoefte meer zich in te spannen voor een goed imago. Die burger vergeet zichzelf.

EPILOOG

En wat betekent dit alles nu met het oog op de zaak van meneer K.? Natuurlijk illustreert die zaak de ernstige maatschappelijke consequenties van overheidsoptreden op grond van verkeerde digitale informatie. Maar er is wel meer over te zeggen.

De agenten die proces-verbaal opmaakten van hetgeen de identiteitsfraudeur C. meldde, hebben ongetwijfeld te goeder trouw de naam van meneer K.? genoteerd. Met het oog op de accuratesse van het handelen van opsporingsambtenaren mogen we hopen dat de Wet identiteitsvaststelling verdachten vergelijkbare toekomstige fouten zal terugdringen. Niettemin moeten we daar geen al te grote verwachtingen van hebben. In de hectiek van een concrete arrestatie is het goed mogelijk dat een (vervalste) kopie van een identiteitsbewijs van de verdachte wordt aanvaard of dat met nog minder wordt volstaan. Dat is ongetwijfeld niet de bedoeling, maar tussen norm en werkelijkheid staan soms praktische overwegingen.

Juist daarom is het goed met het oog op de betrouwbaarheid van de verbalisering door de agenten die C. arresteerden te beseffen dat er geen voorziening was die

hen extra – 'vette' – informatie gaf. Het was toen kennelijk niet mogelijk een automatisch signaal te geven dat de naam van meneer K. moest worden geassocieerd met de kans op identiteitsfraude.

Bovenal werpt de zaak van meneer K. evenwel een blik op de onmacht van een burger die geen enkele controle heeft over het virtuele beeld dat van hem bestaat.

AFKORTINGEN

ADHD	Attention Deficit Hyperactivity Disorder
AFM	Autoriteit Financiële Markten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
ANPR	Automatic Number Plate Recognition
BIBOB	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
Bjg	Besluit justitiële gegevens
Bpolg	Besluit politiegegevens
CBP	College bescherming persoonsgegevens
CIE	Criminele Inlichtingen Eenheden
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
DD	*Delikt en Delinkwent*
DNA	desoxyribo nucleic acid
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
EHRM	Europees Hof tot bescherming van de rechten van de mens en de fundamentele vrijheden
FIU	Financial Intelligence Unit
HC.R-20	The Historical-Clinical-Risk Management-20
HKT-30	historische factoren (H), klinische factoren (K) en toekomst indicatoren (T)
IND	Immigratie- en Naturalisatiedienst
MOT	Melding ongebruikelijke transacties
OJJDP	Office of Juvenile Justice and Delinquency Prevention
OM	Openbaar Ministerie
NIM	Nationaal Intelligence Model
NORA	non-obvious relationship awareness
RID	Regionale Inlichtingendienst
RUG	Rijksuniversiteit Groningen
SAVRY	Structured Assessment of Violence Risk in Youth
SCP	Sociaal en Cultureel Planbureau
TBS	terbeschikking stelling
WHO	World Health Organization
Wjg	Wet justitiële en strafvorderlijke gegevens
WMD	Weapons of Mass Destruction
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum

NOTEN

1 Voorts Radio Nederland Wereldomroep, Surinaamse zakenman krijgt na 15 jaar excuses van justitie, 25 september 2009.

2 Volgens Centraal Meldpunt Identiteitsfraude, Jaarrapportage 2009, kwamen in 2009 349 meldingen binnen waarvan er 241 te relateren waren aan een vermoeden van fraude.

3 Men zie de strafbaarheid van voorbereidingshandelingen sinds 1994 en die van samenspanning sinds 2001. Ook specifiekere bepalingen zoals het opzettelijk geven van inlichtingen tot het plegen van geweld tegen goederen worden tot stand gebracht aldus art. 141a Sr, zoals voorgesteld in w.o. 31467.

4 Betrouwbaarheid is hier gebruikt in de technische betekenis dat verschillende beoordelaars tot hetzelfde resultaat komen. Met die betrouwbaarheid is nog niets gezegd over de validiteit of de geldigheid – dat wil zeggen de vraag of de test meet wat hij moet meten en de voorspelling met behulp van het instrument correct zal zijn.

5 Lodewijks spreekt van een ratio van vals positieven in geval van hoog risico bij meisjes respectievelijk jongens van 66 procent en 32 procent bij de verder sterke SAVRY-test.

6 Kamerstukken 2007-2008, 30517, 6 en 14 en 2008-2009, 30517, 13. Het cijfer is exclusief de 1078 telefoonnummers die de AIVD onder de tap heeft en de 53 van de MIVD (TK 2009-2010, 30517, 21).

7 Over het gebruik van camera's ten behoeve van de opsporing en afluisterapparatuur (opneming vertrouwelijke communicatie) heb ik geen vergelijkbare cijfers.

8 Aldus de stand op 10 april 2010 http://www.DNAsporen.nl/. Er werden ruim 22.000 hits gemeld.

9 Bits of freedom, Nieuwsbrief 5.3 (19 oktober 2009) http://www.bof.nl/nieuwsbrief131009.txt; betrouwbaar lijkt de weergave op https://rejo.zenger.nl/focus/1253127301.php van de cijfers van jaarverslagen van het CIOT. Het rapport van de adviescommissie informatiestromen veiligheid, *Data voor daadkracht*, Den Haag 2007, blz. 48, noemde evenals het jaarverslag voor het jaar 2006 nog ongeveer 1,8 miljoen bevragingen. Dat locatiegegevens hier ook onder kunnen vallen blijkt uit HR 7 september 2004, NJ 2004, 610.

10 Voor de datering is te kiezen tussen Berners-Lee uitvinding van de hyperlink en daarmee van het algemene internet uit 1989 en de commerciële uitbating daarvan sinds 1995. Mobiele telefonie dateert van 1994 en is pas sinds 1998 in Nederland breed verspreid.

11 Mayer-Schönberger (2009) meldt dat op de in 1982 geïntroduceerde cd's een capaciteit van 650 miljoen bytes paste; op de in 1995 ingevoerde dvd zeven tot dertien keer zoveel; en op de in 2006 ingevoerde Blu-ray disks 40 tot 80 keer zoveel.

12 5 Megabytes (2 tot de 20ste bytes; 1 byte is genoeg digitale informatie voor de weer-

gave van 1 letter) vormen het verzamelde werk van Shakespeare; 1 Gigabyte (2 tot de 30ste) is genoeg voor een film van 2 uur; 15 Terabyte (2 tot de 40ste) zijn alle boeken in America's Library of Congress; 1 Petabyte (2 tot de 50ste bytes) is wat Google elk uur verwerkt. Aldus de illustratieve uitleg van K. Cukier, Data, data everywhere, *The Economist*, February 27h- March 5th, 2010.

13 Ik beperk me nu tot het zogenaamde episodische of autobiografische geheugen waarmee we gebeurtenissen opslaan en zie daarmee af van problemen met het spiergeheugen en het semantische geheugen.

14 Schacter voegt nog toe het geval dat men aan niets anders kan denken, maar dat heeft minder met vergeten te maken.

15 Kovach and Rosenstiel citeren Peter Viereck, een historicus.

16 Eerder idem, The Stovepipe, *The New Yorker*, October 27, 2003. Het ging om de rol van de Office of Special Plans met betrekking tot WMD-wapens en de betrokkenheid van al Qaeda bij het regime van Saddam. Zie inmiddels ook de Committee on Technical and Privacy Dimensions 2008, H.6.

17 Belangrijke uitwerkingen zijn te vinden in respectievelijk het Besluit politiegegevens (Bpolg) van 14 december 2007 en het Besluit justitiële gegevens (Bjg) van 25 maart 2004.

18 Art. 18-20 Wpolg en 13 Wjg staan zulks toe bij AMvB – het Bpolg en het Bjg.

19 Zie ook speech procureur-generaal Herman Bolhaar ter gelegenheid van de Toogdag Implementatie Wet Politiegegevens, 30 oktober 2008.

20 Volgens Kruisbergen en De Jong (2010: 18) wordt die plicht 'niet altijd consequent uitgevoerd'. Het College van Procureurs-Generaal dringt aan op verbetering, maar genoemde conclusie lijkt minst genomen eufemistisch.

21 Commissie van Toezicht Inlichtingen- en Veiligheidsdiensten, Toezichtsrapport 24, opgenomen in Jaarverslag 2009-2010 onder verwijzing naar EHRM 6 september 1978 (Klass), EHRM 29 juni 2006 (Weber & Saravia), EHRM 28 juni 2007 (AEIH & Ekimdzhiev).

22 Bijvoorbeeld Nationale Ombudsman, rapport 19 november 2008, nr. 2008/278 en 15 oktober 2009, nr. 2009/220.

23 Je kunt overigens wel opkomen tegen het onaannemelijke geval dat de minister niet de codering van het OM, zoals opgenomen in de Aanwijzing gebruik sepotgronden, Stcrt. 2008, nr. 19 zou hebben gevolgd. Zie echter in verband met art. 12 Sv Gerechtshof 's-Hertogenbosch 27 januari 2009, LJN: BH9911.

24 Er ligt nu een wetsontwerp om de zogenaamde herziening ten nadele mogelijk te maken. De bedoeling is onder meer dat bij levensdelicten waarop levenslang staat de mogelijkheid wordt geïntroduceerd om iemand na vrijspraak alsnog te veroordelen op grond van (nieuw) DNA-onderzoek. DNA-profielen van verdachten die nu nog na vrijspraak moeten worden verwijderd zullen dan in de DNA-bank blijven. Kamerstukken II, 2008-2009, 32044, nr 3, blz. 25-26 naar aanleiding van art. 16 Besluit DNA.

25 Zie ook Wet verwijsindex risicojongeren (Staatsblad 2010, 89), waaromtrent een advies van het College bescherming persoonsgegevens van 25 januari 2010.

26 De verwijsindex heeft een eigen website en er zijn 250 gemeenten aangesloten, maar vergt nog wel een aanpassing van de Wet op de jeugdzorg.

27 Het voorbeeld is geleverd door de Nijmeegse hoogleraar Software security and correctness , prof. dr. B. Jacobs. Zie ook Bart Jacobs, *De menselijke maat in ict*, free online book – 2007; http://www.cs.ru.nl/B.Jacobs/MM/ - ISBN978-90-9021619-5.

28 http://www.europa-nu.nl/id/vikohe4zxszd/nieuws/europese_commissie_presenteert_strategie?ctx=vht7oeqre6yp

LITERATUUR

Allen, A.L. (2008) 'Dredging up the past: lifelogging, memory and surveillance', *University of Chicago Law Review* 75.

Baker, Stephen (2008) *The numerati*, Houghton Miflin.

Bell G. and J. Gemmell (2009) *Total recall; How the e-memory revolution will change everything*, Dutton 2009, with a preface of Bill Gates.

Blanchette, J.F. (in voorbereiding) Working Paper, *Journal of the American Society of Information Science & Technology*, http://polaris.gseis.ucla.edu/blanchette/papers/trd.pdf

Buruma, Y. (2005) *De dreigingsspiraal. Onbedoelde neveneffecten van misdaadbestrijding,* Den Haag: Boom Juridische Uitgevers.

Buruma, Y. (2007) 'Het smalle pad tussen sciëntisme en kwakzalverij', *Delikt en Delinkwent* 26: 350-359.

Buruma, Y. (2008) 'Het strafrecht en de civil society', in *Migratierecht en rechtssociologie* (liber amicorum Kees Groenendijk), Wolf Legal Publishers.

Buruma, Y. (2010), 'Opvragen, bewerken en kennisnemen van gegevens voor de opsporing', *Delikt & Delinkwent* 40, 7: 923-953.

College bescherming persoonsgegevens (2009) *ANPR - De toepassing van automatische kentekenherkenning door de politie*, http://www.cbpweb.nl/Pages/pb_20100128_anpr.aspx

Committee on Privacy in the Information Age (2007) *Engaging privacy and information technology in a digital age*, National Research Council, The National Academies Press: Washington, D.C.

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals (2008) *Protecting individual privacy in the struggle against terrorists: A framework for program assessment, National Research Council.* Executive Summary on www.nap.edu (National Academy of Sciences).

Dodge, M. & R. Kitchin (2007) ''Outlines of a world coming into existence': pervasive computing and the ethics of forgetting', *Environment and Planning B: Planning and Design* 34: 431-445.

Emmerik, J.L. van (2008) 'Risicotaxatie in de forensische psychiatrie', blz. 427-475 in H.C. van Marle, P.A.M. Mevis en M.J.F. van der Wolf, *Gedragskundige rapportage in het strafrecht*, Deventer: Kluwer.

Escoffier, A.-M. & M. Yves Détraigne, *Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique,* Senat (2009-2010) no 93.

Financial Intelligence Unit-Nederland, *FIU-Jaaroverzicht 2008.*

Friedman, L.M. (2007) *Guarding life's dark secrets. Legal and social controls over reputation, propriety, and privacy*, Stanford: Stanford University Press.

Greene, Anthony J. (2010) 'Making connections; the essence of memory is linking one thought to another', *Scientific American Mind*, July/August 2010.

Guttman, M.P. & P.C. Stern (red.) (2007) *Putting people on the map*, National Research Council.
Harte, J. & M. Breukink (2010) 'Objectiviteit of schijnzekerheid?', *Tijdschrift voor Criminologie* 1: 52-72.
Hawkins, J.D. et al. (2000) 'Predictors of youth violence', *OJJDP Bulletin*, April 2000.
Hersh, S.M. (2005) 'Into the intelligence stovepipe', in idem: *Chain of command*, Penguin.
Hey, Tony, S. Tansley & K. Tolle (2009) *The fourth paradigm, data-intensive scientific discovery*, Microsoft Research 2009, http://research.microsoft.com/en-us/collaboration/fourthparadigm/contents.aspx.
Hildebrand, M. et al. (2005) *De waarde van gestructureerde risicotaxatie en van de diagnose psychopathie*, Utrecht: Expertisecentrum Forensische Psychiatrie 2005.
Hildebrandt, M. & B.J. Koops (2010) 'The challenges of ambient law and legal protection in the profiling era', *Modern Law Review* 73, 3: 428-460.
Hissel, S.C.E.M. & S. Dekkers (2008) *Evaluatie cameratoezicht op openbare plaatsen*, BZC/Regioplan.
Inspectie Openbare Orde en Veiligheid (2004) *Landelijke coördinatie en uitwisseling van politie-informatie.*
Inspectie Openbare Orde en Veiligheid, *Jaarverslag 2008.*
Inspectie voor de sanctietoepassing (2009) *De tenuitvoerlegging van de tbs-maatregel*, december 2009.
Inspector General Audit Division, *The Federal Bureau of Investigation's terrorist watchlist Nomination Practices,* Audit Report 09-25 U.S. Department of Justice May 2009.
Jacobs, Bart (2007) *De menselijke maat in ICT*, free online book – http://www.cs.ru.nl/B.Jacobs/MM/ - ISBN978-90-9021619-5.
Keane, John (1998) *Civil society: Old images*, New Visions, Polity Press.
Keizer, Bert (2010) 'Een staaltje van hedendaags politiewerk', *Trouw,* 1 mei 2010.
Kielman, H. (2010) *Politiële gegevensverwerking en privacy*, diss. Leiden.
Klerx, Peter (2008) 'Terughoudend toezicht op omvangrijke private recherche', Themanummer private veiligheidszorg, *Tijdschrift voor veiligheid* 7, 4.
Koelewijn, W.I. (2009) *Privacy en politiegegevens*, diss. Leiden.
Kruisbergen, E.W. & D. de Jong, m.m.v. R.F. Kouwenberg (2010) *Opsporen onder dekmantel*, Boom Juridische uitgevers/WODC. (Onderzoek en beleid 282).
Lazer D. et al. (2009) 'Computational social science', *Science* Vol. 323 6 February 2009: 721-723.
LeDoux, Joseph (2008) *What have you changed your mind about*, www.edge.org/q2008/q08_1.html
Lodewijks, H. (2008) *Violence risk assessment in adolescents in the Dutch juvenile justice system*, dissertatie VU.
Loeber R. & D.P. Farrington (2001) *Child delinquents: Service needs and interventions*, Sage.
Loeber, R., N.W. Slot & J.A. Sergeant (2001) *Ernstige en gewelddadige jeugddelinquentie*, Houten: Bohn Stafleu Van Loghum 2001: 350-351.

Manjoo, F. (2008) *True enough*, New Jersey: Wiley: 188-189.
Margalit, A. (2002) *The ethics of memory*, Harvard University Press.
Mayer-Schönberger, Viktor (2009) *Delete: The virtue of forgetting in the digital age*, Princeton University Press.
Mottram, R. (2007) 'Protecting the citizen in the twenty-first century: Issues and challenges', in P. Hennessy (red.) *The new protective state*, Continuum.
Muijen, P.J.D.J. (2008), 'BIBOB: harde zachtheid', *Nederlands Juristenblad* 26: 1583-1586.
Nagel, Th. (2002) *Concealment and exposure*, Oxford: Oxford University Press.
Narayanan, Arvind & Vitaly Shmatikov (2008) *Robust de-anonymization of large sparse datasets*, 2008 IEEE Symposium on Security and Privacy.
Narayanan, Arvind & Vitaly Shmatikov (2009) *De-anonymizing social networks*, 30th IEEE Symposium on Security and Privacy.
Nationale Ombudsman (2009) *Herzien Openbaar Rapport 2009/199 van 23 september 2009*.
Noije, L. van & K. Wittebrood (2009) *Overlast en verloedering ontsleuteld*, SCP.
O'Harrow, Robert (2006) *No place to hide*, Penguin.
Patel, Amit (2010) 'Cookies, supercookies and ubercookies: Stealing the identity of web visitors, « 33 Bits of Entropy', http://friendfeed.com/amitp/9d55b9b0/cookies-supercookies-and-ubercookies
Pinker, S. (2007) *The stuff of thought*, Londen: Penguin.
Posthumus, F. (2005) *Evaluatieonderzoek in de Schiedammer parkmoord*, Den Haag.
Rosenbaum, James M. (2000) 'In defense of the delete key', *The Green Bag*, Summer 2000 Vol. 3 No 4.
Sacks, J. (2007) *The Home we build together*, Londen: Continuum.
Schacter, D. (2001) *The seven sins of memory: How the mind forgets and remembers*, Boston: Houghton Mifflin Co.
Schreuders, E. & H. van der Wel (2004) *De Wet politieregisters in de praktijk*, WODC.
Sen, A. (2006) *Identity and violence*, Norton.
Sen, A. (2009) *The idea of justice*, Harvard University Press.
Sietsma, R. (2006) *Gegevensverwerking in het kader van de opsporing*, diss. Leiden.
Solove, D. (2007) *The future of reputation, gossip, rumor and privacy on the internet*, Yale University Press.
Solove, D. (2008) *Understanding privacy*, Harvard University Press.
Williams, B. (1985) *Ethics and the limits of philosophy,* Cambridge, Mass.: Harvard University Press.
Williams, B. (1993) *Shame and necessity*, University of California Press.
Williams, B. (2002) *Truth and truthfulness*, Princeton University Press.
Winter H.B. et al. (2008) *Wat niet weet, wat niet deert*, RUG/WODC.

JURISPRUDENTIE

EHRM 23 juni 1976 (Engel), NJ 1978, 224.
EHRM 4 december 2008 *(S and Marper v. UK)*, NJCM bulletin 2009 (34-4) m.n. Van der Staak: 391-406.

HR 23 maart 2010, NJ 2010, 326 m.n. Mevis.
HR 15 december 2009, LJN: BK0679.
HR 7 juli 2009, NJ 2009, 399.
HR 27 januari 2009, NJ 2009, 86.
HR 20 april 2004, LJN: AL8449.
HR 30 maart 2004, NJ 2004, 376 m.n. YB.
HR 10 oktober 2000, *NJ* 2001, 4 m.n. YB.

Hof 's-Gravenhage 6 mei 2010, LJN: BM8433.
Hof Leeuwarden 16 juni 2010, LJN: BM8111.
Hof 's-Hertogenbosch 4 augustus 2009, LJN: BJ7250.
Hof 's Gravenhage 24 maart 2009, LJN: BJ2459.
Hof Arnhem 18 maart 2009, NJFS 2009, 100.
Hof 's-Hertogenbosch 27 januari 2009, LJN: BH9911.

Rb Rotterdam 4 maart 2010, LJN: BL6649.
Rb 's-Hertogenbosch 25 februari 2010, LJN: BM0010.
Rb Den Haag 22 februari 2010, NJFS 2010, 143.
Rb Maastricht 17 februari 2010, NJFS 2010, 133, LJN: BL4080.
Rb Rotterdam 26 januari 2010, LJN: BL4462.
Rb Zwolle 2 juli 2009, NJFS 2009, 225, LJN: BJ2119.
Rb Leeuwarden 9 april 2009, LJN: BI0666.
Rb Dordrecht 24 maart 2009, LJN: BH7597.
Rb Haarlem 13 oktober 2008, LJN: BF8365.

ABRvS 8 juli 2009, LJN: BJ1892.
ABRvS 12 maart 2008, LJN: BC6408.
ABRvS 27 februari 2008, LJN: BC5265.
ABRvS 22 november 2006, LJN: AZ2786.

6 KLACHTEN OVER TOEPASSINGEN VAN INFORMATIETECHNOLOGIE: ANALYSE VAN EEN AANTAL OVERHEIDSBESTANDEN

Sunil Choenni, Erik Leertouwer en Tony Busker

6.1 INLEIDING

De projectgroep Beleid, Informatie en Technologie (BIT) van de WRR is op zoek naar de wijze waarop overheid en burgers zich tot elkaar verhouden in de nieuwe dynamiek die naar voren treedt met het voortschrijden van de informatietechnologische mogelijkheden. De focus ligt op de mogelijkheden om data te verzamelen, te verwerken en te presenteren met behulp van technologie. In het project zijn een aantal beginselen – privacy, transparantie, accountability, identiteit en identificatie, keuzevrijheid en efficiëntie en effectiviteit – onderscheiden die de relatie overheid-burger vormgeven in een informatiesamenleving. Inzicht in de relatie overheid-burger kan enerzijds verkregen worden door de rol van informatietechnologie op de beginselen te bestuderen aan de hand van domeinstudies en blackboxes. Anderzijds kan inzicht in de relatie overheid-burger verkregen worden door het in kaart brengen van *geregistreerde klachten* of *potentiële klachten* van burgers over toepassingen van informatietechnologie zélf, of over feiten waarin deze technologie een aanzienlijke rol speelt. Indien er een centraal overheidsbestand zou zijn waarin dergelijke klachten worden geregistreerd, zou het relatief eenvoudig zijn om een betrouwbare omvangschatting te maken van de klachten. Potentiële klachten zouden dan hieruit kunnen worden afgeleid op basis van trends. Helaas bestaat een dergelijk centraal overheidsbestand met klachten niet. Daarom hebben we ons gericht op de bestanden van een aantal overheidsinstanties die belast zijn met het afhandelen van klachten van burgers.

De Nationale Ombudsman en het College bescherming persoonsgegevens (CBP) hebben een lange traditie in het behandelen van klachten. Het ligt dan ook voor de hand om voor een analyse van *geregistreerde klachten* te putten uit de databases die deze organisaties onderhouden. De Nationale Ombudsman behandelt klachten over bijna alle overheidsinstanties. Het CBP behandelt klachten over de naleving en toepassing van de Wet bescherming persoonsgegevens, de Wet politiegegevens, en de Wet gemeentelijke basisadministratie. Deze klachten kunnen betrekking hebben op zowel de publieke als de private sector.

Na een korte analyse van het bestand van de Nationale Ombudsman bleek het lastig om daaruit de klachten te selecteren waarbij informatietechnologie een rol heeft gespeeld. Het bestand van de Nationale Ombudsman is een relationeel databasesysteem waarvan de verzameling waarden die de meeste velden kunnen

aannemen vooraf gedefinieerd is (Van Dijk et al. 2007). Deze vooraf gedefinieerde waarden zijn slecht te relateren aan ICT. Slechts de waarden van het veld 'trefwoord', dat een klacht beschrijft, zijn niet vooraf gedefinieerd.

Een scan van dit veld op *keywords* gerelateerd aan begrippen en toepassingen van informatietechnologie leverde te weinig op om conclusies aan te verbinden. Deels zou dit te maken kunnen hebben met het feit dat het databasesysteem in 1987 is ingevoerd bij de Ombudsman, terwijl veel ICT-begrippen en -toepassingen van veel latere datum zijn. Anders is dat bij het bestand van het CBP, dat eveneens een relationeel databasesysteem is en tien jaar later is ingevoerd dan het databasesysteem bij de Ombudsman. Hier zijn klachten ingedeeld in categorieën die te relateren zijn aan informatietechnologie, zoals internet, Radio frequency identification (RFID), direct marketing enzovoorts. Voor het CBP-bestand brengen we de klachten in kaart van burgers over toepassingen van informatietechnologie of klachten waarin informatietechnologie een aanzienlijke rol heeft gespeeld. In het vervolg duiden we deze klachten aan als ICT-gerelateerd. Ook beschrijven we de ontwikkeling van ICT-gerelateerde klachten in de tijd. Ten slotte hebben we voor de analyse van geregistreerde klachten de meldingen onderzocht die zijn opgenomen in een bestand van het Centraal Meldpunt Identiteitsfraude (CMI). In dit bestand worden onder andere meldingen geregistreerd die betrekking hebben op identiteiten van personen. Van deze meldingen onderzoeken we welk aandeel ICT-gerelateerd is. Uit onze analyse van het CBP-bestand blijkt dat ongeveer 34 procent van de klachten ICT-gerelateerd is. Uit het CMI-bestand blijkt dat 40 procent van de meldingen ICT-gerelateerd is.

Potentiële klachten hebben betrekking op onterechte registraties die in het nadeel van de burger kunnen uitpakken, maar waarover (nog) geen klacht is ingediend. Om meer inzicht te krijgen in dit fenomeen in de context van de relatie overheid-burger beschouwen we een aantal informatiesystemen op het gebied van politie en justitie. Zo bevat het HerKenningsdienst Systeem (HKS) van de politiegegevens over verdachten. Een verdachte die vrijgesproken is door de rechter dient uit het verdachtenbestand van de politie verwijderd te worden. Vanwege technische en organisatorische redenen vindt deze opschoning echter niet altijd plaats. Om inzicht te verkrijgen in de omvang van dit probleem hebben we het HKS geanalyseerd. Ook nemen we de Onderzoek- en Beleidsdatabase Justitiële Documentatie (OBJD) in ogenschouw, waarin gegevens uit de strafdossiers zijn opgenomen. We hebben voor elke verdachte in het HKS-bestand gekeken van welke delicten hij of zij verdacht wordt. Indien de verdachte voor elk delict is vrijgesproken, staat de verdachte ten onrechte in het bestand. Ook hebben we onderzocht of personen die zijn overleden nog voorkomen in het bestand. Uit de analyse van het landelijke HKS-bestand blijkt dat het ruim 1,5 miljoen verdachten bevat, waarvan 2.800 personen vrijgesproken zijn voor alle delicten waarvan zij verdacht werden, en 8.000 personen de status 'overleden' hebben.

De opbouw van de rest van dit hoofdstuk is als volgt. In paragraaf 6.2 formuleren we onze onderzoeksvragen en geven we een globale beschrijving van onze aanpak om deze vragen te beantwoorden. In paragraaf 6.3 beschrijven we de resultaten uit onze analyse van de bestanden van het CMI en het CBP. Paragraaf 6.4 beschrijft een eerste stap naar meer inzicht in potentiële klachten, en ten slotte verbinden we in paragraaf 6.5 enkele conclusies en aanbevelingen aan onze bevindingen.

6.2 ONDERZOEKSVRAGEN EN AANPAK

Om inzicht te krijgen in de rol die informatietechnologie speelt in klachten die worden geregistreerd door overheidsinstanties trachten we de volgende vragen te beantwoorden:

- Hoeveel klachten in overheidsdatabases hebben betrekking op toepassingen van informatietechnologie of feiten waarin informatietechnologie een aanzienlijke rol heeft gespeeld? Om welke typen klachten gaat het, en in welke sectoren komen deze klachten voor?
- Hoe zijn deze klachten verdeeld over de jaren?

Om inzicht te krijgen in het potentieel aan ICT-gerelateerde klachten trachten we aanvullend de volgende vragen te beantwoorden:

- Welke juridische, technische en/of organisatorische beperkingen kunnen leiden tot onvolkomenheden in overheidsregistraties die in het nadeel van de burger kunnen uitpakken?
- Hoe vaak komen deze onvolkomenheden voor?

Aanpak

Voor de analyse van geregistreerde klachten is gebruikgemaakt van uitgebreide documentatie van het CMI-bestand. Met behulp van aanvullende vragen en het handmatig scannen van een aantal dossiers is dit bestand geanalyseerd. Het CBP-bestand bestaat uit een database- en een documentmanagementsysteem. Uit het databasesysteem worden aan de hand van keywords klachten geselecteerd waarbij informatietechnologie mogelijk een rol heeft gespeeld. Vervolgens wordt uit het documentmanagementsysteem het document behorende bij een klacht gezocht en wordt semiautomatisch geverifieerd of de klacht daadwerkelijk betrekking had op informatietechnologie of feiten waarin deze technologie een rol heeft gespeeld. Dit kan aan de hand van informatie-retrievaltechnieken die geïntegreerd zijn in het systeem van het CBP. Op deze manier hebben we onderzoeksvragen 1 en 2 beantwoord.

Voor de beantwoording van onderzoeksvragen 3 en 4 is gekeken naar architectuurdefinities en literatuur over de werking van een aantal politie- en justitiebestanden, met name HKS en OBJD. Voor zover kwantitatieve analyse mogelijk bleek, is voor de beantwoording van onderzoeksvraag 4 gebruikgemaakt van *SQL-queries*.[1]

We wijzen de lezer erop dat de verkregen aantallen zoals gerapporteerd in dit hoofdstuk als schattingen dienen te worden beschouwd.

6.3 ANALYSE VAN GEREGISTREERDE KLACHTEN

In deze sectie bespreken we de resultaten van de analyse van een tweetal bestanden. Het eerste bestand is afkomstig van het CMI. Dit is een relatief klein bestand in MS ACCESS-formaat dat meldingen met betrekking tot identiteitsfraude registreert. Het bestand bestaat uit een tabel met een beperkt aantal kolommen en rijen. Helaas bevat het bestand geen directe indicatoren die aangeven of een melding te relateren is aan ICT. Derhalve moesten we de data uit het bestand combineren met een beperkte vorm van dossieronderzoek om onze onderzoeksvragen te kunnen beantwoorden. In subparagraaf 6.3.1 doen we verslag van onze werkwijze en bevindingen.

Het tweede bestand is onderdeel van het informatiesysteem CISKA van het CBP. Het onderliggende bestand van CISKA is een relationeel databasesysteem bestaande uit een verzameling van coherente tabellen. Het systeem registreert naast klachten ook informatie over allerlei andere zaken zoals wetgevende adviezen en bemiddelings- en informatieverzoeken. Voor onze analyse hebben we 2.187 klachten geselecteerd uit het systeem. Weliswaar kan ook in dit bestand niet aan de hand van een simpele query bepaald worden welke klachten te relateren zijn aan ICT, maar het bestand bevat een aantal bruikbare velden om hier achter te komen. In het bijzonder hebben we gebruikgemaakt van de velden 'hoofdrubriek', 'hoofdsector' en 'titel'. Iedere klacht wordt ingedeeld in een van de tien vooraf gedefinieerde hoofdrubrieken en een van de elf vooraf gedefinieerde hoofdsectoren. Het veld 'titel' is een vrij tekstveld en bevat een omschrijving van een klacht. Met behulp van relevante keywords hebben we dit veld semiautomatisch geanalyseerd. In paragraaf 6.3.2 doen we verslag van onze werkwijze en bevindingen met betrekking tot het CBP-bestand.

6.3.1 CMI

Op 1 december 2008 is het Centraal Meldpunt Identiteitsfraude gestart met het registreren van meldingen die betrekking hebben op identiteiten van personen. De doelstelling van het CMI is burgers, bedrijven en overheden die te maken hebben met identiteitsfraude of met een fout in de registratie van persoonsgegevens te ondersteunen en te adviseren. In principe kan iedereen een melding maken met betrekking tot identiteitsfraude en fouten in de registratie van persoonsgegevens middels een meldformulier.[2] Het CMI registreert iedere melding die binnenkomt, geleidt deze door naar de juiste instanties voor afhandeling, zoals de politie of een bedrijf, en bewaakt de voortgang.

In de registratie van het CMI wordt onderscheid gemaakt tussen informatievragen, klachten over het meldpunt, meldingen over een fout in de registratie van persoonsgegevens en meldingen van een vermoeden van fraude. In totaal gaat het om 349 meldingen in 2009. Daarvan hebben 102 betrekking op informatievragen, twee op klachten over het meldpunt, vier op vermoedelijke registratiefouten van persoonsgegevens en 241 betreffen meldingen van het vermoeden van fraude. In onze analyse hebben we ons gericht op deze laatste categorie, en proberen we te achterhalen in welk deel van de meldingen van fraudevermoeden informatietechnologie een rol heeft gespeeld.

In de database van het CMI wordt de werkwijze (voor zover bekend) geregistreerd die de fraudeurs hebben gehanteerd om de persoonsgegevens te bemachtigen teneinde fraude te kunnen plegen. Omdat het CMI-bestand een relatief klein bestand betreft, hebben we een globale indeling gehanteerd om onthullingsgevaar vanwege kleine aantallen te voorkomen. Deze globale indeling wordt weergegeven in de eerste kolom van tabel 6.1.[3]

Tabel 6.1 Aantal meldingen van vermoedens van fraude naar wijze van fraude door fraudeur

Wijze van fraude door fraudeur	Aantal	ICT-gerelateerd	Niet geclassificeerd
Elektronisch (phishing, hacking, andere cybercrime)	33	33	0
Nigeriaanse oplichting	11	11	0
Misbruik persoonlijke gegevens	29	5	0
Misbruik openbare gegevens	39	18	1
Misbruik eigen identiteit	6	0	0
Diefstal van fysieke documenten	18	0	0
Contractvervalsing	17	0	0
Posthengelen	7	0	0
Wijze van fraude niet aangegeven	81	30	1
Totaal	*241*	*97*	*2*

Om niet voor alle meldingen dossieronderzoek te hoeven doen hebben we eerst onderzocht in welke categorieën informatietechnologie per definitie wel een rol heeft gespeeld en in welke niet. Zo hebben de categorieën 'posthengelen' en 'diefstal van fysieke documenten' geen directe relatie met informatietechnologie. Derhalve kunnen we vooraf al concluderen dat de kans klein is dat ICT hierin een rol heeft gespeeld. We achten de kans eveneens klein dat ICT een rol heeft gespeeld in de categorie 'contractvervalsing'. Voor contracten is vaak een handtekening nodig. Omdat digitale handtekeningen nog maar net hun intrede beginnen te doen, zijn

we ervan uitgegaan dat dit fenomeen nog geen significante rol speelt bij contractvervalsingen.

Het tegenovergestelde geldt voor de categorieën 'elektronisch' en 'Nigeriaanse oplichting': hierbij is er een directe relatie met informatietechnologie, en derhalve concluderen we dat de meldingen in deze categorieën ICT-gerelateerd zijn.

Wanneer we bovenstaande categorieën buiten beschouwing laten, houden we 155 meldingen over, verdeeld over de categorieën 'misbruik persoonlijke gegevens', 'misbruik openbare gegevens', 'misbruik eigen identiteit' en 'wijze van fraude niet aangegeven'. Voor meldingen uit deze categorieën hebben we de dossiers handmatig gescand om exact vast te stellen in hoeveel gevallen ICT een rol heeft gespeeld. Bij de scans hebben we ons gericht op de omschrijving van de meldingen om de aard van de betreffende melding vast te stellen dan wel de melding te relateren aan ICT-toepassingen, zoals webhosting, digitaal verkrijgen van of verwerken van informatie, pintransacties, internet enzovoorts. Deze werkwijze bleek vrij effectief te zijn. De 155 meldingen konden we op twee na classificeren, dat wil zeggen dat we van 153 meldingen konden vaststellen of deze wel of niet ICT-gerelateerd zijn.

Deze resultaten zijn weergegeven in de derde en vierde kolom van tabel 6.1. Opvallend is dat geen enkele van de meldingen uit de categorie 'misbruik eigen identiteit' iets te maken heeft met ICT.

De algemene conclusie luidt dat 40 procent van de in 2009 bij het CMI binnengekomen meldingen van fraudevermoeden ICT-gerelateerd is. Bij de meeste gevallen zien we dat veelal verkregen informatie wordt gebruikt voor het frauderen, terwijl de technologie, met name internet, wordt ingezet voor het verkrijgen van relevante informatie. Bij de Nigeriaanse oplichting bijvoorbeeld wordt internet gebruikt om via e-mails informatie te ontfutselen van mensen. Vervolgens wordt de informatie gebruikt om te frauderen.

6.3.2 CBP

Het CBP-informatiesysteem bevat naast klachten ook informatie over allerlei andere zaken zoals wetgevende adviezen en bemiddelings- en informatieverzoeken. De registraties in dit systeem beginnen in 1997. Voor onze analyse hebben we ons beperkt tot de totale verzameling klachten die in het systeem voorkomen. In het systeem worden in eerste instantie alle klachten opgeslagen die binnenkomen, pas daarna wordt besloten of een klacht al dan niet door het CBP wordt behandeld. Wij telden op 17 mei 2010 2.187 klachten in de database. De klachten kunnen worden onderverdeeld in 10 hoofdrubrieken, zie tabel 6.2.

Tabel 6.2 Hoofdrubrieken CBP-bestand

Hoofdrubriek	Aantal klachten
Internet	96
Derdenverstrekking	779
Handel	291
Observatie	79
Biometrie	8
Werk	64
Identificatie	94
Risicoselectie	42
Techniek	57
Overig	676
Niet ingedeeld	1
Totaal aantal klachten	*2.187*

Met betrekking tot klachten in de hoofdrubriek 'internet' is het aannemelijk dat deze gaan over informatietechnologie dan wel dat informatietechnologie een rol speelt, terwijl voor de overige rubrieken niet direct vast te stellen is of ICT een rol heeft gespeeld. Deze rubrieken hebben we gedetailleerder bekeken. Omdat iedere hoofdrubriek is onderverdeeld in een aantal subrubrieken, hebben we gebruik gemaakt van deze subrubrieken voor verdere analyse. Zo bestaat de rubriek 'biometrie' uit de subrubrieken 'DNA-onderzoek', 'vingerafdrukken' en 'overig'.

De eerste klacht die onder de rubriek 'biometrie' werd geregistreerd, komt uit 2002 en betrof de subrubriek 'DNA-onderzoek'. De eerste klacht in de subrubriek 'vingerafdrukken' werd in 2008 geregistreerd. Omdat we ervan mogen uitgaan dat in 2008 en daarna vingerafdrukken digitaal worden opgeslagen en met ICT-technieken worden verwerkt, classificeren we de klachten onder deze subrubriek als ICT-gerelateerd. Het resultaat is immers sterk afhankelijk van de ingezette ICT-middelen, zoals resolutie en matchingalgoritmen die vingerafdrukken met elkaar vergelijken.

Omdat er maar twee klachten onder de subrubriek 'vingerafdrukken' geclassificeerd zijn, hebben we aan de hand van de klachten getoetst of onze redenering voor deze gevallen klopte. Dit was het geval. Een soortgelijke redenering zou opgezet kunnen worden voor 'DNA-onderzoek'. Immers, ook daar zijn resultaten sterk afhankelijk van de ICT-technieken die gebruikt worden. Nadere toetsing van de vijf klachten in deze subrubriek had echter als resultaat dat 2 van de klachten te

Tabel 6.3 Subrubrieken van elke hoofdrubriek

Hoofdrubriek	Subrubriek	Aantal	ICT-gerelateerd
(leeg)	(leeg)	1	0
Werk	Overig	53	10
Werk	Screening	10	1
Werk	Volgsystemen	1	0
Biometrie	DNA-onderzoek	5	2
Biometrie	Overig	1	1
Biometrie	Vingerafdrukken	2	1
Derdenverstrekking	Fraudebestrijding	4	1
Derdenverstrekking	Geheimhoudingsplicht	117	20
Derdenverstrekking	Overig	643	155
Derdenverstrekking	Samenwerkingsverbanden	11	3
Derdenverstrekking	Zelfregulering	4	0
Handel	Cliëntvolgsystemen	3	3
Handel	Direct Marketing	117	117
Handel	Kredietwaardigheid	64	11
Handel	Overig	90	47
Handel	Telefoongidsen	17	1
Identificatie	Anonimisering	4	1
Identificatie	Kenteken	12	6
Identificatie	Legitimatie	33	7
Identificatie	Nummeridentificatie	10	6
Identificatie	Overig	23	2
Identificatie	Persoonsnummers	12	7
Internet	E-mail	17	17
Internet	Internet	65	65
Internet	Overig	10	10
Internet	Spam	4	4
Observatie	(leeg)	1	1
Observatie	Cameratoezicht	41	40
Observatie	Heimelijke waarneming	14	2
Observatie	Overig	20	1
Observatie	Tracking en tracing	3	3
Overig	Genealogie	6	3
Overig	Onderzoek	33	7
Overig	Overig	637	143
Risicoselectie	Overig	6	0
Risicoselectie	Risicoselectie	4	2
Risicoselectie	Zwarte lijsten	32	11
Techniek	Authenticatie	4	4
Techniek	Bestandsbeveiliging/ beveiligingsystemen	15	11
Techniek	Overig	37	14
Techniek	RFID	1	1
Techniek	(leeg)	1	0
Totaal		*2.187*	*741*

relateren waren aan ICT en de overige klachten niet gingen over het onderzoek, maar meer over de handelwijze van of wijze van bejegening door instituten.

Daarom hebben we voor alle subrubrieken, op de subrubrieken van internet na, de volgende werkwijze toegepast:
- Per subrubriek hebben we bekeken of er een plausibele redenering kan worden gevonden die verklaart waarom de subrubriek volledig als wel of niet ICT-gerelateerd valt aan te duiden.
- Als een dergelijke redenering te geven is, hebben we op basis van een steekproef getoetst of de geselecteerde klachten ICT-gerelateerd zijn. Als dit het geval is, dan beschouwen we alle klachten in de subrubriek als ICT-gerelateerd.
- Als er geen plausibele redenering te geven is, hebben we alle klachten semi-automatisch gescand, dat wil zeggen dat we per klacht hebben gekeken of er bij de klachtomschrijving ICT-gerelateerde termen zijn te vinden, zoals ‘(GBA) bestand’, ‘website’, ‘wachtwoord/password’, ‘digitaal’, ‘e-mail’, ‘internet’ enzovoorts. Als dit het geval is, beschouwen we de klacht als ICT-gerelateerd.

We merken op dat we relatief veel klachten hebben gevonden waarvan uit de omschrijving blijkt dat deze duidelijk ICT-gerelateerd zijn, maar die vaak onder een andere (hoofd)rubriek (veelal onder ‘overig’) worden geclassificeerd. Van de 676 klachten van de hoofdrubriek ‘overig’ bleken er 153 ICT-gerelateerd te zijn. Enkele voorbeelden zijn ‘naam kroongetuige tegen xxx op internet’, ‘plaatsen van medische gegevens op internet’, ‘verwijderen van persoonlijke gegevens en foto van internet’, ‘verstrekken van e-mailadres/en autorisatie tot e-mailbox aan derden’, ‘inzage digitale logboek’, ‘toelaatbaarheid bestandskoppeling’ en ‘klacht inzake digitaal opslaan van pasfoto’.

Tevens constateerden we dat er binnen de subrubriek ‘overig’ van de verschillende hoofdrubrieken een fors aantal ICT-gerelateerde klachten te vinden zijn. Bijvoorbeeld: 155 van de 643 klachten van de subrubriek ‘overig’ binnen de hoofdrubriek ‘derdenverstrekking’ bleken ICT-gerelateerd te zijn. In tabel 6.3 is te zien hoe de klachten per rubriek zijn onderverdeeld over de verschillende subrubrieken. In de laatste kolom staat aangegeven hoeveel van de klachten in een subrubriek als ICT-gerelateerd zijn te beschouwen.

Uit tabel 6.3 leiden we af dat in het CBP-bestand 741 van de in totaal 2.187 klachten ICT-gerelateerd zijn, ofwel 34 procent.

Verdeling van klachten over sectoren

Het CBP-bestand maakte het mogelijk om de klachten te verdelen over een aantal sectoren. In het bestand wordt bij iedere klacht aangegeven tot welke sector deze behoort. In totaal zijn er 11 sectoren onderscheiden, namelijk openbaar bestuur,

sociale zekerheid, zorg en welzijn, handel en dienstverlening, arbeid, internationale organisaties, politie en justitie, telecommunicatie, betrokkene, overige instellingen en de sector overig. Uit het bestand blijkt dat bij de sector openbaar bestuur het klachten betreft over onder andere de gemeenten, provincies en rijksoverheid, met uitzondering van justitie, de belastingdienst, toezichthouders, onderwijs enzovoorts. Klachten over politie en justitie, die strikt genomen onder het openbaar bestuur vallen, bevinden zich in de sector politie en justitie. Klachten over het UWV zijn ondergebracht onder sociale zekerheid. Klachten die onder andere betrekking hebben op ziekenhuizen, welzijnsorganisaties en de GGD zijn ondergebracht onder de sector zorg en welzijn. De aanwezigheid van het veld sector maakte het mogelijk om tabel 6.4 te genereren, waarin per sector is aangegeven hoeveel klachten betrekking hebben op een sector en het percentage ervan dat ICT-gerelateerd is. Kenmerkend voor de sector 'betrokkene' in tabel 6.4 is dat de beklaagden in deze sector particulieren of particuliere organisaties zijn. De klachten in deze sector hebben bijvoorbeeld betrekking op het verstrekken en gebruik van gegevens door particuliere instanties en het plaatsen van camera's door buurtgenoten. Verder zien we bij de indeling in sectoren een sector 'arbeid'. Deze sector is sterk gerelateerd aan de hoofdrubriek 'werk' in tabel 6.2. Voor de hoofdrubriek 'werk' is kenmerkend dat de klachten veelal gaan over het verstrekken van persoonsgegevens aan derden, de onzorgvuldige omgang met en het vastleggen van persoonsgegevens door een werkgever (van een klager). De sector 'arbeid' is veelomvattender en bevat bijvoorbeeld ook klachten over het arbeidsrecht in brede zin.

Tabel 6.4 **Het aandeel ICT-gerelateerde klachten van totaal aantal klachten verdeeld over sectoren**

Sector	Totaal aantal klachten	ICT-gerelateerde klachten	In %
Openbaar bestuur	344	122	36
Sociale zekerheid	126	20	16
Zorg en welzijn	233	45	19
Handel en dienstverlening	835	315	38
Arbeid	172	35	20
Internationale organisaties	6	3	–*
Politie en justitie	123	31	25
Telecom	167	93	56
Betrokkene	13	7	–*
Overige instellingen	122	55	45
Overig	46	15	–*
Totaal	*2.187*	*741*	*34*

* Vanwege de kleine absolute aantallen hebben we hier geen percentage berekend.

Tabel 6.5 Verdeling van de klachten per sector over de verschillende hoofdrubrieken

Sector	Totaal aantal klachten	ICT-gerelateerde klachten
Openbaar bestuur	*344*	*122*
- Werk	4	1
- Biometrie	1	1
- Derdenverstrekking	157	50
- Handel	10	8
- Identificatie	26	7
- Internet	11	11
- Observatie	17	11
- Risicoselectie	3	2
- Techniek	7	2
- Overig	108	29
Sociale Zekerheid	*126*	*20*
- Werk	6	4
- Derdenverstrekking	36	8
- Handel	1	1
- Identificatie	4	1
- Internet	1	1
- Observatie	3	1
- Risicoselectie	2	0
- Techniek	5	0
- Overig	68	4
Zorg en Welzijn	*233*	*45*
- Biometrie	5	2
- Derdenverstrekking	131	15
- Handel	9	6
- Identificatie	2	1
- Risicoselectie	2	0
- Techniek	5	4
- Overig	79	17
Handel en Dienstverlening	*835*	*315*
- Werk	7	0
- Derdenverstrekking	254	54
- Handel	191	117
- Identificatie	40	8
- Internet	41	41
- Observatie	30	15
- Risicoselectie	24	8
- Techniek	21	9
- Overig	227	63
Arbeid	*172*	*35*
- Werk	45	6
- Biometrie	1	1
- Derdenverstrekking	65	8
- Handel	2	2
- Identificatie	5	2
- Internet	6	6
- Observatie	10	5
- Techniek	3	2
- Overig	35	3

Vervolg	Totaal aantal klachten	ICT-gerelateerde klachten
Internationale Organisaties	*6*	*3*
- Derdenverstrekking	2	0
- Handel	1	1
- Internet	1	1
- Techniek	1	0
- Overig	1	1
Politie en Justitie	*123*	*31*
- Werk	1	0
- Derdenverstrekking	54	6
- Identificatie	1	1
- Internet	2	2
- Observatie	6	5
- Risicoselectie	3	1
- Techniek	8	7
- Overig	48	9
Telecom	*167*	*93*
- Derdenverstrekking	38	21
- Handel	55	25
- Identificatie	11	8
- Internet	24	24
- Observatie	3	1
- Risicoselectie	5	0
- Techniek	5	3
- Overig	26	11
Betrokkene	*13*	*7*
- Biometrie	1	1
- Derdenverstrekking	2	1
- Observatie	3	3
- Overig	7	2
Overige instellingen	*122*	*55*
- Werk	1	0
- Derdenverstrekking	38	16
- Handel	18	15
- Identificatie	5	1
- Internet	7	7
- Observatie	5	4
- Risicoselectie	3	2
- Techniek	2	2
- Overig	43	8
Overig	*46*	*15*
- Derdenverstrekking	2	0
- Handel	4	4
- Internet	3	3
- Observatie	2	2
- Overig	35	6
Totaal	*2.187*	*741*

Als we de typische overheidssectoren beschouwen, dan is het relatief grote percentage van 36 procent ICT-gerelateerde klachten bij de sector openbaar bestuur opvallend. De sector sociale zekerheid heeft het kleinste percentage ICT-gerelateerde klachten, namelijk 16 procent. De telecomsector is koploper als het gaat om het aantal ICT-gerelateerde klachten; meer dan de helft van de klachten is hier ICT-gerelateerd.

Door het combineren van de tabellen 6.2 en 6.4 verkrijgen we inzicht in de manier waarop de onderscheiden hoofdrubrieken verdeeld zijn binnen een sector. In tabel 6.5 zijn de resultaten weergegeven. Bij de overheid-gerelateerde sectoren zien we dat een fors deel van de ICT-gerelateerde klachten betrekking heeft op de hoofdrubriek 'Derdenverstrekking'. Binnen de sectoren 'Openbaar bestuur', 'Zorg en Welzijn' en 'Sociale zekerheid' zien we dat het aandeel van de klachten dat betrekking heeft op 'Derdenverstrekking' meer dan 30 procent is. Bij 'Politie en Justitie' is dat een stuk lager, namelijk rond de 20 procent. Opvallend is dat binnen de sector 'Zorg en Welzijn' geen enkele klacht direct betrekking heeft op de rubriek 'internet', met andere woorden geen klachten over e-mail, spam, login en wachtwoorden, phishing, enzovoort.

Tabel 6.6 Ontwikkeling van totaal aantal en aantal ICT-gerelateerde klachten, 1996-2010

Jaar	Totaal aantal klachten	ICT-gerelateerde klachten	in percentage (%)
1996	1	0	–*
1997	26	6	23
1998	39	12	31
1999	177	52	29
2000	152	53	35
2001	129	59	46
2002	163	53	33
2003	199	75	38
2004	227	69	30
2005	190	62	33
2006	241	81	34
2007	192	68	35
2008	223	74	33
2009	173	63	36
2010	55	13	–*

* Vanwege de kleine absolute aantallen hebben we hier geen percentage berekend.

Ontwikkeling van klachten

In tabel 6.6 brengen we het aantal klachten en het aandeel ICT-gerelateerde klachten per jaar in beeld voor de periode van 1996 tot en met mei 2010. Vanaf 2000 zien we dat het percentage ICT-gerelateerde klachten varieert tussen de 30 en 38, met een uitschieter van 46 procent in 2001. Deze uitschieter zou te maken kunnen hebben met de *internet bubble* die in het voorjaar van 2001 knapte en die wereldwijd een lichte recessie veroorzaakte. Om een verband vast te kunnen stellen is echter nader onderzoek van de klachten nodig.

6.3.3 EEN REFLECTIE OP DE BESTANDEN

Informatiesystemen/databasesystemen kunnen gezien worden als een afbeelding of model van een deel van de werkelijkheid. Bij het ontwerpen van informatiesystemen in organisaties worden de kernprocessen van een organisatie als de werkelijkheid beschouwd die gemodelleerd dient te worden en vervolgens omgezet moet worden in een informatiesysteem/databasesysteem. Deze systemen wor-den gebruikt om de werkelijkheid te begrijpen en/of te sturen. Er bestaat dus een sterke afhankelijkheid tussen deze systemen en de kernprocessen van organisaties. Om adequaat met deze afhankelijkheid om te gaan wordt geadviseerd om bij (ingrijpende) veranderingen in de kernprocessen zorgvuldig na te gaan hoe de informatiesystemen van een organisatie aangepast dienen te worden en vice versa. Aan die zorgvuldigheid ontbreekt het nog regelmatig bij het bouwen van informatiesystemen (Laudon & Laudon 2009). Dientengevolge constateren we dat de ingevoerde systemen verre van optimaal zijn, dat wil zeggen er is een discrepantie tussen de informatiebehoefte van de gebruikers en de informatie en de functionaliteiten die het systeem aanbiedt.

Tijdens onze analyse van de bestanden van het CMI en het CBP troffen we een aantal concrete punten aan waarop deze informatiesystemen voor verbetering vatbaar zijn. Het CMI registreert de meldingen in MS ACCESS en slaat daarnaast de meldingsformulieren digitaal op. MS ACCESS is een pseudo-relationeel databasesysteem dat geschikt is om relatief kleine hoeveelheden data op te slaan en daardoor vooral geschikt is voor persoonlijk gebruik. Naarmate de databasetoepassingen in omvang toenemen, complexer worden en meerdere gebruikers ondersteund moeten worden, wordt MS ACCESS steeds ongeschikter. MS ACCESS beschikt over een beperkt aantal mogelijkheden om data te bewerken. Omdat de verwachting is dat het aantal meldingen en databasetoepassingen bij het CMI zal toenemen in de loop van de jaren, en het CMI een professionele overheidsorganisatie is, is het de vraag of MS ACCESS als databasesysteem wel toereikend is voor nu, en vooral in de toekomst.

Verder bleek dat de database van het CMI relatief weinig kenmerken van de meldingen bevatte. Er worden geen data rechtstreeks vanuit de digitale meldingsformulie-

ren geëxtraheerd naar de database. Daardoor is de database voor analysedoeleinden beperkt bruikbaar. Een uitsplitsing van de meldingen naar verschillende sectoren bijvoorbeeld is niet mogelijk, omdat deze informatie niet opgeslagen wordt. Nu bevat zowel de MS ACCESS-database als de verzameling van meldingsformulieren informatie over meldingen met betrekking tot identiteitsfraude en registratiefouten in persoonsgegevens. Echter, deze informatie kan niet optimaal benut worden, omdat deze gegevens niet met elkaar zijn geïntegreerd. Te overwegen valt om over te stappen op een solide databasesysteem, en de digitale gegevens met betrekking tot identiteitsmeldingen en registratiefouten in persoonsgegevens geïntegreerd op te slaan in dit systeem.[4]

Bij het CBP troffen we wel een systeem aan waar de gegevens met betrekking tot klachten geïntegreerd worden opgeslagen. Echter, ook bij het CBP merkten we een mismatch op tussen het systeem en de organisatie. CBP-medewerkers vullen het systeem met data, maar verschillende CBP-medewerkers hebben verschillende interpretaties van een en hetzelfde begrip waardoor de velden in het systeem inconsequent worden ingevuld. Dientengevolge ontstaat er ruis in het systeem.

Van iedere klacht wordt in het systeem opgeslagen tot welke hoofdrubriek deze behoort. Omdat heldere criteria soms ontbreken wanneer een klacht tot een bepaalde hoofdcategorie behoort, volgt de medewerker hierbij zijn/haar eigen ervaring en kennis. Zo valt een klacht die betrekking heeft op het verwijderen van gegevens van internet de ene keer onder de hoofdrubriek 'Overig' en de andere keer onder de hoofdrubriek 'Internet'. Ook zou een aantal begrippen scherper en/of eenduidiger kunnen worden gedefinieerd, zodat bijvoorbeeld de verschillen tussen sectoren als 'Openbaar bestuur' en 'Politie en Justitie', en tussen de hoofdrubriek 'Werk' en de sector 'Arbeid' duidelijker onderscheiden worden. Het inrichten van een adequate metadatabase, waarin metadata opgeslagen kunnen worden, zou hier een oplossing bieden. Een ander issue waar ons inziens het CBP onvoldoende aandacht aan besteedt, is dat de semantiek van begrippen/data in de loop der tijden aan verandering onderhevig kan zijn en hoe systematisch hier mee om te gaan. Zo was er in de jaren negentig wellicht nog geen noodzaak om een hoofdrubriek 'Internet' of 'Biometrie' te onderscheiden en werden klachten die betrekking hadden op deze zaken onder de hoofdrubriek 'Overig' geplaatst. Op het moment dat besloten wordt om wel een categorie 'Internet' te onderscheiden, dient er een herinrichting van de hoofdrubrieken plaats te vinden, zodat het systeem een afbeelding vormt van de nieuwe werkelijkheid. Concreet kan dit bijvoorbeeld inhouden dat klachten met betrekking tot internet, ook met terugwerkende kracht, overgeheveld worden van de hoofdrubriek 'Overig' naar de nieuwe hoofdrubriek 'Internet'. Omdat databasemanagementsystemen vanuit zichzelf onvoldoende ondersteuning voor dit soort *data evolutie* bieden, zal een organisatie hier zelf een procedure voor moeten ontwikkelen. Indien dit nagelaten wordt, zal het systeem steeds minder goed voldoen aan de informatiebehoefte van

de medewerkers. Ook kan er op termijn een 'systeemwerkelijkheid' gaan ontstaan die sterk afwijkt van de echte werkelijkheid zoals we die kennen. Omdat overheidsorganisaties hun beleid en verantwoording mede baseren op de informatie die afkomstig is uit dit soort systemen, is dit onwenselijk.

6.4 EEN EERSTE STAP NAAR MEER INZICHT IN POTENTIËLE KLACHTEN

Naast het verkrijgen van inzicht in de aard en omvang van daadwerkelijk gemelde klachten op het gebied van informatietechnologie is het zinvol onderzoek te doen naar het potentieel aan klachten over informatietechnologie. In hoeverre komen situaties voor waarin onvolkomenheden in informatie en technologie kunnen leiden tot een klacht van de burger, en wat zijn de juridische, technische en organisatorische omstandigheden waarin deze onvolkomenheden optreden? Om een eerste stap te doen in de beantwoording van deze vragen bekijken we de sector uit sectie 3.2, die het dagelijks werkterrein van het WODC betreft, in meer detail: politie en justitie.

Politie en justitie tellen diverse organisaties, die elk betrekkelijk zelfstandig opereren. Deze organisaties ontwikkelden ieder hun eigen operationele systemen. Zo ontwikkelden de politieregio's, naast de drie operationele systemen die inmiddels zijn vervangen door de landelijk ingevoerde Basisvoorziening Handhaving (BVH), de regionale HerKenningsdienst Systemen (HKS). Het Openbaar Ministerie ontwikkelde het Communicatiesysteem Openbaar Ministerie-Parket Administratiesysteem (COMPAS), dat inmiddels wordt vervangen door het Geïntegreerd Proces Systeem (GPS). De justitiële documentatie wordt geregistreerd in het Justitieel Documentatie Systeem (JDS) en de Dienst Justitiële Inrichtingen voert haar gegevens in het systeem TenUitvoerLegging Penitentiaire Beschikkingen (TULP) in.

Naast de operationele systemen zijn er tegelijkertijd vele daarvan afgeleide databases gebouwd, waarin de gegevens uit de operationele systemen geschikt zijn gemaakt voor analyse en rapportage ten behoeve van de managementinformatie voor de organisatie. Zo ontwikkelde de politie voor onderzoeksdoeleinden een landelijke versie van HKS met daarin gegevens uit alle regionale versies van HKS. Het OM ontwikkelde, ter verkrijging van managementinformatie uit het operationele systeem COMPAS, een landelijke database Openbaar Ministerie Data (OMDATA), waarin de gegevens uit alle arrondissementen worden samengevoegd.[5] De Onderzoek- en Beleidsdatabase Justitiële Documentatie (OBJD) is een database met een selectie van gegevens uit het JDS, speciaal gebouwd voor onderzoeksdoeleinden en beheerd door de Justitiële Informatiedienst in Almelo.

Aangezien de bovengenoemde gegevensbronnen ieder ontwikkeld zijn door een andere organisatie ten behoeve van verschillende doelgroepen met ieder een eigen

informatiebehoefte, zal het niet verbazen dat deze bronnen veelal dezelfde informatie bevatten, maar op veel fronten verschillend van elkaar zijn. Een van de consequenties hiervan is dat, wanneer een informatievraag uit meer dan één van deze bronnen beantwoord kan worden, de antwoorden zelden gelijk zijn. Bovendien kunnen de antwoorden inconsistenties bevatten als gevolg van verschillen in de definities die in de verschillende systemen worden gehanteerd, hetgeen de validiteit en de betrouwbaarheid van informatie niet ten goede komt. Zo kan een strafbaar feit in een proces-verbaal door middel van andere artikelen uit het Wetboek van Strafrecht omschreven zijn (bijv. Wetboek van Strafrecht Sr. 311: diefstal door middel van braak) dan in de strafzaak die daaruit voortvloeit (in dit voorbeeld Sr. 310/311: eenvoudige diefstal/diefstal door middel van braak; Sr. 310 is toegevoegd voor het geval Sr. 311 niet te bewijzen is). Dit strafbare feit kan op het moment dat een officier van justitie een beslissing neemt tot dagvaarding weer anders omschreven zijn dan op het moment van inschrijving van de strafzaak bij het parket (bijv. Sr. 310/311/312: 312 wordt toegevoegd, omdat uit het proces-verbaal ook kan worden afgeleid dat de verdachte tijdens de inbraak de bewoners heeft bedreigd). Het antwoord op een vraag als 'Hoeveel zaken betreffende eenvoudige diefstal zijn er in een jaar?' zal afhankelijk van de gekozen gegevensbron verschillend worden beantwoord.

Naarmate er vanaf het einde van de jaren negentig meer belangstelling kwam voor de strafrechtsketen als geheel en de verhouding van de verschillende ketenpartners ten opzichte van elkaar, groeide de behoefte aan samenhangende, consistente informatie over de gehele keten. Beleidsmakers, politici en onderzoekers willen gegevens van de verschillende ketenpartners met elkaar vergelijken, bijvoorbeeld om inzicht te krijgen in de manier waarop bepaalde groepen van verdachten (bijv. minderjarigen en veelplegers) of strafzaken (bijv. geweldsdelicten en vandalisme) zich door de keten bewegen. Informatie uit verschillende gegevensbronnen dient daarbij steeds vaker op de een of andere manier met elkaar te worden verbonden. Naast informatie op geaggregeerd niveau wordt deze werkwijze ook steeds vaker toegepast voor het volgen van individuen door de strafrechtsketen. Gegeven bovengenoemde eigenschappen en tekortkomingen van de bestanden kan deze werkwijze nadelig uitpakken voor de burger indien de bronnen in onvoldoende mate worden opgeschoond en feiten niet uniform worden opgeslagen. Het adequaat opschonen en uniformeren van bestanden is niet louter een technische aangelegenheid, maar vereist ook een organisatorische component. Hier gaan de implicaties van technologie en informatie dus hand in hand. Verantwoordelijkheden, taken en communicatiestructuren dienen goed ingebed te zijn in een organisatie om het opschonen en uniformeren van data in goede banen te leiden. Door in meer detail te kijken naar bewaartermijnen en de mate waarin systemen zijn vervuild, maken we de gevolgen hiervan inzichtelijk.

Bewaartermijnen en vervuiling van systemen

Voor alle in de strafrechtsketen gehanteerde informatiesystemen gelden wettelijk vastgelegde termijnen waarna de in de systemen opgeslagen gegevens dienen te worden verwijderd. Deze *bewaartermijnen* kunnen echter niet alleen tussen organisaties verschillen, maar ook binnen de organisaties tussen de verschillende informatiesystemen. Zelfs binnen een informatiesysteem kan meestal geen eenduidige bewaartermijn worden gehanteerd. Volgens de Wet justitiële en strafvorderlijke gegevens (Wjg) geldt in het algemeen dat "justitiële gegevens over misdrijven uit de justitiële documentatie worden verwijderd dertig jaren na onherroepelijke afdoening van de strafzaak in het kader waarvan die gegevens zijn verwerkt of het vervallen van het recht tot strafvordering door verjaring dan wel twintig jaren na het overlijden van betrokkene," maar voor ernstige zedenmisdrijven geldt alleen laatstgenoemde termijn.[6] Ook wordt de bewaartermijn van justitiële gegevens omtrent personen veroordeeld tot een onvoorwaardelijke vrijheidsstraf van langer dan drie jaar, tbs of jeugddetentie verlengd met de uitgesproken strafduur, en gelden speciale bepalingen voor misdrijven met een hoge strafdreiging.[7] Van de ruim vijfhonderd personen die in 2008 werden veroordeeld tot een onvoorwaardelijke vrijheidsstraf van drie jaar of langer, mogen de gegevens dus (soms substantieel) langer worden bewaard in de justitiële documentatie dan van de ruim 20.000 personen die een lagere onvoorwaardelijke vrijheidsstraf kregen opgelegd.[8]

Mede vanwege de verschillende bewaartermijnen is het opschonen en uniformeren van informatie een complex proces. Zo leidt het Korps Landelijke Politiediensten (KLPD) uit de 25 regionale versies van het HKS een landelijke versie van HKS af, bedoeld voor managementinformatie en onderzoek. In de regionale HKS-bestanden worden gegevens geregistreerd van alle wegens een misdrijf door de politie aangehouden natuurlijke personen tegen wie een proces-verbaal is opgemaakt. Het kan voorkomen dat een verdachte X in meerdere regionale bestanden voorkomt voor hetzelfde delict, bijvoorbeeld wanneer een verdachte wordt verdacht van het plegen van een delict in regio A, maar wordt opgepakt in regio B. Om dubbeltellingen te voorkomen vindt er bij het samenstellen van het landelijke HKS-bestand een 'ontdubbelingsprocedure' plaats.

In bovenstaand voorbeeld wordt informatie over persoon X op drie plaatsen opgeslagen voor onderzoeksdoeleinden: in het regionale HKS-bestand in regio A, in regio B en in het landelijke HKS-bestand. Daarnaast is de informatie ook opgeslagen in de operationele systemen in regio A en regio B. Dit houdt in dat, als er wijzigingen met betrekking tot de informatie van persoon X plaatsvinden, bijvoorbeeld wanneer verdachte X wordt vrijgesproken of er een sepot plaatsvindt, dit op tenminste vijf plaatsen verwerkt dient te worden. Als dit niet gebeurt, dan hangt het er maar net van af welke bron bevraagd wordt om vast te stellen of persoon X nog steeds al dan niet verdacht is. Om deze onwenselijke situatie te voorkomen

dienen er in principe heldere procedures en communicatiestructuren te zijn voor de verwerking van wijzigingen. Om de rechten van de burger voldoende te beschermen is een zorgvuldige werkwijze van groot belang. Dat blijkt wel uit zaken als die van de Surinaamse zakenman die vanaf 1994 jarenlang slachtoffer bleef van identiteitsfraude (Nationale Ombudsman, 2008).

Er zijn echter aanwijzingen dat het doorvoeren van wijzigingen voor verbetering vatbaar is, in elk geval voor het landelijke HKS-bestand. Dit bestand bevat gegevens over verdachten tegen wie een proces-verbaal is opgemaakt vanaf 1996, en wordt onder andere gebruikt door onderzoeksinstituten en universiteiten. Als we het landelijke HKS-bestand analyseren over de periode 1996 tot en met 2008, dan zien we dat het bestand nog gegevens bevat van overleden personen en van verdachten die zijn vrijgesproken. Zo hebben zo'n 8.000 verdachten van de in totaal 1,5 miljoen (unieke) verdachten in HKS in de periode 1996-2008 de status 'overleden', en komen 2.800 personen die zijn vrijgesproken ten onrechte toch in HKS voor. Relatief gezien valt het aantal onterecht geregistreerden mee: op ruim 1,5 miljoen verdachten in totaal gaat het om minder dan 0,7 procent. Bovenstaand voorbeeld laat echter wel zien dat het landelijke HKS zonder aanvullende bewerkingsslagen[9] niet geschikt is voor gebruik van gegevens op individueel niveau, aangezien dat nadelige gevolgen zou kunnen hebben voor onterecht geregistreerde burgers of hun nabestaanden.

Vanwege de complexiteit omtrent bewaartermijnen en de omvang van de informatiesystemen is het in het kader van deze studie niet mogelijk gebleken om een bredere analyse uit te voeren naar de mate waarin gegevens over burgers ten onrechte nog voorkomen in bronnen als HKS, OMDATA, OBJD en TULP. Cijfermatige conclusies omtrent de mate van vervuiling en het potentieel aan klachten van burgers hierover blijven daarom hier achterwege. Zeker nu de mogelijkheden voor politie en justitie om geavanceerde onderzoekstechnieken als datamining in te zetten voor het opstellen van risicoprofielen zich steeds verder uitbreiden (Cocx 2009), waarbij gegevens uit verschillende informatiesystemen aan elkaar worden gekoppeld, verdient uitgebreider onderzoek echter nadrukkelijk aanbeveling.

6.5 CONCLUSIES

Inzicht in de relatie overheid-burger onder invloed van ICT kan enerzijds verkregen worden door de rol van informatietechnologie op beginselen te bestuderen aan de hand van domeinstudies en blackboxes. Anderzijds kan dat inzicht verkregen worden door het in kaart brengen van *geregistreerde klachten* of *potentiële klachten* van burgers die ICT-gerelateerd zijn. In dit hoofdstuk hebben we de laatste invalshoek gekozen en hebben we de omvang van ICT-gerelateerde klachten bepaald voor een aantal overheidsbestanden.

Het eerste bestand dat we in de analyse van geregistreerde klachten onder de loep hebben genomen, is een bestand van het CMI dat een relatief klein aantal klachten bevat. Uit onze analyse blijkt dat 97 van de 241 klachten die ontvangen zijn in 2009, dus 40 procent, te relateren is aan ICT. Het tweede bestand is een bestand van het CBP, dat vanaf 1996 klachten registreert. Dit bestand bevat in totaal 2.187 klachten, waarvan 741 te relateren zijn aan ICT, ofwel 34 procent. Voor 2009 ligt het percentage ICT-gerelateerde klachten op 37 procent. Van de typische overheidssectoren die zijn onderscheiden in onze analyse (openbaar bestuur, zorg en welzijn, politie en justitie, sociale zekerheid) blijkt dat bij de sector openbaar bestuur het percentage ICT-gerelateerde klachten het hoogst is, namelijk 36 procent. Om de informatie uit en functionaliteiten van deze bestanden (blijvend) goed te laten aansluiten op de informatiebehoefte van de gebruikers ervan, is het van belang dat gegevens geïntegreerd worden opgeslagen, dat er een adequate metadatabase wordt ingericht en dat er oog is voor in de loop der tijd veranderende definities (data-evolutie).

Wat betreft potentiële klachten hebben we gekeken naar het ten onrechte voorkomen van burgers in het HKS-bestand van de politie. Zo blijken in het landelijke HKS-bestand 8.000 verdachten de status 'overleden' te hebben, en komen 2.800 personen die zijn vrijgesproken toch ten onrechte in HKS voor. Relatief gezien valt het aantal onterecht geregistreerden mee: op ruim 1,5 miljoen verdachten in totaal gaat het om minder dan 0,7 procent. Om dergelijke onterechte registraties en inconsistenties te voorkomen is tijdig en zorgvuldig opschonen en uniformeren van registraties van belang. Dit is niet slechts een technische maar ook een organisatorische aangelegenheid. Het bleek in het kader van deze studie niet mogelijk om tot cijfermatige conclusies te komen met betrekking tot het potentieel aan ICT-gerelateerde klachten, maar gezien de voortschrijdende technische mogelijkheden tot koppeling van gegevens en de mogelijke impact van onterechte registratie is nader onderzoek zeker gewenst.

DANKWOORD

Onze dank gaat uit naar het CBP, in de persoon van mw. mr. A.C.J.M. Emmaneel, en het CMI, in de persoon van drs. M.J.E.P. Savelkoul, voor hun medewerking aan dit onderzoek en het verlenen van toegang tot de databases. Daarnaast zijn we dank verschuldigd aan Wim Alblas, Marisca Brouwers, Soenil Jangbahadoer Sing, Laurens de Jonge en Ronald Meijer voor het analyseren van de bestanden en het geven van waardevolle suggesties voor dit onderzoek.

AFKORTINGEN

BIT	Beleid, Informatie en Technologie
BVH	Basisvoorziening Handhaving
CBP	College bescherming persoonsgegevens
CBS	Centraal Bureau voor de Statistiek
CMI	Centraal Meldpunt Identiteitsfraude
COMPAS	Communicatiesysteem Openbaar Ministerie-Parket Administratiesysteem
DNA	desoxyribo nucleic acid
GBA	Gemeentelijke Basis Administratie
GPS	Geïntegreerd Proces Systeem
HKS	HerKenningsdienst Systeem
ICT	Informatie en Communicatie Technologie
JDS	Justitieel Documentatie Systeem
KLPD	Korps Landelijke Politiediensten
OBJD	Onderzoek- en Beleidsdatabase Justitiële Documentatie
OMDATA	Openbaar Ministerie Data
RFID	Radio frequency identification
TULP	TenUitvoerLegging Penitentiaire Beschikkingen
Wjg	Wet justitiële en strafvorderlijke gegevens

NOTEN

1 Een SQL-query is een opdracht aan een relationeel databasemanagementsysteem die gespecificeerd is in een formele taal.

2 Melding maken kan via http://www.overheid.nl/media/downloads/Meldingsformulier_Identiteitsfraude.pdf en http://www.overheid.nl/media/downloads/Meldingsformulier_fout_registratie_persoonsgegevens.pdf.

3 In de categorie 'misbruik eigen identiteit' worden meldingen geregistreerd waarbij de personen hun eigen identiteit misbruiken, zoals het zelf verkopen of als vermist opgeven van eigen identiteitspapieren, het opgeven van verschillende personalia, look-a-like fraudes et cetera. Uiteraard zijn deze personen veelal niet zelf de melders van de meldingen in deze klasse.

4 Een (niet uitputtende) vergelijking tussen databasesystemen is te vinden op http://en.wikipedia.org/wiki/Comparison_of_relational_database_management_systems.

5 Met de overgang van COMPAS naar GPS wordt ook het managementinformatiesysteem OMDATA vervangen door het nieuwe datawarehouse PHOENIX.

6 Zie Wet justitiële en strafvorderlijke gegevens (Wjg), artikel 4.

7 Zie Wjg, artikel 5.

8 Bron: Onderzoek- en Beleidsdatabase Justitiële Documentatie (OBJD).

9 Het CBS, dat verdachten uit het landelijke HKS koppelt aan het Sociaal Statistisch Bestand ten behoeve van onderzoek naar achtergronden van daders, verwijdert de overledenen voor koppeling uit het HKS-bestand.

LITERATUUR

Cocx, T. (2009) *Algorithmic tools for data-oriented law enforcement,* proefschrift Leiden: Leiden University Press; https://openaccess.leidenuniv.nl/bitstream/1887/14450/5/thesis.pdf

Dijk, J. van, F. Leeuw & S. Choenni (2007) 'Klachtprofielen, trefkansen en intermediairs: de Nationale Ombudsman tussen 1985 en 2006' in *Werken aan behoorlijkheid, De Nationale Ombudsman in zijn Context*, Den Haag: Boom Juridische Uitgevers.

Laudon, K. & J. Laudon (2009) *Management information systems (11th Edition)*, New York: Prentice Hall.

Nationale Ombudsman (2008) *Openbaar rapport 2008/232*, Den Haag: Nationale Ombudsman.

DEEL II

7 GRENSOVERSCHRIJDENDE MOBILITEIT VAN PERSONEN EN DE DIGITALE GRENZEN VAN EUROPA

Dennis Broeders

7.1 INLEIDING

In het domein van 'internationale mobiliteit' en de toepassing van technologie daarin lopen verscheidene zaken door elkaar. Er zijn drie verschillende vormen van grensoverschrijdende mobiliteit die aan het beleid trekken, meestal in verschillende richtingen. De eerste zijn de *migranten* en het migratiebeleid. Wie mag wel komen en wie niet? Bij het migratiebeleid gaat het om mensen die zich willen vestigen, dat kan voor kortere of langere tijd zijn, maar het is een cruciaal onderscheid met de tweede groep, die van de reizigers. *Reizigers* zijn passanten; mensen die een land als Nederland voor korte tijd bezoeken in het kader van zaken of toerisme. Een belangrijke groep die van vitaal belang is voor de economie. De derde groep is die van de *terroristen* en de criminelen; deze 'groep' heeft een heel ander karakter, is klein in aantal, maar staat centraal in de aandacht van beleidsmakers. Deze drie groepen vereisen een andere benadering en aan die benadering liggen ook andere belangen ten grondslag. In het immigratiebeleid moeten gewenste migranten snel doorgang krijgen en ongewenste migranten worden geweerd. Zakenlieden en toeristen moeten makkelijk toegang of doorgang krijgen, reisgemak en economische belangen staan daarbij voorop. Terroristen en criminelen moeten geen toegang krijgen, of, nog beter, moeten worden opgepakt. Veiligheid is de belangrijkste overweging en controle – in vele vormen – is daarvan de belangrijkste uitwerking.

In termen van beleid en praktische controle is het probleem natuurlijk dat de verschillende categorieën hopeloos met elkaar vermengd zijn. Met name de ongewenste categorieën (ongewenste migranten, terroristen en criminelen) proberen op te gaan in de stroom van reizigers in de hoop ongemerkt toegang te verkrijgen of de grens te kunnen passeren. De link tussen terrorisme en immigratie heeft in de eerste jaren na 9/11 veel aandacht gekregen, hoewel vrij snel na de aanslagen al bekend was dat de meeste van de kapers eerder reizigers dan immigranten waren. Volgens Koslowski is "migration not the 'new security issue'; it is increasing global mobility, which is primarily tourism and business travel" (Koslowski 2008: 105). De omvang van dat (beleids)probleem is goed af te lezen aan het volume van het internationale toerisme. Tussen 1995 en 2005 steeg het aantal internationale toeristenaankomsten (*tourist arrivals*) wereldwijd van 535 miljoen naar 803 miljoen per jaar (zie tabel 7.1). Dat is inclusief de dip na 9/11. De laatst beschikbare cijfers zetten de teller voor de wereld al op 922 miljoen in 2008 (UNWTO 2009).

Voor Nederland steeg het aantal internationale aankomsten in dezelfde periode van 6.5 miljoen naar 10 miljoen aankomsten per jaar. Ter vergelijking: het cijfer voor de immigratie naar Nederland in het jaar 2005 was 92.297 personen en achter dat cijfer gaan vele categorieën schuil, zoals arbeidmigratie, asielmigratie, familiemigratie en studie. Een deel van deze migratie bestaat bovendien uit remigrerende Nederlanders (Snel et al. 2007).

Tabel 7.1 Internationale toeristenaankomsten in geselecteerde landen (in miljoenen)

	1995	2000	2003	2004	2005
Wereld	535.0	682.0	691.0	761.0	803.0
Frankrijk	60.0	77.2	75.0	75.1	75.9
Spanje	34.9	47.9	50.8	52.4	55.9
Verenigde Staten	43.5	51.2	41.2	46.1	49.2
China	20.0	31.2	33.0	41.8	46.8
Italië	31.1	41.2	39.6	37.1	36.5
Verenigd Koninkrijk	23.5	25.2	24.7	27.7	28.0
Nederland	6.5	10.0	9.2	9.6	10.0

Bron: Koslowksi 2008: 111; UNWTO 2006

Ook achter de noemer toeristen gaat een aantal categorieën schuil. In 2008 was 51 procent daadwerkelijk toerist in de strikte zin, 27 procent kwam om vrienden en kennissen te bezoeken of voor redenen van gezondheid of religie, 15 procent was zakelijk verkeer en 7 procent was *not specified* (UNWTO 2009). Bovendien moet hierbij nog opgemerkt worden dat 922 miljoen aankomsten niet gelijk staat aan 922 miljoen individuele reizigers: een deel van de internationale reizigers neemt meerdere, of zelfs vele, reizen voor zijn rekening. Maar zelfs met die kanttekening in het achterhoofd is het volume van deze internationale mobiliteit enorm.

Het volume van migratie en mobiliteit en de grote politieke druk om bepaalde problemen op te lossen (voorkomen van aanslagen en het indammen van illegale en ongewenste migratie) maakt van informatie de sleutel tot het migratiebeleid. Informatie bepaalt het verschil tussen toelating en weigering en informatie is de sleutel tot herkenning en detectie. Die informatie lag en ligt traditioneel vast in documenten (paspoorten, visa, aanvragen en onderliggende documentatie), maar in toenemende mate wordt die ook vastgelegd in systemen en registraties waardoor deze informatie overal en snel opvraagbaar is (informatiesystemen ten behoeve van het Europese asielbeleid en visabeleid, signaleringslijsten en systemen voor de veiligheid, informatie van luchtvaartmaatschappijen enz.). De druk

op het migratiebeleid (door het politieke klimaat, het volume van migratie en de vermenging met terrorisme en criminaliteit) in combinatie met het wegvallen van de interne grenzen binnen de Schengenzone, heeft ertoe geleid dat belangrijke delen van het migratiebeleid zijn geëuropeaniseerd en gedigitaliseerd (Broeders 2007; 2009).

Technologie speelt aan de grens in toenemende mate een grote rol. In het kat en muisspel tussen migranten en grensbewakers wordt volop moderne techniek ingezet: denk aan radar, infrarood scanningapparatuur, röntgenapparatuur en kooldioxide meters om voertuigen en andere potentiële schuilplaatsen te controleren. Een andere groep van instrumenten bestaat uit grote databanken waarin de persoonsgegevens van migranten worden opgeslagen met migratiecontrole als doel. In eerste instantie zijn er voornamelijk databanken ontwikkeld die de lastige – en grotendeels ongewenste – groepen van migranten 'beheersbaar' moeten maken. Daarbij gaat en ging het vooral om asielzoekers, illegale migranten en migranten die op een kortlopend visum inreizen – vanwege het risico van illegaliteit. De voornaamste databanken voor deze groepen zijn: het Schengen Informatie Systeem (SIS I en II), het Visum Informatie Systeem (VIS) en het Eurodac-systeem.

Van meer recente datum zijn de Europese voornemens om het digitale net in het kader van het migratiebeleid veel verder uit te werpen. In november 2007 kwam JBZ-commissaris Frattini met het voorstel voor een eigen EU Passenger Name Record (PNR) systeem, vergelijkbaar met het Amerikaanse systeem (Geyer 2008). In februari 2008 presenteerde de Europese Commissie haar voorstel voor een nieuw *border package*, met als hoofdbestanddelen een op te zetten Entry/Exit-systeem en een Automated Border Control System. Daarmee komen ook niet-visumplichtige reizigers die minder dan drie maanden blijven en EU-burgers zelf in beeld in de Europese migratiedatabanken en informatie-uitwisseling (Guild, Carrera & Geyer 2008). Daarnaast is de introductie en de uitrol van het Europese biometrische paspoort een belangrijke ontwikkeling die alle Europese burgers in beeld brengt. Met deze laatste voorstellen, die dus deels nog een tekentafelgeneratie zijn, komen naast de migranten straks voor het eerst ook de reizigers volop in beeld van de overheid. In eerste instantie van de immigratieautoriteiten, maar in het kielzog daarvan ook van de veiligheidsdiensten en de opsporingsautoriteiten.

Dit hoofdstuk gaat dus in hoofdzaak over de digitalisering van de grens waar die raakt aan de (immigratie)controle van – al dan niet verdachte – migranten, reizigers en EU-burgers. Het gaat niet om de – aanzienlijke – bijdrage die deze ontwikkelingen hebben geleverd aan het faciliteren van het vrije verkeer van personen binnen de grenzen van het Schengengebied. De ambitie is om in kaart te brengen op welke manier de Europese migratiecontrole zich heeft ontwikkeld in de afgelopen jaren, welke ontwikkelingen nog te verwachten zijn en wat de invloed daarvan is op het karakter van de – digitale – buitengrenzen van de EU en de controle

op internationale mobiliteit. De opzet van dit hoofdstuk is als volgt. In paragraaf 7.2 wordt de relatie tussen informatie, documentatie en mobiliteit kort uiteengezet. Ook schetst deze paragraaf kort de belangrijkste actoren in dit veld, te weten overheden, de industrie en de rol van standaarden. Paragraaf 7.3 schetst in vogelvlucht de ontwikkeling van het Europese beleidsterrein van Justitie en Binnenlandse Zaken (JBZ) aan de hand van de verschillende EU-verdragen en wat die betekenen voor de (institutionele) machtsverhoudingen en aan de hand van de 'vijfjaarsagenda's' die voor het JBZ-terrein worden opgesteld. De eerste generatie databanken (SIS I en II, Eurodac en VIS) wordt in paragaaf 7.4 geanalyseerd en de tweede generatie (PNR, Entry/Exit-systeem en het biometrisch paspoort) in paragaaf 7.5. De rol van de IT- en (biometrische) industrie komt aan de orde in paragaaf 7.6 en de rol van (technologische) standaarden in paragraaf 7.7. In paragraaf 7.8 worden conclusies getrokken.

7.2 STATEN, STANDAARDEN EN INDUSTRIE

De staat heeft in de afgelopen eeuwen, met een enorme versnelling in de afgelopen decennia, de controle over internationale mobiliteit naar zich toegetrokken. De grootschalige introductie van het paspoort is een vrij recente, negentiende-eeuwse[1], uitvinding die vooral sinds de Eerste Wereldoorlog niet meer uit het internationale statensysteem is weg te denken (Torpey 2001). Controle over de grens en de populatie werd in toenemende mate een element van (natie-)staatsvorming. Zoals Weber staatsvorming onder meer beschreef als een proces waarin de staat zich het monopolie op het legitieme gebruik van geweld toe-eigende (het geweldsmonopolie), stelt Torpey (2000) dat moderne staten steeds beter in staat zijn om de *legitimate means of movement* te monopoliseren. Legitieme internationale mobiliteit werd afhankelijk gemaakt van documenten als het paspoort, dat uitsluitend door soevereine staten kon worden verstrekt. Beide monopolies werden gevestigd op het fundament van de toenemende bureaucratische macht van de staat. Volgens Torpey (2000: 35) moest het monopolie op de *legitimate means of movement* wachten op "(…) the creation of elaborate bureaucracies and technologies that only gradually came into existence, a trend that intensified dramatically toward the end of the nineteenth century". Volgens de historicus Groebner (2007: 219) gaf de introductie van het paspoort ook aanleiding voor de opkomst van de "con-man and the imposter", wiens "career in dissimulation took place not in spite of, but through the expanding system of bureaucratic control". In de moderne tijd heet dat look-alike fraude en identiteitsfraude, maar het idee blijft hetzelfde: elk bureaucratisch systeem van identificatie geeft aanleiding tot nieuwe mogelijkheden voor fraude. Toch lijken bureaucratie en techniek in recente jaren toe aan de volgende stap. Lyon (2007: 122) spreekt van de monopolisering van de *legitimate means of identification*, hoewel hij daar onmiddellijk aan toevoegt dat er wellicht eerder sprake is van een oligopolie. In later werk blijkt de gedachte van een monopolie inderdaad aan erosie onderhevig. Lyon & Bennet (2008) en Lyon

(2009) schrijven in hun studie naar de internationale verspreiding van het fenomeen van de nationale identiteitskaarten over het ontstaan van een *Card Cartel*. Dit kartel bestaat uit de staat, de bedrijven die de kaarten ontwikkelen en als derde de technische standaarden en protocollen die architectuur en de karakteristieken van ID-kaarten en paspoorten bepalen. In plaats van een nieuw monopolie ontstaat een soort oligopolie. Lyon & Bennet noemen het ook wel een *oligopoly of the means of identification*. Dit kartel bestaat niet alleen voor identiteitskaarten, maar speelt een rol in de algemene ontwikkeling van het Europese systeem voor 'identiteitsmanagement' in internationale migratie. Databanken, biometrie, paspoorten en andere technologische toepassingen kennen allemaal hun 'kartels' van actoren die op elkaar zijn aangewezen. Naast overheden spelen dus ook bedrijven een grote rol. Naast deze twee actoren krijgt ook een schijnbaar technische aangelegenheid (standaarden en protocollen) een plaats in het triumviraat toebedeeld. Technieken, artefacten of bijvoorbeeld standaarden worden in de literatuur van de *Science and Technology Studies* echter wel vaker als een zelfstandige actor gezien (zie bijvoorbeeld Latour 2005).

Het belang van protocollen en standaarden moet niet onderschat worden. Volgens Galloway is het protocol een managementstijl, die controle mogelijk maakt in een tijd waarin traditionele controlemechanismen zoals bureaucratische hiërarchie en centralisatie aan belang inboeten (in Lyon 2009: 78). Galloway dacht hierbij voornamelijk aan internet, maar hetzelfde idee is relevant bij andere genetwerkte vormen van sturing. De digitale en op Europese schaal georganiseerde registratie van, en controle op, migratiestromen is daarop geen uitzondering, eerder een duidelijk voorbeeld. Standaarden zijn het resultaat van politieke besluitvorming en *corporate struggle*, en de interactie tussen die twee. Er zijn in ieder geval drie vormen: standaarden, zoals het besluit om gezichtsherkenning en vingerafdrukken de norm te maken voor de nieuwe biometrische EU-paspoorten (en niet bijvoorbeeld de irisscan), protocollen die bepalen op welke wijze gegevens worden verwerkt tot informatie en wat in deze studie voornamelijk voor zal komen onder de noemer van interoperabiliteit (*interoperability*). Daarnaast zijn er meer 'informeel' georganiseerde vormen van standaardisering, zoals het principe van de *availability* dat de normen stelt voor de uitwisseling van sommige soorten van informatie tussen lidstaten, maar de informatie zelf niet standaardiseert.

Het internationale bedrijfsleven speelt een belangrijke rol in het tot stand komen van het netwerk van databanken dat de Europese digitale grens vormt. Daarbij is de industrie vaak een aanjagende partij (Liberatore 2005; Lyon 2009), al is meestal moeilijk te zeggen hoe de verhoudingen precies liggen. Vaststaat wel dat de markt van databanken, biometrie en andere interne veiligheidssystemen en toepassingen sinds de aanslagen in New York in 2001 sterk in de lift zit. De OECD sprak in een studie uit 2004 over de *emerging security economy* (Stevens 2004) en Hayes (2009) spreekt van de groeiende *Homeland Security Market*. Duidelijk is in ieder

geval dat het hier om groeimarkten gaat en dat bedrijven actief de markt opgaan om hun producten aan de man te brengen. In de OECD-studie wordt de security market (die veel breder is dan waar het in deze studie over gaat) geschat op een waarde van 100 miljard dollar. Op een iets kleinere – en meer op deze casus toegesneden – schaal verwacht de International Biometric Group dat de markt voor biometrie tussen 2009 en 2014 groeit van 3,42 naar 9,37 miljard dollar. Vanwege de crisis wordt bovendien verwacht dat het grootste deel van de markt in de eerste jaren wordt bepaald door contracten van overheden (Biometric Technology Today 2009: 11). De security-industrie heeft dus alle belang bij haar plaats in het kartel.

De laatste actor in het 'kartel' is de staat. De staat of de overheid is in de praktijk altijd een samengestelde actor. Zeker als het gaat om de Europese politiek op het gebied van Justitie en Binnenlandse Zaken (JBZ) geldt dat vele overheidsactoren, zowel nationaal als Europees, het toneel bevolken. In de politicologie en politieke sociologie wordt de grote populariteit van het intergouvernementele JBZ-terrein mede verklaard vanuit het perspectief van de *venue shopping* of de *policy laundering*. Dit perspectief stelt dat nationale staten, of preciezer de uitvoerende macht, het Europese beleidsveld opzoeken om te ontkomen aan beperkingen die bepaalde beleidsmaatregelen op het nationale niveau in de weg staan (Wolf 1999; Guiraudon 2000, 2003; Lahav & Guiraudon 2006; Lavenex 2006 & Boswell 2007). Guiraudon (2000) heeft het in dit verband over *venue shopping*: ministeries en overheidsorganisaties die een verticale ontsnapping zoeken van de 'domestic constraints on policymaking resulting from democratic, judicial and public scrutiny'.

Dit geldt bij uitstek voor die delen van de uitvoerende macht die zich met veiligheidsvraagstukken bezighouden, zoals politie en inlichtingendiensten, maar in toenemende mate ook voor de immigratieautoriteiten. Dit laatste is mede een gevolg van de steeds sterkere vervlechting van veiligheid en migratie in zowel het politieke taalgebruik als in de beleidsinstrumenten (zie bijv. Guild 2009; Boswell 2007). Of in de woorden van Lahav & Guiraudon (2006: 207): "International organisations and supranational participation legitimize the role of certain actors in policy-making that defend a logic of control." De Europese 'Ruimte van Vrijheid, Veiligheid en Rechtvaardigheid', zoals het JBZ-terrein sinds het verdrag van Amsterdam heet, biedt bepaalde overheidsorganisaties in ieder geval de 'ruimte' en 'vrijheid' die in de drukte van de nationale politiek en media vaak niet te vinden is. Of die strategie op de lange termijn ook houdbaar blijft, staat nog te bezien. De Europese instituties geven uiteraard weerwerk tegen een dergelijke instrumentele opvatting van Europa, net als de breed gedragen politieke overwegingen over het doel en de legitimiteit van de Europese samenwerking die vaak neerslaan in nieuwe verdragen en verdragswijzigingen. Zoals de volgende paragraaf laat zien, is de ontwikkeling van het beleidsterrein er dan ook een van een steeds verdere europeanisering en institutionalisering. Een ontwikkeling die volgens Lavenex (2006: 346) niet nieuw is: "(…) the EU has hitherto proved to be particularly

resistant to long-term instrumentalisation by national actors" (zie ook Broeders 2009c).

7.3 DE INSTITUTIONELE SETTING: VAN MAASTRICHT NAAR LISSABON

De wortels van het JBZ-beleidsterrein reiken terug tot in de jaren zeventig als de eerste samenwerking op het gebied van de strijd tegen het – dan nog hoofdzakelijk Europese – terrorisme tot stand komt in de intergouvernementele Trevi-groep. In de jaren daarna ontstaan er vele intergouvernementele en informele werkgroepen waarin vertegenwoordigers van de Europese lidstaten problemen op het gebied van immigratie, politiesamenwerking en terrorisme bespreken en naar grensoverschrijdende oplossingen zoeken (WRR 2003). Veel van het huidge JBZ-terrein is oorspronkelijk buiten de structuren van de EG/EU ontstaan, met als meest prominente voorbeeld het Schengenverdrag, en is vanaf 1992 met vallen en opstaan opgenomen in de officiële structuren van de EU. Door de tijd heen zijn de institutionele verhoudingen en de machtsverhoudingen tussen nationale overheden en Europese instellingen enerzijds en tussen Europese instellingen onderling anderzijds voortdurend in ontwikkeling. Het Verdrag van Lissabon is de meest recente wijziging in de onderlinge verhoudingen en de aanname van het Stockholmprogramma geldt als de meest recente koersbepaling voor het beleidsterrein als geheel.

Het Verdrag van Maastricht (1992) wordt gezien als het formele, in een verdrag vastgelegde, begin van de samenwerking inzake JBZ en dus ook inzake mobiliteit en migratie. De pijlerstructuur die met dit verdrag van de Europese Unie (1992) werd ingevoerd is van grote invloed geweest op de rol en positie van de verschillende politieke actoren en, daarmee, op de ontwikkeling van het terrein van Justitie en Binnenlandse Zaken. Dit beleidsterrein – justitiële samenwerking, politiesamenwerking en samenwerking op het gebied van asiel en migratie – werd vanwege gevoeligheden over soevereiniteit en autonomie opgenomen in de derde pijler van de EU.[2] De samenwerking in de derde pijler is intergouvernementeel van aard, wat betekent dat de normale Europese besluitvormingsprocedures, zoals die gelden in de eerste pijler, niet van toepassing zijn. De commissie heeft geen alleenrecht van initiatief, het Europees Parlement wordt alleen 'geconsulteerd' en kan niet meebeslissen (de zogenaamde codecisie) en het Hof van Justitie is niet bevoegd om zich over het beleid uit te spreken. Dat betekent dat de lidstaten in grote lijnen de dienst uitmaken. De JBZ-raad waarin, afhankelijk van het onderwerp, de ministers van Binnenlandse Zaken en/of die van Justitie van de lidstaten zitting hebben, bepalen de koers en invulling van het beleid. De stemmingen moeten bovendien unaniem zijn, wat het intergouvernementele karakter van de samenwerking onderstreept. Het intergouvernementele karakter in combinatie met het feit dat op dit nieuwe terrein een heel ander soort 'diplomaat' zijn intrede in Europa doet (grensbewakers,

politie, opsporingsdiensten, maar ook rechters en openbare aanklagers) maakten van het JBZ-terrein een ondoorzichtig en geheimzinnig beleidsproces, waarbij de nadruk bovendien vaak op restrictief en op veiligheid gericht beleid ligt (Mitsilegas, Monar & Rees 2003; Peers 2000; Koslowski 1998).

Met het Verdrag van Amsterdam (1998) veranderde een deel van het plaatje: de Schengenverdragen werden in het EU-verdrag opgenomen en het JBZ-terrein werd gesplitst: immigratie, asiel, buitengrenzen en justitiële samenwerking op het gebied van civiel recht werden in de communautaire eerste pijler ondergebracht, terwijl politiesamenwerking en justitiële samenwerking betreffende strafrecht in de intergouvernementele derde pijler achterbleven (WRR 2003). Voor die delen van het JBZ-terrein – dat sinds Amsterdam officieel de Ruimte van Vrijheid, Veiligheid en Rechtvaardigheid heet – die in de communautaire eerste pijler zijn opgenomen, gold een overgangsperiode waarin de samenwerking toch intergouvernementeel bleef. De Europese Commissie kreeg wel al vrij snel de rol toebedeeld om met initiatieven te komen, maar moest die rol formeel delen met de lidstaten en had daarmee een beperkte bewegingsruimte. Sinds de europeanisering van JBZ is er zeer veel politieke en beleidsactiviteit geweest. Jörg Monar, die jaarlijks het overzicht JBZ in de *Annual Review* van het *Journal of Common Market Studies* schrijft, houdt daarin ook een jaarlijkse hitlijst met het aantal door de Raad aangenomen teksten bij. De voorlopige piek lag in 2007 met 164 teksten, maar de productie is in elk jaar hoog te noemen (Monar 2008). Geheel in lijn met het informele en vaak ondoorzichtige karakter van de JBZ-samenwerking, is dat lang niet altijd 'wetgeving', maar juist vaak 'soft law' of andere meer informeel sturende teksten. In de laatste jaren neemt de wetgeving, dankzij de institutionalisering van het terrein, wel toe.

In december 2009 trad het Verdrag van Lissabon in werking, dat als 'opvolger' van het in de Franse en Nederlandse referenda afgewezen 'grondwettelijke' verdrag geldt. Dit verdrag brengt grote veranderingen met zich mee voor het JBZ-terrein. Sterker nog, verreweg de meeste verdragswijzigingen zijn volgens Monar (2010: 158) gerelateerd aan dit beleidsterrein dat ook met stip steeg in de lijst van *fundamental treaty objectives*. Met het Verdrag van Lissabon komt er een einde aan de pijlerstructuur van de EU, hetgeen betekent dat het hele JBZ-terrein dezelfde (klassieke) EU-wetgeving en instrumenten hanteert. Bovendien worden de normale EU-procedures, codecisie voor het Europees Parlement en stemmen met een gekwalificeerde meerderheid in de Raad, nu ook van toepassing op de (meeste) onderwerpen uit de oude derde pijler. Ook wordt de bevoegdheid van het Europese Hof van Justitie om JBZ-onderwerpen te beoordelen en controleren sterk uitgebreid. Bovendien maakt het verdrag het zogenaamde Handvest van Fundamentele Rechten juridisch bindend als een soort van *bill of rights* voor de Europese burger. Volgens Guild & Carrera (2010: 3) markeert dit verdrag dan ook niets minder dan een *before and after point* in de geschiedenis van het beleidsterrein.

Dat blijkt ook uit de verdeling van de portefeuilles van de nieuwe Commissie van Barroso die in 2010 aantrad. De portefeuille Justitie en Binnenlandse Zaken is daarin gesplitst: Reding is de nieuwe commissaris voor Justitie, grondrechten en burgerschap en Malmström neemt het commissariaat voor Binnenlandse Zaken op zich. De hoop en de verwachting is dat deze splitsing meer evenwicht zal brengen in de JBZ-beleidsvoorstellen en de balans tussen 'veiligheid' en 'rechtvaardigheid' die de afgelopen jaren te veel in het voordeel van de eerste uitsloeg, kan herstellen (Guild & Carrera 2010; Lieber 2010).

De verdragen schetsen de brede institutionele kaders waarin het JBZ-terrein zich heeft ontwikkeld en zijn van grote invloed op de mogelijkheden en de bewegingsruimte van de verschillende politieke actoren. De ambities voor het beleidsterrein zijn, met een start in 1999, vastgelegd in vijfjaarplannen die als agenda gelden en inzicht geven in het karakter en de beleidsambities voor de komende vijf jaar. In december 2009 stelde de Europese Raad het Stockholm-programma vast dat de grote lijnen uitzet voor de JBZ-aganda in de jaren 2010-2014.

7.3.1 DE JBZ-AGENDA: VAN TAMPERE NAAR STOCKHOLM

De ministers van Justitie en Binnenlandse Zaken stelden in 1999 het 'Tampere-programma' (2000-2004) vast en in 2004 werd het 'Den Haag-programma' vastgesteld dat van 2005 tot en met 2009 liep. Het Tampere-programma was ambitieus en kende bovendien een balans tussen de nadruk op veiligheid enerzijds en vrijheid en rechten anderzijds, hetgeen afweek van het daarvoor dominante geluid van 'Fort Europa' (WRR 2003). De schok van 9/11 en de nasleep daarvan liet zich voelen in het Den Haag-programma, waarin de balans weer stevig uitslaat naar de kant van de veiligheid. Het Den Haag-programma legde veel nadruk op het principe van de interoperabiliteit van systemen en het principe van beschikbaarheid (availability) als uitgangspunt voor data-uitwisseling tussen landen. Zowel Tampere als Den Haag werden in het geheim voorbereid en kwamen voor de buitenwereld als een duveltje uit een doosje. De tekst van Tampere werd openbaar een paar uur voordat de JBZ-raad hem aannam en 'Den Haag' was slechts enkele weken voordat het in de Raad als hamerstuk werd aangenomen, beschikbaar (Bunyan 2008). In december 2009 is het Stockholm-programma vastgesteld.
In vergelijking met de eerdere programma's, is de aanloop naar het Stockholm-programma iets openlijker geweest. In juni 2008 werd het rapport van de zogenaamde Future Group gepubliceerd waarin de eerste voorzetten voor het Stockholm-programma zijn opgenomen.[3] Deze Future Group is opgezet vanuit de lidstaten (de Raad) en bestond uit de ministers van Binnenlandse Zaken van Duitsland, Portugal, Slovenië, Frankrijk, Tsjechië en Zweden. Commissaris Franco Frattini (en na mei 2008 zijn opvolger Jacques Barrot) was ook vol lid van de groep. Daarnaast waren er een drietal waarnemers: het Verenigd Koninkrijk (om het *common law*-perspectief te vertegenwoordigen), de voorzitter van het

LIBE-comité[4] van het Europees Parlement en de directeur-generaal voor JBZ van het secretariaat van de Raad. Verscheidene zinsneden uit het rapport zijn in ieder geval opmerkelijk en geven inzicht in de denkwijze van de lidstaten. De huidige tijd wordt gekarakteriseerd als een *digital Tsunami environment* waarin het beschermen van privacy een haast onmogelijke opgave is. Om dit toch mogelijk te maken zijn *privacy enhancing technologies* absoluut noodzakelijk (Future Group 2008: 43). Hoe dat vorm moet krijgen wordt verder niet uitgewerkt.[5] Als één ding uit de tekst van dit rapport duidelijk wordt, is het wel dat technologie en data-uitwisseling als de weg van de toekomst worden gezien. De hele tekst ademt een sterk 'technovertrouwen'. De passage waarin de centrale rol van 'databanken en nieuwe technologieën' voor de toekomst van het JBZ-beleid wordt bevestigd, geeft een mooi beeld van de verhouding mens-machine in de ogen van de Future Group (2008: 18): "Even if technology can never completely replace the human factor, technological progress can provide the necessary means to optimise mobility, security and privacy simultaneously."

Het rapport van de Future Group was één stap in het proces dat in juni 2009 werd vervolgd in de vorm van de concepttekst van het Stockholm-programma (CEC 2009). Deze tekst is veel breder (want hij behandelt het hele JBZ-terrein) en anders van toon: veel meer aandacht voor gegevensbescherming en privacy en minder 'technovertrouwen'. Maar ook in deze meer zakelijke tekst blijven de hoofdlijnen van de technologisch ingeslagen weg overeind. De EU moet op termijn toe naar een *European Information Model* (blz. 15) en het voorstel om te komen tot een nieuw EU-agentschap dat het management van alle JBZ-databanken op zich kan nemen, dat al eerder was gedaan (CEC 2009b), wordt herbevestigd. SIS en VIS worden in de context van de taken van dit agentschap genoemd, net als het nog op te zetten Entry/Exit-systeem en het *registered traveller programme* die in 2015 operationeel zouden moeten worden (blz. 19). De Europese Toezichthouder voor Gegevensbescherming is in zijn opinie over dit stuk van de Commissie positief over de aandacht voor gegevensbescherming en privacy, maar benadrukt dat de toekomst van het JBZ-terrein niet *technology driven* vorm mag worden gegeven (EDPS 2009: 12). Het feit dat interoperabiliteit technisch mogelijk is betekent nog niet dat het ook gedaan moet worden. Doelbinding blijft een vereiste. De toezichthouder herhaalt zijn positie dat de noodzaak voor een Entry/Exit-systeem wat hem betreft niet is aangetoond (blz. 15) en verbaast zich over het feit dat biometrie, alomtegenwoordig in de nieuwe systemen, eigenlijk niet in de tekst wordt genoemd. Ook de analisten van de Brusselse denktank CEPS zagen in het concept een "(…) temptation inside the Commission to resolve the question of 'border controls' via a technological fix" (Guild & Carrera 2009: 7).

Tijdens de Europese Raad van 11-12 december 2009 namen de regeringsleiders de inmiddels tot 82 pagina's uitgedijde tekst van het Stockholm-programma aan (CEU 2009). In de uiteindelijke tekst ligt volgens Guild en Carrera (2010) de

nadruk sterker op de rechten van burgers (*a Europe of rights*) en minder op de veiligheid die lange tijd heeft gedomineerd. Waar het voorgaande Den Haag-programma nog uitging van het vinden van een balans tussen vrijheid en veiligheid, stelt het Stockholm-programma vrijheid voorop: "… the challenge will be to ensure respect for fundamental freedoms and integrity while guaranteeing security in Europe" (Guild & Carrera 2010: 5). Monar (2010: 158-159) wijst er echter wel op dat de voorgenomen implementatie voor uitwerkingen van individuele vrijheden (zoals de rechten van individuen in strafrechtprocedures) relatief vaag zijn en het zonder deadlines moeten stellen. Op andere gebieden – waaronder gegevensuitwisseling, terrorisme en de geïntegreerde grensbewaking – zijn de prioriteiten veel steviger geformuleerd. In combinatie met de institutionele wijzigingen als gevolg van het in werking treden van het Verdrag van Lissabon is hij evenwel relatief positief over de mogelijkheden voor het Stockholm-programma. "While in no way guaranteeing the necessary political will, the Lisbon Treaty provides the EU at least with an improved constitutional framework to deliver on the Stockholm Programme objectives"(Monar 2010: 159).

7.4 EERSTE GENERATIE DATABANKEN: MOEILIJKE MIGRANTEN IN BEELD

Verreweg de meeste datasystemen die de Europese Unie heeft ontwikkeld of aan het ontwikkelen is, zijn gerelateerd aan migratiecontrole. Naarmate de EU meer een vrij verkeer van personen binnen de buitengrenzen toestaat, neemt de noodzaak van een gezamenlijk immigratiebeleid toe. Niet in de zin van het nemen van juridische beslissingen over toelating of afwijzing van migranten – de lidstaten zijn niet bereid die bevoegdheid af te geven – maar wel in de zin van instrumenten voor migratiecontrole en gezamenlijk beleid aan de buitengrenzen van de EU.

Moderne technologie speelt al langer een belangrijke rol bij de controles van de uitgestrekte grenzen van de EU. Een stap verder zijn de recente plannen voor de ontwikkeling van EUROSUR, het European Border Surveillance System, waarbij alle nationale surveillancesystemen aan voornamelijk de blauwe zuidgrens van de Unie aan elkaar gekoppeld gaan worden (Jeandesboz 2008). Een andere groep instrumenten bestaat uit grote databanken waarin de persoonsgegevens van migranten worden opgeslagen met migratiecontrole als doel. In eerste instantie zijn er voornamelijk databanken ontwikkeld die de risicogroepen van migranten 'beheersbaar' moeten maken. Daarbij gaat het om asielzoekers, illegale migranten en migranten die op een kortlopend visum inreizen – vanwege het risico van illegaliteit. De voornaamste databanken voor deze groepen zijn: het Schengen Informatie Systeem (SIS I en II), het Visum Informatie Systeem (VIS) en het Eurodac-systeem.

7.4.1 SCHENGEN INFORMATIE SYSTEEM I EN II

De Schengen Conventie van 1990, die in essentie een lange lijst is van compenserende maatregelen voor het vrije verkeer van personen dat in het Schengen Verdrag van 1985 is vastgelegd, voorziet ook in de introductie van het Schengen Informatie Systeem (SIS). De conventie legt de basis voor een breed scala aan instrumenten bedoeld om grote groepen mensen te registreren en te volgen die van, naar en binnen het gebied van de Schengenstaten bewegen (Mathiesen 2001). Het systeem slaat informatie op over zowel objecten als personen. Zowel in de categorie personen als in de categorie objecten is het grootste deel van de opgeslagen informatie gerelateerd aan immigratie. Hoewel het doel van het SIS is gerelateerd aan 'orde en veiligheid', lijkt de belangrijkste preoccupatie van het systeem toch (illegale) immigratie te zijn (Guild 2001). Van de vijf categorieën personen die in het systeem kunnen worden ingevoerd, wordt het leeuwendeel geregistreerd onder artikel 96 (personen die de toegang tot het Schengengebied ontzegd moet worden omdat ze ongewenste vreemdelingen zijn).[6] De voornaamste categorie objecten in het SIS is die van de 'verloren en gestolen identiteitsdocumenten'. De informatie die over personen in het systeem mag worden ingevoerd is beperkt: voor- en achternaam, bekende aliassen, eerste letter van de tweede naam, geboortedatum en -plaats, onderscheidende fysieke kenmerken, sekse, nationaliteit, of de persoon als gewapend en/of gevaarlijk wordt beschouwd, de reden voor het SIS-rapport en welke maatregelen getroffen moeten worden. Dat laatste heeft te maken met het feit dat het SIS een zogenaamd *hit/no hit*-systeem is: een persoon wordt in het systeem ingevoerd en als hij of zij wordt herkend (hit), antwoordt het systeem met een instructie, zoals 'houd deze persoon aan' (De Hert 2004: 40).

Volgens het Duitse ministerie van Binnenlandse Zaken waren er in 2005 meer dan 30.000 terminals in het Schengengebied die toegang tot het SIS hadden. Het SIS is een relatief sober systeem, met slechts beperkte mogelijkheden voor de gebruiker, hetgeen de reden is dat de lidstaten een tweede systeem (SIRENE – een acroniem afgeleid van *Supplément d'Information Requis a l'Entrée Nationale*) aan deze database hebben gekoppeld. In de dagelijkse praktijk functioneert het SIS als een index voor SIRENE, dat wel de mogelijkheid biedt om aanvullende informatie zoals vingerafdrukken en foto's uit te wisselen. Op nationaal niveau zijn de contactpunten voor SIS en SIRENE dan ook meestal aan dezelfde organisatie toevertrouwd.

Hoewel SIRENE soms wel de 'operationele kern van Schengen' wordt genoemd, is er in de Schengen Conventie geen enkele referentie naar het systeem te vinden (Justice 2000: 19).

Het SIS bleek een populair beleidsinstrument. De snelle groei van het aantal Schengenlidstaten, ook van buiten de EU door middel van associatieverdragen[7], leidde ertoe dat al in december 1996 besloten werd om een tweede generatie van

het SIS te ontwikkelen om het groeiend aantal deelnemers te accommoderen en om nieuwe functies aan het systeem toe te voegen. Het nieuwe systeem, SIS II, had al operationeel moeten zijn, maar verschillende vertragingen hebben de datum telkens naar achter verschoven. In 2010 werd de datum wederom verschoven, nu naar het eerste kwartaal van 2013 (CEC 2010b). Het vooruitzicht van een nieuwe generatie van het systeem bracht de lidstaten in de verleiding om gedurende de ontwikkelingsfase steeds nieuwe 'verlanglijstjes' op tafel te leggen. De Gemeenschappelijke Controle-Autoriteit Schengen vatte het karakter van die verlanglijstjes treffend samen in twee trends: één trend om meer informatiecategorieën aan het systeem toe te voegen, en dan in het bijzonder biometrische informatie, en een tweede trend om nieuwe organisaties (zoals Europol) toegang te verlenen tot de informatie in het systeem (Joint Supervisory Authority of Schengen 2004: 14). Er waren ook voorstellen om de verschillende (immigratie) datasystemen van de EU aan elkaar te linken en in sommige documenten was zelfs een pleidooi te lezen voor het opgaan van het SIS in één groot op te richten Europees Informatie Systeem (Brouwer 2004: 5). De Europese Commissie is vrij pragmatisch omgegaan met de onzekerheid over de uitkomst van de politieke onderhandelingen over de functies van het nieuwe systeem. In 2003 schreef de Commissie dat SIS II, hangende het besluit van de Europese Raad, "must be designed and prepared for biometric identification to be implemented easily at a later stage, once the legal basis, allowing for the activation of such potential functionalities, has been defined" (CEC 2003: 16). Met andere woorden, de politiek hoeft alleen maar te volgen in de voetstappen van de technologie, een zorg die in 2008 werd geuit door de Europese Toezichthouder voor Gegevensbescherming: "One can safely assume that technical means will be used, once they are made available; in other words, it is sometimes the means that justify the end (. . .) legal changes quite often confirm practices which are already in place" (geciteerd in Balzacq 2008: 78). Het definitieve besluit over de ontwikkeling en functies van SIS II dat in januari 2007 van kracht werd, geeft duidelijkheid over de nieuwe functies en andere uitbreidingen. De belangrijkste uitbreiding betreft de opname van biometrische gegevens in de databank. Voorlopig gaat het om de opname van vingerafdrukken en foto's, maar volgens een onderzoeksrapport van de Britse House of Lords zou het systeem ook geschikt zijn voor irisscans en DNA, als daarvoor in de toekomst de wettelijke ruimte wordt gecreëerd (House of Lords 2007: 20, n. 43). Met de opname van biometrische gegevens verandert het karakter van het SIS aanzienlijk.

Sweeping searches waarbij een vingerafdruk wordt vergeleken met alle opgeslagen vingerafdrukken worden nu mogelijk. Dat geeft het systeem veel meer dan zijn voorganger het karakter van een opsporingssysteem, hetgeen het aantrekkelijk maakt voor verschillende (veiligheids)instanties, maar ook zeer hoge eisen stelt aan de kwaliteit van de biometrische gegevens die worden opgeslagen. De Europese Toezichthouder heeft al gewaarschuwd voor overschatting van de betrouwbaarheid van biometrie (in House of Lords 2007: 20, zie ook Van der Ploeg &

Sprenkels 2009). Ook het aantal organisaties dat toegang krijgt tot de tweede generatie van het SIS is toegenomen; zo hebben Europol en Eurojust inmiddels toegang gekregen tot delen van de database (zie Balzacq 2008) voor een uitgebreide analyse van de toegang van veiligheids- en inlichtingenorganisaties tot EU-migratiedatabases).

De interactie tussen het systeem en de lidstaten is op meerdere punten onhelder, in die zin dat bepaalde zaken niet of nauwelijks officieel zijn vastgelegd die echter wel van grote invloed zijn op het dagelijks gebruik van het systeem. Die onduidelijkheid heeft op haar beurt weer gevolgen voor een toch al moeizaam toezicht op het functioneren van het systeem. Twee voorbeelden. Niet alleen Europol en Eurojust krijgen beperkt toegang tot het SIS II, maar er zijn ook lijsten toegevoegd met nationale autoriteiten die toegang tot het systeem krijgen. Sommige van die omschrijvingen zijn echter dusdanig generiek dat het nagenoeg onmogelijk is om te weten welke organisaties nu (legitiem) toegang tot het systeem hebben gekregen (Balzacq 2008). Een ander voorbeeld is de manier waarop met signaleringen in het SIS (II) wordt omgegaan. Het SIS gaat uit van het beginsel van de wederzijdse erkenning van nationale besluiten, ook wel het 'interstatelijk vertrouwensbeginsel' genoemd. Een signalering die door een andere lidstaat is ingevoerd, wordt door Nederland in principe niet ter discussie gesteld. Gechargeerd gesteld: als het SIS zegt 'geen visum verlenen', dan wordt er geen visum verleend. De criteria die verschillende Schengenlanden voor een signalering hanteren, lopen echter sterk uiteen en zijn bovendien onvoldoende inzichtelijk voor rechters en toezichthouders (Brouwer 2009). Er is, met andere woorden, via de band van de wederzijdse erkenning geharmoniseerd op het niveau van het systeem, maar niet op het niveau van het onderliggende beleid. Ook in de verordening voor SIS II is er niet voor gekozen om de criteria voor opname in SIS te harmoniseren. Toezicht op deze zaken, via toezichthouders of via de rechter, is dus uitermate ingewikkeld. Het SIS-systeem heeft dus trekjes van wat wel 'automatische besluitvorming' wordt genoemd, hoewel overheden die term altijd zorgvuldig vermijden. Als signaleringen gebaseerd zijn op het beleid van een andere lidstaat en niet ter discussie worden gesteld, maar eenvoudigweg worden uitgevoerd, heeft dat een 'automatische component'. Uit recent onderzoek van de Nationale Ombudsman (2010) blijkt bovendien dat de Koninklijke Marechaussee en de IND een relatief 'automatische procedure' hanteren om mensen te signaleren (zie ook Besters & Brom 2010). Zonder echte individuele beoordeling zet de IND mensen in het SIS voor relatief kleine incidenten als een visum dat een week is verlopen (wat strikt genomen natuurlijk in overeenstemming is met de wet) zonder daarin de context mee te nemen. Dat heeft grote gevolgen, aangezien een signalering in het SIS bij een volgend bezoek aan de EU als standaardreactie een weigering van toegang oplevert, of zelfs een verblijf in vreemdelingendetentie. In de SIS II-verordening is overigens wel als nieuw criterium opgenomen dat "een signalering gebaseerd moet zijn op een individuele beoordeling en iemand dus niet op basis van alge-

mene criteria in het SIS II opgenomen kan worden" (Brouwer 2009: 20). De Nederlandse praktijk is dus niet in overeenstemming met de (komende) regels.

De gang van zaken rondom de technische ontwikkeling van het SIS II geeft zowel technisch als politiekorganisatorisch sterk te denken. Oneerbiedig gezegd, is de ontwikkeling van het systeem een puinhoop geweest. De ontwikkeling duurt al ongeveer dertien jaar en heeft ettelijke miljoenen meer gekost dan voorzien. In 2009 gaven diplomaten aan dat het systeem al tussen de 60 en 80 miljoen euro had gekost, veel meer dan de oorspronkelijk begrote 23 miljoen euro.[8] In 2010 stond de teller zelfs al op 90 miljoen euro (cf. Besters & Brom 2010). Dat had te maken met de slechte prestaties van de uitvoerders, de politieke aansturing en met de slechte aansturing vanuit de Commissie. In ieder geval is duidelijk dat de ontwikkeling van het SIS II de ontwikkeling van een *moving target* is. Gaandeweg de rit zijn de functionaliteiten uitgebreid en het aantal lidstaten dat aangesloten moest worden groeide ook sterk. Door de uitbreiding van Schengen in 2007 met 9 nieuwe lidstaten – waar het SIS niet op berekend was – moest een noodsprong worden gemaakt en werd een update van het oude SIS gemaakt, onder de welluidende naam SISone4All (er was overigens al een eerdere update, het zogenaamde SIS 1+). Dat alternatieve systeem draait nu al een tijdje en, gezien de vernietigende resultaten van een technische test van het centrale systeem van het SIS II in 2008, zal dat nog wel even zo blijven. Bij deze test kwam een aantal grote problemen aan het licht: gegevens uit het nationale en het centrale deel kwamen niet overeen, registraties verdwenen of kwamen dubbel voor en het centrale systeem was niet bestand tegen de invoer van de grote hoeveelheid gegevens (CEC 2009c: 5). Het capaciteitsprobleem is het grootst: het centrale deel is in 2004 ontworpen om 15 miljoen gegevens te kunnen verwerken. Op 1 januari 2008 stond het aantal signaleringen echter al op 23 miljoen (Brouwer 2009: 9). In de laatste update van de Commissie over de plannen voor het SIS II is de capaciteit voor het systeem flink omhoog geschroefd. Wanneer het systeem in 2013 on line zou gaan, moet het 70 miljoen meldingen op kunnen slaan en dat aantal moet bovendien naar 100 miljoen kunnen worden bijgesteld zonder technologische verandering (CEC 2010b: 4). Ondanks alle vertragingen en problemen met het SIS II, hebben de lidstaten toch besloten om door te zetten vanwege alle investeringen die al gedaan zijn. Op de achtergrond ligt al wel een plan klaar om een nieuwe versie op basis van het oude systeem te maken, het zogenaamde SIS 1+ renewal and evolution (SIS 1+ RE), dat echter is verworpen vanwege de politieke *lock* in op het SIS II. De toekomst van het systeem blijft echter onzeker, getuige het diplomatengrapje waarin sprake is van SIS 14Ever.

7.4.2 EURODAC

Het Eurodac-systeem is de database die de Conventie van Dublin 'handen en voeten' moet geven. Deze conventie, inmiddels omgezet in een EU-besluit, is

bedoeld om vast te stellen welke lidstaat verantwoordelijk is voor een asielaanvraag en moet ook het zogenaamde *asielshoppen* (een asielverzoek doen in meerdere EU-lidstaten) zien te voorkomen. Om te bepalen of een asielzoeker al elders een asielverzoek heeft ingediend, werd Eurodac (*European Dactylographic System*) opgezet: een Uniebreed datasysteem dat alle asielaanvragen in de Unie vastlegt en vergelijking op basis van vingerafdrukken mogelijk maakt. De ontwikkeling van dit systeem kent een bewogen politieke geschiedenis die begon in 1991 met de beslissing het systeem te ontwikkelen, in 2003 leidde tot de ingebruikname en voortduurt in het huidige tijdperk van 'veiligheid en terrorisme' (zie Aus 2006 voor een uitgebreide analyse). In de periode tussen 1991 en 2003 is het bereik van Eurodac behoorlijk opgerekt. Oorspronkelijk zou de database alleen de vingerafdrukken van asielzoekers bevatten, maar in 1998 oefende Duitsland zware druk uit om ook illegale migranten in Eurodac op te nemen. In de 'parallelle wereld' van de ontwikkeling van het SIS was de wens om de vingerafdrukken van illegale migranten op te slaan ook al ter tafel gekomen (Brouwer 2002: 235), maar omdat dit in de eerste generatie van dat systeem niet mogelijk was, moesten de lidstaten hun heil elders zoeken. Mathiesen (2001: 18) stelt dan ook dat de 'geschiedenis van het afnemen van de vingerafdrukken van 'illegale immigranten' laat zien hoe vervlochten Schengen en Eurodac zijn'.

Eurodac ging in januari 2003 online met een lege database en is sindsdien snel volgelopen met in totaal drie categorieën van personen en vingerafdrukken. Categorie 1 bevat de vingerafdrukken van alle individuen ouder dan 14 jaar die in een van de EU-lidstaten asiel hebben aangevraagd. Dit zijn de vingerafdrukken die nodig zijn om aan de doelstellingen van 'Dublin' te voldoen. Categorie 2 bevat de vingerafdrukken van illegale migranten die werden aangehouden bij een illegale grensoversteek en categorie 3 bevat de vingerafdrukken van illegale migranten die in een van de lidstaten werden aangehouden. De vingerafdrukken van categorie 3 worden gecontroleerd ten opzichte van de opgeslagen vingerafdrukken van de eerste twee categorieën, maar worden niet opgeslagen. Bovendien is het gebruik van deze categorie optioneel; lidstaten bepalen zelf of ze er gebruik van maken. Met name deze laatste categorie illustreert de groeiende interesse van (een aantal) lidstaten om deze moderne surveillancetechnieken toe te passen op het probleem van illegaal verblijf. Net als het SIS is Eurodac een hit/no hit-systeem dat slechts beperkte informatie bevat.

Het grootste deel van de invoer in Eurodac betreft de asielaanvragen in de lidstaten van de Europese Unie en het grootste deel van de 'hits' betreft de detectie van dubbele, of zelfs meervoudige asielverzoeken (in 2006 was er zelfs een persoon die in totaal 13 aanvragen had gedaan), de functie waar het systeem voor is opgezet. Als instrument om asielshoppen in kaart te brengen lijkt het systeem dus goed te functioneren, aldus de Commissie in de evaluatie van Eurodacs eerste drie operationele jaren (CEC 2007). Dat zegt overigens nog weinig over de vraag of

landen ook in de praktijk daadwerkelijk 'Dublin-aanvragers' aan elkaar overdragen. Het gebruik van categorie 3 kan op veel enthousiasme rekenen onder een selecte groep landen. De snel oplopende aantallen 'hits' met de data van categorie 3 – van 1.181 in 2003 naar 15.612 in 2006 – zijn een indicatie dat Eurodac een belangrijk instrument aan het worden is voor de Europese 'strijd tegen illegale immigratie'. Illegale immigranten die een asielgeschiedenis hebben (vanaf 2003) kunnen door middel van controle van hun vingerafdruk in het Eurodac-systeem worden gekoppeld aan een asieldossier dat zich bevindt in de staat waar ze die aanvraag hebben gedaan. Dat dossier betekent voor de autoriteiten van het land dat de controle uitvoert een bron van informatie over identiteit en land van herkomst. Deze informatie, waar veel illegale migranten in alle toonaarden over zwijgen, is noodzakelijk om een uitzetting naar het land van herkomst mogelijk te maken. Met andere woorden, Eurodac kan illegale migranten 're-identificeren' (Broeders 2007). In de praktijk is slechts een beperkt aantal landen verantwoordelijk voor het stijgende gebruik van de data van categorie 3. Landen als Nederland, Duitsland en Groot-Brittannië waar illegaliteit als een groot politiek probleem wordt gezien, zijn de grote gebruikers van dit deel van het systeem. De 'populariteit' van deze categorie is de Europese Commissie ook niet ontgaan. In haar evaluatie stelt de Commissie dan ook voor om deze data voortaan ook in het systeem op te slaan, in plaats van ze alleen maar te controleren tegen de data van categorie 1. In dezelfde evaluatie wordt ook het voorstel gedaan om uit te zoeken wat de mogelijkheden zijn om het bereik van Eurodac te vergroten in het licht van "law enforcement purposes and as a means to contribute to the fight against illegal immigration" (CEC 2007: 11). Met andere woorden, ook aan dit systeem wordt (nog steeds) getrokken om steeds meer en andersoortige functies te vervullen dan die waarvoor het systeem oorspronkelijk is opgezet. De ontwikkeling van Eurodac is een schoolvoorbeeld van function creep.

7.4.3 VISUM INFORMATIE SYSTEEM

Het Visum Informatie Systeem (VIS) is de logische volgende stap in de ontwikkeling van het netwerk van EU-migratiedatabases. 'Ongewenste' migranten reizen immers niet alleen illegaal of via de asielprocedure in. Een groot deel van de latere populatie illegale migranten komt volkomen legaal naar de Europese Unie op een toeristenvisum en wordt pas illegaal als de geldigheid van dit visum verloopt: de zogenaamde *overstayers* in het Europese jargon. In de conclusies van het voorzitterschap van de Europese Raad van Sevilla in 2002 wordt dan ook onder het kopje 'maatregelen om illegale immigratie tegen te gaan' opgeroepen tot 'de introductie, zo spoedig mogelijk, van een gemeenschappelijk identificatiesysteem voor visagegevens' (CEU 2002: 8). Dat systeem, het VIS, is nu in ontwikkeling en wordt geacht in 2012 volledig operationeel te zijn in alle consulaten en bij alle grensovergangen (Hobbing & Koslowski 2009: 8). Het VIS moet een aantal doelen gaan dienen, zoals de verbetering van de uitvoering van het gemeenschappelijk visum-

beleid en de consulaire samenwerking door middel van data-uitwisseling over aanvragen en besluiten, het tegengaan van visa-shopping en visumfraude. Verder wordt het systeem ook geacht bij te dragen aan het bepalen welke lidstaat verantwoordelijk is voor een asielaanvraag (een 'Dublin-taak' dus) en dient het, geheel in lijn met de tijdsgeest, ook bij te dragen aan het voorkomen van bedreigingen voor de interne veiligheid van de lidstaten. Als het om ongewenste migratie gaat, heeft het systeem de volgende identificatietaak: "to assist in the identification of any person who may not, or may no longer fulfill the conditions for entry, stay or residence of the territory of the Member States" (CEU 2007). Met andere woorden, ook dit systeem heeft een specifieke taak waar het gaat om het 're-identificeren' van illegale migranten.

Net als Eurodac zal het Visum Informatie Systeem starten met een lege database. De data die het systeem gaan vullen zijn veel minder minimaal dan de data die in Eurodac en SIS worden opgeslagen. In de eerste plaats gaat het om de basisinformatie over de aanvrager (eigenlijk een digitale versie van het aanvraagformulier), en informatie over de data waarop visa zijn aangevraagd, verstrekt, geweigerd, geannuleerd, ingetrokken of verlengd. De basisinformatie bevat ook gegevens over de persoon of het bedrijf dat de visumaanvraag ondersteunt en die vaak verantwoordelijk werden gesteld voor de kosten van het levensonderhoud van de aanvrager gedurende zijn of haar verblijf. Dat betekent dat in dit systeem de familie en bedrijven die 'instaan' voor de aanvrager duidelijk in beeld zijn en ook worden geregistreerd en opgeslagen. Als tweede categorie zal het VIS biometrische data opslaan: van elke aanvrager zullen 10 vingerafdrukken en een foto in het systeem worden opgeslagen. Volgens de Commissie wordt het VIS daarmee het grootste 10-vingerafdruk systeem in de wereld.

De opzet van het VIS is dus ambitieus. In de *feasability study* van de Commissie ging men uit van een systeem dat minimaal 27 lidstaten, 12.000 VIS-gebruikers en 3.500 consulaire posten moest kunnen verbinden. Uitgangspunt daarbij was de schatting dat de EU-lidstaten jaarlijks ongeveer 20 miljoen visumaanvragen zouden afhandelen (CEC 2003: 26). In het persbericht dat de Commissie deed uitgaan toen het Parlement en de Europese Raad in 2007 politieke overeenstemming over het systeem bereikten, was te lezen dat het VIS data kan opslaan tot een aantal van 70 miljoen personen. De toverwoorden bij de ontwikkeling van het VIS zijn 'interoperabiliteit' en 'synergie', met name met het SIS II, dat in technische zin exact hetzelfde 'DNA' heeft. De database, de technische lay-out en zelfs de fysieke locatie voor de centrale database (de SIS-bunker in Straatsburg) zijn hetzelfde. De systemen delen in de ontwikkelingskosten van een 'gemeenschappelijk technisch platform', zodat de databanken goed op elkaar aansluiten en klaar zijn voor eventuele toekomstige interoperabiliteit en data-uitwisseling. Nu is daarover nog geen politieke overeenstemming en blijven de twee systemen 'aparte containers', maar de wens om de verschillende EU-immigratiedatasystemen te koppelen of zelfs

samen te voegen is, zoals eerder opgemerkt, duidelijk aanwezig. Deze geluiden worden ook gehoord bij de ontwikkeling van het VIS, de andere 'te koppelen' databases zijn dan steevast Eurodac en het SIS II. De vraag van een bredere toegang, met name voor veiligheidsautoriteiten, tot het VIS speelt ook volop en bracht de Europese toezichthouder tot de waarschuwing dat het VIS is ontwikkeld 'ten behoeve van het Europese visumbeleid, niet als een instrument voor ordehandhaving en veiligheid' (EDPS 2006: 2).

Om de interoperabiliteit tussen de verschillende biometrische systemen te vergroten is de EU begonnen met de opzet van een Biometric Matching System (BMS). Dit BMS moet de krachtige zoekmachine worden die de biometrie van de aanvrager en de centraal opgeslagen biometrische gegevens met elkaar gaat matchen. Voorlopig is de BMS gekoppeld aan het VIS, maar in de plannen van de Commissie is al voorzien om ook Eurodac en het SIS II op BMS te laten draaien (Hobbing & Koslowski 2009: 9). Het nieuwe systeem wordt ontwikkeld door Sagem en Accenture, terwijl Eurodac op een Amerikaans systeem draaide.[9] Ook het Entry/Exit-systeem zal – als en wanneer het komt – op het BMS gaan draaien waarmee de technologische infrastructuur tussen al deze systemen gelijk is getrokken. Dat maakt koppelingen en interoperabiliteit tussen deze systemen mogelijk – als daar een politiek besluit toe wordt genomen – en makkelijk.

7.4.4 TUSSENCONCLUSIE

Een paar trends kunnen op basis van het bovenstaande beeld al geschetst worden. De digitale controle in Europa is in eerste instantie uitgerold voor specifieke groepen. Illegalen en asielzoekers zijn, naast specifieke groepen criminelen, de eerste groepen die in databanken worden opgeslagen. In eerste instantie gaat het daarbij om *reactief* beleid (in het SIS werden alleen mensen 'opgeslagen' die ongewenste vreemdeling zijn verklaard). Naarmate de tijd en technologie vordert, worden er steeds meer mensen opgeslagen zonder dat deze migranten al iets 'gedaan' hebben. Het gaat er dan om dat een deel van hen iets gedaan heeft (al elders asiel aangevraagd heeft), maar met name om wat zij zouden kunnen doen (in de illegaliteit verdwijnen bijvoorbeeld). Daarmee krijgen beleid en databank al veel meer een *preventief* karakter: ze registreren personen om wat zou kunnen gebeuren.

Met de toename van terroristische dreiging en de keuze om ook daarvoor de mogelijkheden van de digitale techniek ten volle te willen benutten, veranderen er nog een paar zaken. In de eerste plaats raken de categorieën 'immigratiebeleid' en 'interne veiligheid' met elkaar vermengd. Voor een belangrijk deel – en in eerste instantie – is dat aanbodgestuurd. Er zijn eerst immigratiedatabanken ontwikkeld en daar is later een doelstelling van terrorismebestrijding aan gekoppeld. Op de voet gevolgd door georganiseerde misdaad (en het zou niet al te veel verbazing wekken als die categorie steeds meer uitgebreid wordt naar andere vormen van

criminaliteit). Een klassiek geval van function creep, maar ook een geval van 'de gelegenheid maakt de dief': de data zijn er, dus waarom zouden we die niet gebruiken? Dat maakt het politiek ook verkoopbaar, want de omgekeerde redenatie zou veel minder makkelijk te verkopen zijn ("we willen terrorisme en/of criminaliteit bestrijden en daarom willen we vingerafdrukken van asielzoekers en migranten met een toeristenvisum afnemen"). Later wordt de doelstelling van terrorismebestrijding en criminaliteit steeds meer vanaf het begin meegenomen. In aansluiting daarop kan, in de tweede plaats, gezegd worden dat de Europese overheden het digitale net steeds wijder uitgooien. Er worden veel data verzameld, over veel personen – het overgrote merendeel onverdacht – om een relatief kleine groep te kun-nen opsporen. *Dragnet policies* wordt dat in de surveillancestudies genoemd (Lyon 2003). Daarmee worden opsporing en migratiecontrole dus steeds meer een kwestie van vissen in de data. In de derde plaats betekent de verbreding van de groep die onder toezicht staat ook dat de Europese burger in toenemende mate in het vizier van de dataverzamelende autoriteiten komt. Via de migranten, de criminelen en de terroristen is nu de tijd aangebroken dat de 'gewone' (Europese) burger en zijn internationale mobiliteit in kaart wordt gebracht.

7.5 TWEEDE GENERATIE DATABANKEN: IEDEREEN IN BEELD

De tweede generatie systemen markeert in sterke mate de verschuiving van datasystemen voor alleen de (problematische) migranten als doelgroep naar alle reizigers als doelgroep. Bij elkaar opgeteld zijn de voorstellen een *catch-all*-strategie voor de mobiliteit van alle personen die de buitengrenzen van de EU passeren. Een aantal ontwikkelingen is daarbij van belang. Zowel het voorstel voor een PNR-systeem als het biometrische paspoort dat nu in heel Europa wordt ingevoerd, heeft veel te maken met ontwikkelingen in de Verenigde Staten die Europa in een bepaalde richting drongen (paspoort) of verleidden tot het willen nabootsen van Amerikaanse 'oplossingen' (PNR). Ook de voorstellen voor nieuwe systemen als onderdeel van het door de Europese Commissie in 2008 gelanceerde *border package* (CEC 2008) zijn sterk geënt op de systemen die in de jaren daarvoor al in de Verenigde Staten waren ontwikkeld of geagendeerd. De systemen die in dit document van de Commissie – slechts tien pagina's die de gemoederen al tijden bezighouden – worden geschetst, zoals het Entry/Exit-systeem, zijn gemodelleerd naar systemen (en plannen) elders in de wereld, in het bijzonder de VS en Australië.

7.5.1 PASSENGER NAME RECORDS (PNR-DATA)

PNR-data zijn de gegevens die luchtvaartmaatschappijen van hun passagiers opslaan. Daarbij gaat het om meer dan alleen naam en stoelnummer, maar ook om telefoonnummers, adresgegevens, bank- en creditcardgegevens en de maaltijdvoorkeuren. Deze PNR-data werden een zaak toen de Verenigde Staten als onder-

deel van de antiterrorismewetgeving alle luchtvaartmaatschappijen verplichtte deze data ter beschikking van de autoriteiten te stellen voordat een vliegtuig op een Amerikaanse luchthaven landt (De Hert & De Schutter 2008; Mitsilegas 2009). Deze Amerikaanse eis kwam in conflict met de Europese wetgeving voor de bescherming van persoonsgegevens die het aan Europese bedrijven niet toestaat dergelijke gegevens over te dragen zonder toestemming van de passagiers. De Amerikaanse druk op de luchtvaartmaatschappijen was enorm – de boetes zijn zeer hoog en worden per passagier opgelegd – en de Europese Commissie moest met een oplossing zien te komen. De oplossing werd dat de relevante Amerikaanse autoriteiten door de Europese Commissie *adequate* werden verklaard in termen van het niveau van gegevensbescherming (Mitsilegas 2009). Het *adequacy criterion* bepaalt of gegevensuitwisseling met een derde partij in principe mogelijk is. De PNR-overeenkomst met de Verenigde Staten is met het nodige kunst- en vliegwerk, inclusief een interim-overeenkomst, in elkaar gezet. Ondertussen ging de uitwisseling van gegevens uiteraard door en de uiteindelijke overeenkomst moet worden gezien als een codificatie van een staande praktijk. Het Europees Parlement is altijd zeer kritisch geweest over de overeenkomst met de VS en nam in mei 2010 een resolutie aan waarin de Commissie werd opgeroepen deze te heronderhandelen op basis van een duidelijke set van principes (CEC 2010: 18, zie ook Mitsilegas 2009).

Door de nieuwe schok van de bomaanslagen in Londen in 2005 begon Europa zelf ook interesse te krijgen in PNR-data. In 2007 lag de ontwerp-Passenger Name Record Framework Decision van JBZ-commissaris Frattini op tafel. Dit ontwerp houdt in dat de autoriteiten van alle lidstaten PNR-data verzamelen van alle passagiers die uit derde landen naar de EU komen en dat deze data geanalyseerd en uitgewisseld kunnen worden tussen de lidstaten. De verschillen tussen de lidstaten in termen van nationale wetgeving op dit punt zijn opvallend. De meeste lidstaten hebben geen enkel PNR-systeem, maar vele lidstaten hebben wel interesse, Frankrijk en Denemarken hebben de wetgeving voor een PNR-systeem op orde en het Verenigd Koninkrijk is het enige land dat met zijn e-Borders-programma een operationeel PNR-systeem heeft (House of Lords 2008: 7). Het Verenigd Koninkrijk dat in de JBZ-samenwerking een buitenbeentje is, omdat het geen lid van Schengen is maar wel via een opt-in desgewenst met elke maatregel mee *mag* doen, heeft bovendien het langste verlanglijstje voor het voorliggende PNR-voorstel. In essentie vindt de Engelse regering de restricties op het gebruik van de gegevens in het voorstel te streng: veiligheid moet meer prioriteit krijgen en de bescherming van persoonlijke gegevens moet daarvoor wijken. Zo wil de Britse regering dat de data gebruikt kunnen worden voor opsporing en onderzoek van alle 'serieuze misdaad' en voor het immigratiebeleid (in plaats van alleen terrorisme en georganiseerde misdaad). Bovendien moet het PNR-regime gelden voor alle reizen (en niet alleen luchtvaart) en moeten alle vluchten, ook tussen lidstaten en zelfs interne vluchten, worden opgenomen (en niet alleen die tussen

een EU-land en een derde land). Hoewel het niet waarschijnlijk is dat dit Britse lijstje overgenomen wordt, is het een schoolvoorbeeld van de manier waarop function creep tot stand komt of kan komen.

Het voorstel van de Commissie was en is omstreden, zowel bij het EP als bij de Raad (Brouwer 2009b; Leonard 2010). In 2008 besloot de Europese Raad al om het oorspronkelijke voorstel van de Commissie te verlaten om meer ruimte te geven aan een aantal zorgen van bepaalde lidstaten. Veel van die 'zorgen' komen erop neer dat de reikwijdte van de overeenkomst wat de lidstaten betreft uitgebreid moet worden. Zo zouden de verzamelde gegevens niet alleen gebruikt moeten kunnen worden voor 'counter-terrorism and fighting serious crime', maar ook voor 'other offences brought to light during controls' (EU Council in Hobbing & Koslowski 2009: 31). Bovendien zouden de data niet alleen worden gecontroleerd in internationale en Europese *watchlists*, maar ook in 'highly divergent national watchlists' (Ibid.: 32). Brouwer (2009b: 2) verwacht op basis van de stukken van de Raad dat de data "[…] will also be used to investigate other crimes and to prevent irregular migration". Het PNR-voorstel is inmiddels echter door de institutionele vooruitgang van het Verdrag van Lissabon ingehaald. Omdat er voor de inwerkingtreding van dit verdrag geen overeenstemming bereikt was over deze *framework decision* (een instrument van de door Lissabon afgeschafte derde pijler), is het ontwerp van tafel gehaald. In het Stockholm-programma verzoekt de Europese Raad de Commissie om op zo kort mogelijke termijn te komen met een voorstel voor een Passenger Name Record Package dat voorziet in een strategie om de overeenkomsten met de VS, Australië en Canada te (her)onderhandelen en om een nieuw EU PNR-voorstel op tafel te leggen (CEC 2010: 20). Gezien de gewijzigde institutionele verhoudingen na Lissabon zal de Commissie daarbij niet alleen de wensen en belangen van de Europese Raad moeten betrekken, maar ook die van het Europese Parlement dat het PNR-dossier in de afgelopen jaren kritisch, maar noodgedwongen vanaf de zijlijn, heeft gevolgd.

7.5.2 ENTRY/EXIT-SYSTEEM

Het Entry/Exit-systeem is onderdeel van de zogenaamde *border package* dat de Commissie in 2008 in een drietal Communications neerlegde. Naast Communications over Frontex en over EUROSUR ging de derde over de digitale toekomst van het Europese *border management* (CEC 2008). In een kort stuk introduceert de Commissie de mogelijkheden voor drie nieuwe systemen: het Entry/Exit-systeem, een *automated border control system for EU citizens* en een *electronic travel authorisation system* (ESTA). Wanneer dit border package wordt afgezet tegen de verschillen van inzicht tussen de VS en de EU zoals die bijvoorbeeld in het PNR-dossier naar voren kwamen, valt de trans-Atlantische verwantschap en overeenstemming over digitale grenzen sterk op. Hobbing (2010: 68) spreekt van een keerpunt: "All that seemed of doubtful value before, such as fully automated

border checks, comprehensive systems of entry-exit control, air passenger surveillance and electronic travel authorisation, hi-tech border installations including virtual fences, has all of a sudden become part of the EU's vision for the 21st century."

Het border package bevat in principe alleen voorstellen en intenties en heeft nog geen enkele juridische status. Het is vooralsnog een visie op de toekomst (Hobbing & Koslowski 2009). Het Entry/Exit-systeem blijft echter wel voortdurend terugkomen in de Europese discussies en lijkt zich in ieder geval tussen de oren van de Commissie en veel van de lidstaten te hebben vastgezet. Het voorgestelde Entry/Exit-systeem is erop gericht om het probleem van de visa *overstayers*, oftewel illegalen, aan te pakken. Dat probleem wordt door de Commissie en de Europese Raad vaak als zeer groot voorgesteld. Het door de EU gefinancierde wetenschappelijke onderzoeksproject *Clandestino* 'berekende' op basis van het best beschikbare materiaal uit de verschillende lidstaten dat de populatie ergens tussen de 1,9 en 3,8 miljoen illegalen ligt. Dat is veel minder dan de 4,5 tot 8 miljoen die tot voor kort in officiële EU-documenten werd genoemd (Clandestino-project 2009). Er worden met andere woorden veel politieke *number games* rondom de populatie illegale vreemdelingen gespeeld, terwijl er in werkelijkheid nauwelijks goed onderbouwde schattingen te geven zijn. Sterker nog, dat nieuwe systeem moet daar juist informatie over gaan opleveren. Het Entry/Exit-systeem moet zowel de aankomst als het vertrek registreren van alle 'derdelanders' die voor een korte periode tot de EU worden toegelaten (drie maanden) of dat nu met een visum is of zonder. Als iemand niet vertrekt, of niet 'uitklokt' bij vertrek, geeft het systeem na drie maanden een waarschuwing af aan de autoriteiten dat deze persoon niet langer legaal in de EU verblijft. Het systeem is bedoeld om 'overstayers' te kunnen identificeren, 'derdelanders' te ontmoedigen om te overstayen en om operationele informatie te leveren over het fenomeen van overstaying (omvang van de populatie, routes, frauduleuze sponsors, landen van herkomst en opgegeven reden voor de reis) (CEC 2008: 8). Die informatie kan dan weer worden gebruikt om nieuwe risicoprofielen te maken en leidt dus tot meer, en meer toegespitste, profilering. Het Entry/Exit-systeem moet bovendien gaan werken met biometrische *identifiers*. Van iedereen die een visum aanvraagt, worden de vingerafdrukken in het VIS opgeslagen en bij het inreizen en uitreizen worden die gecontroleerd met de vingerafdrukken van de persoon die zich aan de grens meldt. Van de personen die geen visum nodig hebben, worden de vingerafdrukken aan de grens afgenomen. Het systeem zou dus sterk verbonden zijn met het VIS en het SIS en de Commissie geeft al aan dat ook dit systeem zou moeten draaien op het Biometric Matching System dat nu wordt ontwikkeld voor de andere biometrische JBZ-systemen.

Australië heeft al sinds 1981 een, niet-biometrisch, Entry/Exit-systeem. Uiteraard heeft dit land een geografisch voordeel in het feit dat een dergelijk afgelegen eiland

nu eenmaal een overzichtelijk aantal *ports of entry* heeft via de lucht en de zee. Geen landsgrenzen die het voor een land als de Verenigde Staten en een verbond van landen als de EU een stuk ingewikkelder maken. Het automatische Australische systeem vergelijkt de gedigitaliseerde aankomst- en vertrekkaartjes die reizigers invullen en inleveren en identificeert op die manier overstayers. Wie zijn visum meer dan 28 dagen heeft laten verlopen is voor drie jaar uitgesloten voor een nieuw visum. Dit, niet-biometrische, systeem lijkt goed te werken, zij het onder de gunstige geografische voorwaarden van de eiland-staat. De grootste groep overstayers bleek in 2005 overigens de Amerikanen te zijn (Koslowski 2008: 116). Het Europese voorstel voor een Entry/Exit-systeem is echter gemodelleerd naar het Amerikaanse US-VISIT-systeem[10], dat wel met biometrie werkt. Plannen voor dit systeem bestonden al sinds 1996, maar het waren de aanslagen van 9/11 die ervoor zorgden dat het systeem daadwerkelijk tot stand is gekomen. Het US-VISIT-systeem slaat de digitale foto's en vingerafdrukken op van alle individuen die naar de Verenigde Staten reizen op een niet-immigranten visum en van alle bezoekers die burgers zijn van landen die onder het Visa Waiver-programma vallen (zoals de meeste EU-lidstaten). De biometrische gegevens die mensen hebben afgestaan toen ze een Amerikaans visum aanvroegen (vergelijk het toekomstige VIS) worden aan de grens gecontroleerd met de vingerafdrukken van de persoon in kwestie. Het systeem is in gebruik sinds 2004 en in februari 2008 hadden de Amerikaanse autoriteiten reeds de biometrische gegevens van 113 miljoen personen opgeslagen en gecontroleerd tegen de verschillende *watch list databases* (Koslowski 2008: 117). Het is wel belangrijk om vast te stellen dat het US-VISIT-systeem, in tegenstelling tot het Entry/Exit-systeem, sterk is gericht op het probleem van terrorisme. Dat wil zeggen, in termen van zijn doelstelling, want gezien de praktische beperkingen van het systeem lijkt de daadwerkelijke bijdrage aan de *war on terrorism* vooralsnog beperkt. Het grootste probleem zit hem in de landsgrenzen van de VS: er worden geen exit-controles gehouden aan de landsgrenzen, hetgeen betekent dat de achterdeur van het systeem wagenwijd openstaat. Bovendien worden er weliswaar controles gehouden aan de officiële grensovergangen tussen bijvoorbeeld Canada en de VS, maar die staan in geen verhouding tot het gemak waarmee deze uitgestrekte grens op (vele) andere plaatsen kan worden overgestoken (Hobbing & Koslowski 2009: 17-18). Vanwege de enorme drukte aan de Amerikaanse grensovergangen via land wordt de controle meestal *on sight* en op basis van het inzicht van de grensbewaker uitgevoerd.

Amerikaanse burgers maken een *oral declaration of citizenship* en vaak wordt er geen bewijs van burgerschap gevraagd. Deze 'achterdeur' verwerkt echter wel veruit de meeste grensoverschrijdingen in de VS. Koslowski (2009: 20) concludeert dan ook: "Deployment of US-VISIT is limited to entry and enrollment is required of a relatively small percentage of all those who enter the US. Therefore, US-VISIT is far from the entry-exit system that was initially envisioned by Congress." Dit ondanks het vele geld dat er al aan uitgegeven is en dat er nog voor

gereserveerd staat. Het probleem van de landsgrenzen zal bij het uitrollen van een Europees Entry/Exit-systeem uiteraard ook een belangrijke factor zijn. De uitgestrekte grenzen, zowel via land als via de zee, zijn een probleem, net als de potentiële lange rijen aan de grens als het regime voor afname van biometrie en biometrische identificatie wordt ingevoerd bij de officiële grensovergangen. De situatie aan de grenzen van de EU aan het begin van 2010 laat zich in de volgende cijfers samenvatten: 27 lidstaten die formeel verantwoordelijk zijn voor de 10.000 kilometer landsgrenzen, 50.000 kilometer zeegrenzen en 1.800 officiële ports of entry van de EU (Hobbing 2010). Ter vergelijking: de Verenigde Staten hebben 'slechts' 327 officiële ports of entry. Het Entry/Exit-syteem staat, ondanks dit soort cijfers, nog steeds stevig op de agenda. In het Stockholm-actieprogramma, de praktische uitwerking van het Stockholm-programma, is vastgelegd dat de Commissie in 2011 met een *legislative proposal* voor dit systeem komt (CEC 2010: 20).

Het border package combineert de toename van controle door middel van het Entry/Exit-systeem met een tweetal voorstellen die de grenspassage sneller en makkelijker moeten maken: controle en comfort in één pakket is de boodschap. Voor sommige reizigers zou een zogenaamd Registered Travelers Programma (RTP) moeten worden ingesteld. Dit programma zou bepaalde groepen van *frequent travelers* uit derde landen een versnelde toegang tot de EU moeten geven via automatische toegangspoortjes. Daarbij gaat het om reizigers met een laag risico die van tevoren uitgebreid worden gescreend om de status van *registered traveler* te krijgen en die dan op basis van een biometrische controle de grens kunnen passeren (CEC 2010). Dit systeem doet sterk denken aan het Priviumprogramma dat op Schiphol al commercieel wordt aangeboden. In dit programma kunnen reizigers zich na uitgebreide screening en de opname van een irisscan in een database registreren en voor hun grenspassage gebruikmaken van aparte poortjes waarbij hun iris wordt gecontroleerd in plaats van hun paspoort (Van der Ploeg & Sprenkels 2009). De Commissie verwacht in 2011 een *legislative proposal* te doen voor dit programma. Het derde deel van de border package is het voorstel om een European System of Travel Authorisation (ESTA) te onderzoeken. Een dergelijk systeem, wederom geïnspireerd op Amerikaanse en Australische voorbeelden, vereist dat 'derdelanders' voor vertrek een elektronische aanvraag bij de autoriteiten doen, waarbij persoons- en paspoortgegevens verstuurd worden, die als voorwaarde voor het inreizen in de EU gelden. Een 'derdelander' kan dan alleen vertrekken als deze online check tegen een aantal migratiedatabanken geen contra-indicatie afgeeft (Guild et al. 2008). Het ESTA wordt in het kader van het Stockholm-actieprogramma door de Commissie op zijn haalbaarheid onderzocht om te bepalen of en hoe de EU met dit plan verdergaat (CEC 2010: 20).

Met het border package zouden in feite twee stromen reizigers worden gecreëerd: een groep reizigers die individueel gescreend wordt en de status van *trusted traveler* krijgt en een (grote) groep die onder de algemene surveillance van de grens-

systemen valt op basis van risicofactoren als herkomst uit een visumplichtig land. De ene reiziger krijgt een versnelde procedure, de andere blijft in de risicocategorie en wordt als zodanig behandeld. De Commissie gebruikte voor de eerste groep het zeer ongelukkig gekozen etiket van de 'bonafide reiziger', hetgeen volgens critici impliceert dat de grote groep visumplichtige reizigers kennelijk collectief weggezet wordt als 'malafide' (EDPS 2008; Mitsilegas 2009). Te kwader trouw omdat ze – statistisch gezien – de intentie zouden (kunnen) hebben om hun visum te overstayen.

7.5.3 BIOMETRISCH PASPOORT

Het feit dat alle EU-burgers in de komende jaren in het bezit zullen komen van een biometrisch paspoort heeft alles te maken met 9/11 en de Amerikaanse *war on terror* die daarop volgde. De 'binnenlandse' pendant van die strijd tegen het terrorisme, belichaamd door de oprichting van het nieuwe Department of Homeland Security (DHS), richtte zich in sterke mate op de veiligheid op vliegvelden en de controle op migratiestromen. De EU-lidstaten die onder het zogenaamde Visa Waiver Programme vielen, en waarvan de burgers dus zonder visum de Verenigde Staten in konden reizen, ondervonden daarvan al snel de gevolgen. In het kader van de aangescherpte migratiecontrole vereiste de US Patriot Act van 2001 dat de Visa Waiver-landen in 2004 zogenaamde machine-leesbare paspoorten met biometrische identificatiegegevens aan hun burgers zouden uitgeven (Aus 2008). Het missen van deze eenzijdig afgekondigde deadline zou worden beantwoord met het opzeggen van het visumprogramma. De voorbereidingen om deze Amerikaanse eis om te zetten in EU-beleid hebben zich voor het grootste gedeelte afgespeeld in de internationale fora van de G8 en de ICAO (International Civil Aviation Organization) waarin de Verenigde Staten en een aantal grote lidstaten van de EU een dominante positie hebben (Aus 2008; Stanton 2008). In 2002 kwamen de migratie-experts van de G8 naar buiten met een standpunt over een universele standaard voor biometrie op reis-documenten: "a full and complete common interoperable technical standard [shall] be recommended to all nations of the world as the basis for interoperable biometric authentication of machine readable travel documents" (Aus 2006: 15). Deze aan-beveling aan de wereld, waar geen parlement aan te pas was gekomen, werd vervolgens uitgewerkt in samenspraak met de relevante werkgroepen van de ICAO.

In 2003 kwam de ICAO met een standpunt dat gezichtsherkenning als de *globally interoperable biometric for machine assisted identity confirmation* ging gelden. Staten die een tweede biometrisch kenmerk aan het paspoort toe wilden voegen, werd geadviseerd te kiezen voor vingerafdrukken en/of irisscans (Aus 2006: 16). In 2004 presenteerde de Commissie haar voorstel voor een *biometric passports regulation* waarin naast de verplichte opname van een gezichtsscan en een optionele opname van vingerafdrukken het – wat onlogische – voorstel stond om ook

een centraal EU biometrisch paspoortregister op te bouwen waarin alle vingerafdrukken van de aanvragers worden opgeslagen. Het voorstel voor een centraal Europees register werd niet gevolgd, maar als gevolg van de aanslagen in Madrid begon een aantal lidstaten wel hevige druk te zetten op de *verplichte* opname van vingerafdrukken op het paspoort. Met name de Groep van Vijf, een informele groep van de ministers van Binnenlandse Zaken en ambtenaren van Frankrijk, Duitsland, Italië, Spanje en het Verenigd Koninkrijk, startte daar een lobby voor op. De ontwikkeling van de Europese standaarden voor het biometrisch paspoort zijn verder uitgewerkt in de Visa Working Party waarin deze 'G5' een doorslaggevende stem bleek te hebben (Aus 2008). In het verdere proces werden *alle* bezwaren van het Europees Parlement genegeerd en werd het uiteindelijke voorstel afgehamerd door de General Affairs and External Relations Council. Met andere woorden: niet de ministers van Justitie en Binnenlandse Zaken die het hele voortraject hebben gedaan, maar de ministers van Buitenlandse Zaken hebben het voorstel in een verordening omgezet waarin elke Europese burger uiteindelijk een biometrisch paspoort met gezichtsherkenning en vingerafdrukken krijgt (zie Aus 2008 voor een gedetailleerde weergave van het proces). Vaak ver buiten het blikveld van Europese burgers en hun verkozen vertegenwoordigers werden besluiten over techniek, standaarden en informatie-uitwisseling genomen die doorwerken in de technologie die uiteindelijk wordt gebruikt en in de informatie die tussen overheden wordt uitgewisseld.

De Europese paspoortverordening geeft de lidstaten op een aantal punten volop de ruimte om een 'nationale kop' op de Europese verplichtingen te zetten. In Nederland greep de regering de verordening aan om in aanvulling op de opslag van biometrie op het paspoort zelf, de vingerafdrukken ook in een nationale centrale databank op te willen slaan (zie voor een uitgebreide bespreking Böhre 2010). Door de vingerafdrukken centraal op te slaan is het in principe mogelijk de nationale databank als een biometrisch opsporingsregister te gebruiken. In aanvulling op verificatie (horen paspoort en houder bij elkaar) wordt met een centraal biometrisch register ook identificatie mogelijk (een persoon is via zijn vingerafdruk in de databank vindbaar). Hoewel de regering zegt dat niet van plan te zijn, blijft het een feit dat de centrale opslag veel meer functionaliteiten mogelijk maakt dan wanneer de biometrie alleen op het paspoort zelf is opgeslagen, hetgeen de keuze van de meeste Europese lidstaten is. De Paspoortwet die de centrale oplag mogelijk maakt is in 2009 door zowel de Tweede als de Eerste Kamer aangenomen. Inmiddels gaan er in de nieuwe Tweede Kamer (van na de verkiezingen van juni 2010) stemmen op om de centrale opslag weer te blokkeren. Dit niet zozeer vanwege mogelijke function creep, maar uit overwegingen van beveiliging van de centrale opslag (risico van fraude en misbruik) en overwegingen van nationale veiligheid.[11]

7.5.4 TUSSENCONCLUSIE

Met de tweede generatie migratiesystemen wordt het digitale netwerk van de Europese grens tegelijkertijd breder en fijnmaziger. Riskcalculatie, data-uitwisseling (van persoonsgegevens, gedragsgegevens en biometrische gegevens) en de uitbreiding van het netwerk naar de controle op alle reizigers zorgen ervoor dat "(…) border controls are transformed into a model of generalised surveillance of movement, based on profiling, and on concepts such as the trusted or suspect passenger" (Mitsilegas 2009: 34). Daarmee moet ook bereikt worden dat grenscontrole steeds meer *remote control* (Zolberg 2002) wordt: de systemen moeten hun werk bij voorkeur doen ver voordat de eigenlijke fysieke grens van de EU is bereikt. Het idee van remote control zit ook sterk verankerd in wat de Amerikanen hun *smart borders* concept noemen en dat de EU, met alle voornemens uit het border package, in feite aan het volgen is. *Pushing the borders out*, is het centrale idee dat ervoor moet zorgen dat controles aan de grenzen steeds minder nodig zijn. Het doel is "for borders to increasingly exist *de facto* in cyberspace, i.e., become 'virtual borders'" (Hobbing & Koslowski 2009: 14). Ook op dit punt is de industrie volop bezig om de (toekomstige) wensen van de EU van instrumenten te voorzien. Nanne Oland, directeur van Dartagnan BV, dat zich specialiseert in grenssystemen, schetste in 2007 het volgende toekomstbeeld.

> "The border Police officer at the port of arrival will become the last line of defence, rather than the first (…) dealing with exceptions rather than checking travelers and granting them admission to the country on the spot. (…) In fact, we could theoretically foresee that the vast majority of the travelers arriving at certain borders will be (pre) registered travelers and hence a 'friendly flow'" (geciteerd in Hayes 2009: 35).

Oftewel, met het uitrollen van al deze systemen, en nog een aantal dat hier verder niet is uitgewerkt[12], worden steeds meer twee stromen gecreëerd in het internationale verkeer van personen. Eén geprivilegieerde en één risicogroep. De groep van ongewensten, de derde groep, zou steeds meer al ver voor de grens de toegang ontzegd moeten zijn en zouden 'ideaaltypisch' gezien niet eens aan de reis beginnen. De interactie tussen de risicogroep en informatietechnologie is van groot belang, omdat deze wordt bepaald door profielen en dus door een actuarieel beleid.

De risicogroep – Lyon noemt ze in het volgende citaat 'de anderen', fluctueert als gevolg daarvan mee met de algoritmen en de instellingen van de techniek: "One difficulty of such others, in current identification regimes, is that their ranks may expand at will – or whim – through slight statistical adjustments expressed in the algorithms controlling for entry and eligibility" (Lyon 2009: 148). Risico en risicocategorieën zijn dus wel degelijk politiek, ook al worden ze vaak als neutrale, technische aangelegenheden gezien en/of gepresenteerd. Daarmee wordt er nog steeds

een beslissing genomen die in de software en het systeem heel reële consequenties krijgt. Aradau et al. (2008: 152) wijzen op de politieke consequenties van systemen gebaseerd op risicocalculatie: "'Who decides?' is increasingly supplemented by 'Who gets to imagine the future?' The imagination of the future has become one of the main political stakes."

7.6 ROL VAN INDUSTRIE EN ADVISEURS

Voormalig JBZ-commissaris Franco Frattini was in 2007 duidelijk toen hij in Berlijn de EU Security Research Conference toesprak: "Security is no longer a monopoly that belongs to public administrations, but a common good, for which responsibility and implementation should be shared by public and private bodies" (geciteerd in Hayes 2009: 8). Private partijen geven dus niet alleen de technische uitwerking van politiek-ambtelijke wensen en opdrachten, maar hebben wat de EU-commissaris betreft een bredere verantwoordelijkheid en taak. Deels is dat natuurlijk niets nieuws onder de zon. Zowel uit pragmatisch oogpunt – gebruikmaken van de kennis en kunde uit het bedrijfsleven – als uit het oogpunt van het winstoogmerk aan de kant van de bedrijven, is het zinvol om samen te werken met de industrie die de systemen uiteindelijk maakt en bouwt. Bovendien speelt er op Europees en op nationaal niveau nog een ander relevant argument: het beschermen en versterken van de concurrentiepositie van het Europese bedrijfs-leven, meer specifiek in dit geval de concurrentiepositie van Europese veiligheidsbedrijven op wat wel de *homeland security*-markt wordt genoemd. Lyon (2009: 117) refereert bijvoorbeeld aan het EU-rapport *Biometrics at the frontier. Assessing the impact on society* waarin ook het doel opgenomen staat "to promote a vibrant European Biometrics Industry". Voor de EU lopen hier de rollen van afnemer van biometrische systemen en het stimuleren van de Europese industrie door elkaar.

Ook is er een sterke vermenging tussen de defensie-industrie en de industrie die zich richt op homeland security die de databanken, biometrie en RFID et cetera levert voor de systemen rondom de Europese migratie en mobiliteit. Bepaalde bedrijfsnamen komen veelvuldig terug. Europese Defensiegiganten als Sagem, Thales, BAE System, Finmeccanica en IT-giganten als Ericsson en Siemens figureren vaak in de aankondigingen van de Commissie over wie welk systeem voor de EU mag gaan ontwikkelen. In Brussel, dat van oudsher veel meer een lobbycircuit kent dan bijvoorbeeld Den Haag, werden in de afgelopen jaren dan ook een aantal lobbyclubs opgericht die de belangen van de industrie promoten. In 2008 werd de European Organisation for Security (EOS) opgericht, een lobbygroep van de defensie en veiligheidsindustrie (Hayes 2009: 26). In 2003 verenigde de Europese biometrie-industrie zich, in reactie op een eerste *call for research* van de EU, in het European Biometrics Forum (EBF, zie Liberatore 2005: 13). Naast de politiek zijn het immers de adviseurs, consultants en vertegenwoordigers van de industrie die een belangrijke rol spelen bij het inschatten en framen van de 'interne veilig-

Box 7.1

Follow the money?
De verwevenheid tussen de veiligheidsindustrie en het EU-onderzoeksbudget

Het startschot voor de invloed van de IT en veiligheidsindustrie in het EU research programma werd gegeven door de zogenaamde Group of Personalities (GOP) die in 2004 een rapport presenteerde over de toekomst van het securityonderzoek. De GOP bestond uit vertegenwoordigers van de defensie-industrie, de IT-industrie, onderzoeksinstellingen (zoals Rand Corporation en TNO (-defensie) en enkele leden van het Europees Parlement. Hoofdboodschap van het rapport was dat het Europese veiligheidsonderzoek op hetzelfde niveau gefinancierd zou moeten worden als in de Verenigde Staten, om de slag om de markt voor homeland security-technologie niet te missen. De Amerikaanse overheid investeerde jaarlijks 1 miljard dollar in defensie- en veiligheidsonderzoek (R&D) en de Group of Personalities vroeg eenzelfde investering van de EU. De vrees voor Amerikaanse dominantie op die markt lijkt het belangrijkste argument om de Europese politiek tot actie aan te sporen. Anders gezegd: als de EU en de lidstaten dan toch miljarden Euro's uit gaan geven aan nieuwe technologieën op het gebied van (interne) veiligheid, dan zou het toch goed zijn als dat ten goede komt aan de Europese industrie. Bovendien zou een voorspong van de Amerikaanse industrie zich volgens de GOP zeer lang laten voelen: US technology would "progressively impose normative and operational standards" (geciteerd in Hayes 2009: 11). De standaarden en protocollen sturen immers de toekomstige mogelijkheden en creëren een padafhankelijkheid. Uiteindelijk kreeg de industrie haar miljard per jaar niet. Maar de structurele financiering van ruim 200 miljoen per jaar die het wel kreeg, wordt nog aangevuld uit verschillende andere projecten waardoor het geheel toch nog stevig optelt. Belangrijker is wellicht dat de industrie zich een permanente plek in het onderzoeksveld heeft verworven. De GOP 'advies groep' voor security research, liep over in de European Security Research Advisory Board (ESRAB), die op zijn beurt overliep in het European Security Research and Innovation Forum (ESRIF). De continue betrok-kenheid van dezelfde industrieën en personen is daarbij opmerkelijk, net als het feit dat de samenstelling relatief eenzijdig is en weinig recht doet aan de *balanced representation of stakeholders* die de Commissie had beloofd (Hayes 2009: 24). In het Stockholm-programma roept de Europese Raad de Commissie op om het instellen van een Internal Security Fund te onderzoeken (CEU 2009: 36).

heidssituatie' en die bepleiten welke oplossingen en technologieën daarbij een rol moeten spelen (zie bijv. Amoore 2006; Salter 2008; Hayes 2009). Het feit dat een belangrijk deel van de industrie die veel van de technische oplossingen en systemen levert haar wortels in de defensie-industrie heeft, draagt bij aan de toch al steeds grotere – door veel wetenschappers bekritiseerde – vermenging van het veiligheidsbeleid en het immigratiebeleid (Guild 2009; Huysmans 2006; Boswell 2007).

Gezien de grote uitgaven die de EU heeft aan de verschillende datasystemen voor immigratie en (interne) veiligheid, de commerciële belangen van de (Europese) industrie en het politieke belang van een sterke IT-industrie in Europa, is er naast

de relatie opdrachtgever en uitvoerder van de Europese IT-plannen, nog een relatie ontstaan. Een nieuwe vermenging tussen publieke en private verantwoordelijkheid ten aanzien van veiligheid ligt in de relatie tussen het EU-onderzoeksbeleid (en de onderzoeksgelden) en de Europese veiligheidsindustrie. Ben Hayes (2009 en 2006), verbonden aan *Statewatch* en het *Transnational Institute*, heeft uitgebreid studie gemaakt van die verwevenheid.

Hoewel publiek-private samenwerking grote voordelen oplevert en bovendien deels onvermijdelijk is, zijn er ook redenen om de ontwikkelingen met enige argwaan te volgen. In de eerste plaats omdat het over veiligheid gaat: dat is traditioneel een kerntaak van de overheid en het is maar de vraag of die kerntaak zich wel zo goed leent voor een gedeelde verantwoordelijkheid van overheid en bedrijfsleven.[13] Zeker als de grondstof van die veiligheid persoonlijke informatie over burgers en migranten is die in grote datasystemen wordt verwerkt en bewerkt. De recente ophef in de Tweede Kamer over het gegeven dat een Frans bedrijf in principe de databank voor de centrale opslag van de (biometrische) paspoortgegevens van de Nederlandse bevolking zou leveren – overigens een logisch uitvloeisel van de privatisering van de Sdu – geeft al aan dat dit gevoelig ligt.[14] De Tweede Kamer lijkt zich in de winter van 2010 om redenen van beveiliging en nationale veiligheid tegen de centrale opslag van de (biometrische) paspoortgegevens te keren[15], terwijl de Kamer de wet eerder nog had goedgekeurd (Böhre 2010). Naast overwegingen van nationale veiligheid en de vraag of en hoe zich dat laat verenigen met het (buitenlandse) bedrijfsleven, geldt dat de homeland security market voor een groot deel een opkomende en nog weinig uitgebalanceerde markt is. Snijder (2010) laat zien dat de Europese biometrische industrie een relatief afgebakende en tegelijkertijd onvolwassen markt is. De grootte van de projecten die de EU uitzet, maakt dat er maar een handvol bedrijven wereldwijd in staat is te leveren wat er gevraagd wordt. Specifiek voor de markt voor biometrische systemen geldt bovendien dat de markt historisch gezien sterk langs nationale lijnen verkaveld is en er nog weinig animo is voor daadwerkelijke interoperabiliteit tussen systemen. Investeren in de nationale klanten waarmee langdurige banden zijn opgebouwd, geniet vaak nog de voorkeur voor bedrijven. Standaarden zijn daarmee in de praktijk, ondanks een overvloed aan testen en formeel afgesproken (ISO) standaarden, nog lang niet op een hoog niveau van interoperabiliteit (Snijder 2010).

7.7 ROL VAN STANDAARDEN

Ondanks de technische en bedrijfsstrategische belemmeringen moet de rol van standaarden op het terrein van de JBZ-databanken niet worden onderschat. Het is een voordurend terugkerend streven. De belangrijkste vorm daarvan is die van het magische woord interoperabiliteit. De verschillende datasystemen moeten zoveel mogelijk in staat zijn 'met elkaar te praten' en moeten in feite allemaal technisch gezien koppelbaar zijn of worden. In 2002 kwam de interoperabiliteit op de

agenda met het instellen van een *ad hoc group on Third Pillar Information Systems*, die de synergie tussen SIS II, CIS, Europol en Eurodac moest onderzoeken. Zoals deze vier databanken al aangeven ging het om de volle breedte van het JBZ-terrein.

Naast migratiedatabanken (SIS & Eurodac) ging het ook om goederen (Customs Information System, CIS) en om opsporing (Europol). De ad-hocgroep kwam met twee mogelijkheden voor de toekomst: (1) alle systemen samenvoegen in een nieuw Union Information System, dat leek de groep echter zowel onwettig als technisch onhaalbaar en (2) het harmoniseren van *data formats* en de regels voor toegang tot de data. De ontwikkeling van bestaande en nieuwe systemen moet zich in de richting van grotere interoperabiliteit bewegen. Die laatste lijn is de afgelopen jaren stevig doorgetrokken. In 2005 bracht de Commissie een document uit over het verbeteren van de effectiviteit, interoperabiliteit en synergie van de JBZ-databanken (CEC 2005). De context van het stuk was de strijd tegen terrorisme en zware criminaliteit, maar de databanken in kwestie waren in hoofdzaak de bekende migratiedatabanken. In de tekst wordt een voorbehoud gemaakt dat het hier niet gaat om de juridische en politieke overwegingen, om vervolgens tot de toch nog ongemakkelijke stelling te komen dat "Interoperability is a technical rather than a legal or politcial concept" (CEC 2005: 3). Als iets duidelijk is geworden uit het voorgaande is het wel dat deze tekst – zelfs met dit voorbehoud – gewantrouwd moet worden. Techniek en politiek zijn op dit terrein moeilijk van elkaar te scheiden. Mitsilegas (2009: 56) ziet grote gevaren in de combinatie van het vergroten van interoperabiliteit en het verbreden van de toegang tot de informatie in de verschillende JBZ-databases voor steeds meer autoriteiten:

> "It can be seen as an attempt to de-politicise an issue which may have major repercussions for the protection of fundamental rights and civil liberties, and which has the potential to shield far-reaching developments (including the blurring of the boundaries between databases established for different purposes and containing different categories of data, for the benefit of law enforcement agencies) from effective scrutiny and democratic control."

In 2009 legde de Commissie het plan op tafel om te komen tot en EU-agentschap dat het operationele management van alle grootschalige IT-systemen in het JBZ-domein op zich gaat nemen. Daarbij gaat het in ieder geval om SIS II, VIS en Eurodac en "any new system that may be set up in the future in the area of freedom, security and justice" (CEC 2009b: 4). Om tot een *optimale synergie* te komen moeten alle systemen op één locatie worden gehuisvest en op hetzelfde technologische platform gaan draaien. Praktisch gezien houdt dat in dat Eurodac naar het technische model van SIS en VIS moet worden overgezet. Alle nieuwe systemen volgen dan hetzelfde technische model. In het recent door de Commissie gepubliceerde overzicht van alle informatiesystemen en overeenkomsten voor informatie-uitwisseling binnen het JBZ-terrein (CEC 2010) valt het woord interoperabi-

liteit dan weer op door zijn volledige afwezigheid in de tekst. Net als in het Stockholm-programma ligt de nadruk hier juist veel meer op alle rechten en waarborgen voor burgers waarmee de systemen zijn en worden omkleed. Het feit dat de vele datasystemen aparte containers zijn, wordt in deze tekst niet als een probleem, maar als een voordeel gepresenteerd: "The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralized alternative" (CEC 2010: 3). Dat is wel eens anders geweest.

Daarnaast geldt er binnen het JBZ-terrein ook nog een heel ander soort standaarden. Deze standaarden zijn meer politiek en pragmatisch van aard en 'harmoniseren' niet de techniek of de informatie zelf, maar de condities waaronder informatie uitgewisseld en aanvaard kan worden. Bij de uitwisseling van PNR-data met de VS ging het bijvoorbeeld om het voldoen aan een *adequacy*-criterium op het gebied van privacy en gegevensbescherming. In het Den Haag-programma stond het principe van de beschikbaarheid (availability) centraal als uitgangspunt voor gegevensuitwisseling. Dat principe zou de uitwisseling van informatie tussen de autoriteiten van de lidstaten sterk moeten vereenvoudigen op basis van het mechanisme dat:

> "(…) the authorities of any Member State would have the same right of access to information held by any other authority in the Union as applies to state authorities within the state where the data are held. Thus the element of the national settlement on the collection, retention and manipulation of data expressed in national constitutions is transformed into an EU-wide right of use of data" (Balzacq et al. 2006: 2).

In feite is het principe van beschikbaarheid een vorm van wederzijdse erkenning van beslissingen (in dit geval beslissingen rondom de verzameling, opslag, verwerking en uiteindelijk de uitwisseling van data). Niet het proces waarmee men op nationaal niveau tot beslissingen komt wordt geharmoniseerd, maar de uitkomsten van die nationale processen worden onderling geaccepteerd vanuit de gedachte dat de zorgvuldigheid en betrouwbaarheid daarvan weliswaar niet hetzelfde is tussen lidstaten, maar wel aan vastgestelde eisen voldoet. Het gebruik van migratiedatabanken komt in de praktijk ook vaak neer op een wederzijdse erkenning van beslissingen, ook al wordt dat niet altijd ook expliciet zo genoemd.

Eurodac codificeert de wederzijdse erkenning van beslissingen inzake asiel tussen de lidstaten: wie door één lidstaat is afgewezen, is in feite door alle lidstaten afgewezen en die informatie is terug te vinden in Eurodac. De kwaliteit van de asielprocedure in sommige landen is daarbij soms echter een probleem; zo heeft het Duitse hooggerechtshof het uitwijzen van Irakese Dublin-claimanten naar Griekenland in 2009 stopgezet, omdat het twijfelde aan de rechtmatigheid van de

Griekse asielprocedure.[16] Nederland deed dat overigens niet. Maar ook het SIS, het VIS wanneer het operationeel wordt en het Entry/Exit-systeem, mocht dat ontwikkeld worden, opereren op basis van het principe dat afwijzing en signalering door één lidstaat gelijkstaat aan afwijzing door alle lidstaten. Hoewel dit soort systemen niet tot automatische procedures mogen leiden, blijkt dat in de praktijk wel degelijk voor te komen, zoals de Nationale Ombudsman (2010) in het geval van het SIS heeft laten zien. In de praktijk legt het 'antwoord' dat uit een migratiedatabank komt rollen een zwaar gewicht in de schaal voor de grensbewaker, consulaatmedewerker of medewerker van de immigratiedienst die besluit over weigering of toelating. Het systeem wordt op die manier zelf een standaard.

7.8 CONCLUSIE

De grenzen van de EU ontwikkelen zich langzaamaan tot een digitaal net dat de Unie omspant en tegelijkertijd ver voor(bij) zijn fysieke grenzen opereert. Dat net is in de afgelopen jaren bovendien steeds wijder uitgegooid en dat zal naar verwachting in de komende jaren nog verder toenemen. Terwijl de eerste generatie datasystemen (SIS, Eurodac en VIS) zich nog in hoofdzaak richt op 'problematische groepen' of bekende overtreders van (immigratie)wetten, legt de tweede generatie immigratiedatabanken zich toe op de surveillance van alle reizigers. Wie de EU-grens passeert wordt straks altijd op enigerlei wijze geregistreerd of hij nu visumplichtig is, visumvrij of zelfs burger van de Europese Unie. Nieuwe systemen als het voorgenomen Entry/Exit-systeem, de uitwisseling van PNR-data en de invoering van het biometrisch paspoort brengen migratie- en mobiliteitsstromen straks uitputtend in kaart. Het verzamelen van al die data leidt tot nieuwe bewerkingen: in aanvulling op het signaleren van bekende overtreders, gaat het steeds vaker om het signaleren en in kaart brengen van risicogroepen. Met de risicoprofielen moet worden voorkomen dat de verkeerde mensen toegang tot de EU krijgen, het liefst preventief, voordat er daadwerkelijk een wet is overtreden. Dat maakt dat de risicoprofielen en categorieën waarmee datasystemen werken en rekenen van groot belang worden voor de kansen die internationale reizigers hebben. Wel of niet een visum, wel of niet toegang aan de grens. Die keuzes komen deels in de software van systemen terecht, maar zijn nog steeds keuzes over risico's en de toekomst. 'Wie beslist' wordt in toenemende mate aangevuld met de belangrijke vraag *Who get's to imagine the future?*, zoals al eerder in dit hoofdstuk werd vastgesteld. Internationale mobiliteit wordt steeds meer gestroomlijnd langs categorieën als de 'verdachte' en de 'vertrouwde' reiziger.

Naarmate de technologische verwerking van informatie dominanter wordt, neemt de aandacht voor het 'verhaal' van mobiliteit en migratie af. Aas (2004: 383) wees al eerder op dit kenmerk van databanken: "This collection of items is not run by a cause and effect logic, does not tell stories and does not have a beginning and an end, or any thematical development at all. As such, the database is a strong

contrast to the narrative." Databanken en categorieën structureren de te nemen beslissing, het verhaal verdwijnt achter de data. Migranten lopen het risico te worden gereduceerd tot de informatie die in het systeem over hen is opgenomen en de ambtenaar heeft minder mogelijkheden en ruimte om daarvan af te wijken. Een te groot vertrouwen in de juistheid van systemen leidt daarmee mogelijk tot een 'dubbele depersonalisering' (Broeders 2009b), die zowel de behandelende ambtenaar als de migrant reduceert tot de categorieën van het systeem. Door deze ontwikkelingen 'virtualiseert' de grens tot op zekere hoogte: de digitale grens komt steeds losser te staan van de fysieke, territoriale scheidslijn tussen staten. Dat wil echter niet zeggen dat de grens minder hard wordt. Het tegendeel is eerder waar: de grens manifesteert zich op vele plaatsen en in vele gedaanten en maakt vaak een scherp en moeilijk aan te vechten onderscheid tussen gewenste, ongewenste en gevreesde reizigers en migranten.

De digitalisering van de Europese grenzen wordt door een aantal factoren gedreven die er tezamen voor hebben gezorgd dat de ontwikkelingen snel zijn gegaan en relatief onevenwichtig zijn opgebouwd in termen van de balans tussen veiligheid en vrijheidsrechten. In de eerste plaats is het *technovertrouwen* van de lidstaten en tot op zekere hoogte ook van de Commissie erg groot. Over technische beperkingen wordt eigenlijk alleen gesproken in termen van tegenslagen bij de ontwikkeling van systemen (zoals bij SIS II). De beperkingen in de zin van de inherente foutmarges in technologie krijgen zeer weinig politieke aandacht van de lidstaten. Carlos Coelho, lid van het Europees Parlement, sprak tegen de achtergrond van dit technovertrouwen al eens over de noodzaak van "protecting the integrity of the innocent citizen in an atmosphere of the 'impossibility of error' under all circumstances" (in Liberatore 2005: 15). In de tweede plaats is er de verleiding van de function creep. Zoals de geschiedenis van de databanken laat zien, wordt het JBZ-beleid voor internationale mobiliteit en databanken sterk door function creep gekenmerkt. Geen enkel systeem is beperkt gehouden tot het doel waarvoor het oorspronkelijk is opgericht en vooral de vermenging tussen immigratie/mobiliteit en veiligheid is sterk toegenomen, zowel in het politieke denken als in de technische instrumenten. *Veiligheid* is zelf een van de grote motoren achter de digitalisering van de grenzen en de Verenigde Staten hebben de snelheid na 9/11 stevig opgejaagd. Veel systemen en maatregelen zijn of het resultaat van eisen die de Verenigde Staten aan Europa hebben gesteld in het kader van hun homeland security (biometrisch paspoort, PNR-overeenkomst), of het gevolg van 'beleidsimitatie', zoals in het geval van de Europese PNR-richtlijn en het Entry/Exit-systeem dat van het US-VISIT-systeem is afgeleid. Als laatste drijvende kracht geldt de invloed van de IT en *veiligheidsindustrie* zelf. De markt voor digitale grenzen en biometrie kent een grote dynamiek waarin het aanbod ook zelf zijn eigen vraag creëert: de belangen en winsten zijn groot en de beloften van de techniek vinden vaak een gewillig politiek oor.

Tot op heden heeft de ontwikkeling van nieuwe systemen in het JBZ-domein zich op weinig punten laten remmen. De lidstaten hebben het karakter en de snelheid van de digitalisering bepaald en zich tot op heden weinig aangetrokken van bezwaren die werden geuit door onder meer het Europees Parlement en de EDPS, die keer op keer wezen op risico's voor privacy, function creep, vermenging van veiligheid en immigratie en een gebrek aan doelbinding. Ook het evalueren van bestaande systemen en het leren van evaluaties van systemen over de grens lijkt niet erg in zwang. De eigen EU-systemen worden hoofdzakelijk op systeemniveau zelf geëvalueerd. De evaluaties van Eurodac laten keurig zien dat het systeem doet wat het moet doen in termen van de detectie van meervoudige asielaanvragen, maar zwijgt over de onderliggende beleidsdoelen (verdeling van asielaanvragen over Europa, terugzenden van Dublin-claimanten enz.). Maar ook bij nieuwe voornemens ligt de nadruk op wat men graag zou willen: het Entry/Exit-systeem brengt het probleem van de overstayers nauwgezet in kaart. De evaluaties, moeilijkheden en beperkingen van het US-VISIT-systeem daarentegen, worden eigenlijk nooit genoemd in de EU-stukken over het Entry/Exit-systeem, terwijl ze wel degelijk bekend en relevant zijn (vgl. Hobbing 2010). De gebrekkige balans in het JBZ-domein wordt vaak toegeschreven aan de scheve verhoudingen tussen de lidstaten en de andere Europese instituties die in de afgelopen jaren vaak nauwelijks de mogelijkheid – en de formele positie – hadden om de ontwikkelingen mede te sturen. Met de inwerkingtreding van het Verdrag van Lissabon is de vrije hand die de lidstaten lang hebben gehad duidelijk ingeperkt en hebben het EP, het Hof van Justitie en de Commissie de komende jaren een veel grotere invloed op de ontwikkeling van het digitale regime voor mobiliteit en grenzen. De toon van het Stockholm-programma, met veel meer aandacht voor rechten en vrijheid dan het door veiligheid getekende Den Haag-programma dat aan Stockholm voorafging, is daarbij een teken aan de wand. De wal van de Europese instituties kan de komende jaren het schip van de lidstaten keren en zo wat meer evenwicht tussen vrijheid en veiligheid in de digitale grenzen van Europa aanbrengen.

NOTEN

1 Strikt genomen bestaan paspoorten al (veel) langer. De eerste paspoorten duiken op in de tweede helft van de vijftiende eeuw. De koppeling van het paspoort aan de natiestaat en dus aan nationaliteit zoals we dat nu begrijpen is van veel latere datum, namelijk zo halverwege de negentiende eeuw (Groebner 2007: 9).

2 Het Verdrag van Maastricht (1992) 'richtte' de Europese Unie op, bestaande uit drie pijlers. In de eerste pijler werd het EEG-verdrag ondergebracht, in de tweede pijler werd het Gemeenschappelijk Buitenlands- en Veiligheidsbeleid ondergebracht en de derde pijler besloeg het JBZ-terrein. De tweede en derde pijler waren nieuw en werden sterk intergouvernementeel gehouden.

3 Er zijn twee Future Group reports. Een over 'Binnenlandse Zaken' die in deze tekst centraal staat en een over 'Justitie'.

4 LIBE (Committee on Civil Liberties, Justice and Home Affairs) is de commissie van het Europees Parlement die de voorstellen op het gebied van JBZ behandelt.

5 De geschreven bijdrage van het VK – die geen lid, maar observer, van de Future Group was – had nog wel wat meer te melden over PET's. Hoewel het kon helpen om privacy te beschermen en dataprotectie mogelijk te maken, melden zij ook: "however, this technology also has the potential to undermine the work of law enforcement agencies. For example, PETs may be used by individuals carrying out illegal activities on the internet to prevent their identity being discovered" (geciteerd in Statewatch 2008: 12).

6 Zie Broeders (2009) voor een cijfermatig overzicht van opslag en gebruik van de data in het SIS.

7 Noorwegen, IJsland en Zwitserland hebben associatieverdragen met de Schengen-groep, ondanks het feit dat ze geen lid van de EU zijn.

8 Zie het artikel 'EU security database over budget, won't be ready' in de *New Europe* van 19 januari 2009, http://www.neurope.eu/articles/EU-security-database-over-budget-wont-be-ready/92028.php, opgevraagd 8 oktober 2010.

9 Volgens Laurent Beslay van de EDPS speelt hierbij ook mee dat de EU zijn databankinfrastructuur graag door de Europese industrie wil laten ontwikkelen. Gesprek met Beslay 4 november 2008.

10 US-VISIT: The United States Visitor and Immigrant Status Indicator Technology.

11 Zie *de Volkskrant* 'Kamer tegen centrale opslag paspoortgegevens', 7 oktober 2010.

12 Het JBZ-terrein kent vele databanken en systemen. Er is voor gekozen om de systemen uit te werken die het sterkst aan migratie zijn gerelateerd en/of die de meest 'enerverende' geschiedenis in termen van wetgeving en politiek hebben gehad. Zie voor een volledig overzicht van de systemen op het JBZ-terrein CEC (2010).

13 Overigens past dit natuurlijk in een bredere trend waarbij veiligheid steeds verder geprivatiseerd wordt. Ook in geval van externe veiligheid (het domein van oorlog/vrede/veiligheid) hebben overheden delen van hun geweldsmonopolie

geprivatiseerd. Het meest besproken voorbeeld komt van de Verenigde Staten met de grote inzet van Private Military Companies als Blackwater in Irak. Je kunt overigens ook zeggen dat militaire operaties daarmee teruggaan in de tijd (geen geld, geen Zwitsers). De steeds intensievere vermenging tussen interne en externe veiligheid, maakt dat privatisering bij het beleid voor interne veiligheid ook een steeds grotere rol speelt. Dat de vermenging tussen interne en externe veiligheid zich ook in de private sector afspeelt, mag blijken uit het feit dat de meeste grote industrieën op het gebied van Homeland Security hun wortels hebben in de defensie-industrie.

14 Zie *de Volkskrant* 'Kamer: databank vingerafdrukken niet in Franse handen', 15 september 2010.

15 Zie *de Volkskrant* 'Kamer tegen centrale opslag paspoortgegevens', 7 oktober 2010.

16 http://weblogs.nrc.nl/rechtenbestuur/2009/09/14/duitse-grondwet-verbiedt-uitzetting-iraakse-asielzoekers-nederlandse-niet/, opgevraagd 18 oktober 2010.

LITERATUUR

Aas, K. (2004) 'From narrative to database. Technological change and penal culture.' *Punishment and Society*, vol. 6, nr. 4: 379-393.

Acosta, D. (2009) 'The good, the bad and the ugly in EU migration law: is the European Parliament becoming bad and ugly?' (the adoption of directive 2008/15: the Returns Directive), *European Journal of Migration and Law*, vol. 11, nr. 1: 19-39.

Amoore, L. (2006) 'Biometric borders: Governing mobilities in the war on terror', *Political Geography*, vol. 25, nr. 3: 336-351.

Aradau, C., L. Lobo-Geurro & R. van Munster (2008) 'Security, technologies of risk, and the political: Gust editors' introduction', *Security Dialogue*, vol. 29, nr. 2-3: 147-154.

Aus, J. (2006) 'Eurodac: a solution looking for a problem?', *European Integration Online Papers*, vol. 10, nr. 6 http://eiop.or.at/eiop/index.php/eiop/article/view/2006_006a/23

Aus, J. (2008) *EU Governance in an area of freedom, security and justice. Logics of decision making in the Justice and Home Affairs Council*. Dissertation: University of Oslo.

Balzacq, T., D. Bigo, S. Carrera & E. Guild (2006) *Security and the two-level game: The treaty of Prüm, the EU and the management of threats*. CEPS Working Document no. 234/January 2006.

Balzacq, T. (2008) 'The policy tools of securitization. Information Exchange, EU Foreign and Interior Policies', *Journal of Common Market Studies,* vol. 46, nr. 1: 75-100.

Besters, M. & F. Brom (2010) '"Greedy" information technology: the digitalization of the European Migration Policy', in *European Journal of Migration and Law,* vol. 12, nr. 4: 455-470.

Biometric Technology Today (2009) 'Biometrics review: 2008/2009', in: *Biometric Technology Today*, January 2009: 9-11.

Böhre, V. (2010) *Happy Landings? Het biometrische paspoort als zwarte doos*. WRR-webpublicaties nr. 46. Den Haag: WRR.

Bovens, M. & S. Zouridis (2002) 'From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control', *Public Administration Review*, vol. 62., nr. 2: 174-184.

Boswell, C. (2007) 'Migration control in Europe after 9/11: Explaining the absence of securitization', *Journal of Common Market Studies*, vol. 45, nr. 3: 589-610.

Broeders, D. (2007) 'The new digital borders of Europe: EU databases and the surveillance of irregular migrants', *International Sociology*, vol. 22, nr. 1: 71-92.

Broeders, D. (2009) *Breaking down anonymity. Digital surveillance of irregular migrants in Germany and the Netherlands*, Amsterdam: Amsterdam University Press.

Broeders, D. (2009b) 'Mobiliteit en Surveillance: een migratiemachine in de maak?', pp. 35-60 in H. Dijstelbloem & A. Meijer (red.) *De migratiemachine. De rol van technologie in het migratiebeleid*. Amsterdam: Van Gennep.

Broeders, D. (2009c), 'Add a little Europe for extra national strength? The Europeanization of Justice and Home Affairs', in W. Schinkel (red.), *Globalization and the state. Sociological perspectives on the state of the state*, 121-143. Houndsmills, Basingstoke & Hampshire: Palgrave.

Brouwer, E. (2002) 'Eurodac: its limitations and temptations', *European Journal of Migration and Law*, vol. 4: 231-247.

Brouwer, E. (2004) 'Persoonsregistraties als grensbewaking: Europese ontwikkelingen inzake het gebruik van informatiesystemen en de toepassing van biometrie', *Privacy & Informatie*, februari 2004.

Brouwer, E. (2009) 'Digital borders and real rights: effectieve rechtsmiddelen voor niet-EU-onderdanen in het Schengen Informatie Systeem', *NJCM-Bulletin*, jr. 34, nr. 1: 6-21.

Brouwer, E. (2009b) *The EU Passenger Name Record System and human rights. Transferring passenger data or passenger freedom?*, CEPS Working Document No. 320/ September 2009.

Bunyan, T. (2008) *The shape of things to come. EU future report*. Londen: Statewatch.

Clandestino Project (2009*) Clandestino project final report*. Brussel: European Commission. http://clandestino.eliamep.gr/wp-content/uploads/2010/03/clandestino-final-report_-november-2009.pdf

Commission of the European Communities (2003) *Communication from the Commission to the Council and the European Parliament. Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)*. COM (2003) 771 final, Brussel, 11.12.2003.

Commission of the European Communities (2005) *Communication from the Commission to the European Parliament and the Council. On improved effectiveness, enhanced interoperability and synergies among European databases in the Area of Justice and Home Affairs*. COM (2005) 597 final. Brussel, 24.11.2005.

Commission of the European Communities (2007) *Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system*. COM (2007) 299 final, Brussel, 6.6.2007.

Commission of the European Communities (2008) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the next steps in the border management in the European Union*. COM (2008) 69 final. Brussel, 13.2.2008.

Commission of the European Communities (2009) *Communication from the Commission to the European Parliament and the Council. An area of freedom, security and justice serving the citizen*. COM (2009) 262 final. Brussel, 10.6.2009.

Commission of the European Communities (2009b) *Communication from the Commission. Legislative package establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice*. COM (2009) 292 final. Brussel, 24.6.2009.

Commission of the European Communities (2009c) *Report from the Commission to the Council and the European Parliament on the Development of the Second Generation*

Schengen Information System (SIS II). Progress Report July 2008-December 2008. COM(2009) 133 final, Brussel, 24.3.2009.

Commission of the European Communities (2010) *Communication from the Commission to the European Parliament and the Council. Overview of information management in the area of freedom, security and justice.* COM (2010) 385 final. Brussel, 20.7.2010.

Commission of the European Communities (2010b) *Commission staff working document. Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II).* COM (2010) 1138 final. Brussel, 21.9.2010.

Council of the European Union (2002) *Presidency conclusions, Seville European Council*, 21-22 June 2002 (SN 200/02).

Council of the European Union (2007) Interinstitutional file: 2004/0287 (COD), 9753/07, Brussel, 19.6.2007.

Council of the European Union (2009) *'The Stockholm Programme – An open and secure Europe serving and protecting the citizens'*, 17024/09, Brussel, 2.12.2009.

EDPS (2006) *Opinion of the European Data Protection Supervisor*. Brussel, 20 January 2006.

EDPS (2008) *Preliminary comments of the European Data Protection Supervisor,* Brussel 3 March 2008.

EDPS (2009) *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament and the Council. An area of freedom, security and justice serving the citizen*. Brusssel: EDPS, 10.7.2009.

Future Group (2008) *Freedom, Security, Privacy – European Home Affairs in an open world.* Report of the informal High Level Advisory Group on the Future of European Home Affairs ('The Future Group'), June 2008.

Geyer, F. (2008) 'Taking stock: Databases and systems of information exchange in the Area of Freedom, Security and Justice', *Challenge Research Paper*, nr. 9 – May 2008.

Groebner, V. (2007) *Who are you? Identification, deception, and surveillance in Early modern Europe.* New York: Zone Books.

Guild, E., S. Carrera & F. Geyer (2008) 'The Commission's New Border Package. Does it take us one step closer to a 'cyber-fortress Europe?', *CEPS Policy Brief*, nr. 154 – March 2008.

Guild, E. & S. Carrera (2009) 'Towards the next phase of the EU's Area of Freedom, Security and Justice: the European Commission's proposals for the Stockholm Programme', *CEPS Policy Brief*, nr. 196, August 2009.

Guild, E. & S. Carrera (2010) 'The European Union's area of freedom, security and justice ten years on', pp. 112 in: E. Guild, S. Carrera & A. Eggenschwiler (red.) *The area of freedom, security and justice ten years on. Successes and future challenges under the Stockholm Programme,* Brussel: CEPS.

Guild, E. (2001) Moving the Borders of Europe, inaugural lecture, University of Nijmegen.

Guild, E. (2009) *Security and migration in the 21st century*. Cambridge: Polity Press.

Guiraudon, V. (2000) 'European integration and migration policy: vertical policy making as venue shopping', *Journal of Common Market Studies*, vol. 38, nr. 2: 249-269.

Guiraudon, V. (2003) 'The constitution of a European immigration policy domain: a political sociology approach', *Journal of European Public Policy*, vol. 10, nr. 2: 263-282.

Hayes, B. (2006) *Arming Big Brother. The EU's Security Research Programme*. TNI Briefing Series 2006/1. Amsterdam/London: Transnational Institute/Statewatch.

Hayes, B. (2009) *NeoConOpticon. The EU security-Industrial complex*. Amsterdam/London: Transnational Institute/Statewatch.

Hert, P. de (2004) 'Trends in de Europese politiële en justitiële informatiesamenwerking", *Panopticon*, jrg. 25, januari/februari.

Hert, P. de & B. de Schutter (2008) 'International transfers of data in the field of JHA: The lessons of Europol, PNR and Swift', pp. 299-335 in B. Martenczuk & S. van Thiel (red.) *Justice, liberty, security: New challenges for EU external relations*. Brussel: VUB Press.

Hobbing, P. & R. Koslowski (2009) *The tools called to support the 'delivery' of freedom, security and justice: A comparison of border security system in the EU and in the US,* Ad Hoc Briefing Paper, European Parliament, Directorate-General Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, Committee on Civil Liberties, Justice and Home Affairs, PE 410.681, February 2009.

Hobbing, P. (2010) 'The management of the EU's external borders. From the Customs Union to Frontex and E-Borders', pp. 63-72 in: E. Guild, S. Carrera & A. Eggenschwiler (red.) *The area of freedom, security and justice ten years on. Successes and future challenges under the Stockholm Programme,* Brussel: CEPS.

House of Lords (2007) *Schengen Information System II (SIS II), Report with evidence*, 9th Report of Session 2006-7 of the House of Lords' European Union Committee. London: The Stationary Office Limited.

House of Lords (2008) *The Passenger Name Record (PNR) framework decision. Report with evidence.* 15th report of session 2007-2008 of the House of Lords' European Union Committee. London: The stationary Office Limited.

Huysmans, J. (2006) *The politics of insecurity, fear, migration and asylum in the EU*. London: Routledge.

Jeandesboz, J. (2008) *Reinforcing the surveillance of EU borders. The future development of FRONTEX and EUROSUR*. Challenge Research paper nr. 11. CEPS: Brussel.

Joint Supervisory Authority of Schengen (2004*) Activities of the Joint Supervisory Authority. Sixth report January 2002/December 2003*. http://www.schengen-jsa.dataprotection.org.

Justice (2000) *The Schengen Information System: a human rights audit*. London: Justice.

Koslowski, R. (1998) 'European Union migration regimes, established and emergent', in: C. Joppke (red.) *Challenge to the nation-state. Immigration in Western Europe and The United States*. Oxford: Oxford University Press.

Koslowski, R. (2008) 'Global mobility and the quest for an international migration regime', in J. Chamie & L. Dall'Oglio (red.) *International migration and development: Continuing the dialogue: Legal and policy perspectives.* Geneva: International Organization for Migration.

Lahav, G. & V. Guiraudon (2006) 'Actors and venues in immigration control: closing the gap between political demand and policy outcomes', *West European Politics*, Vol. 29, nr. 2: 201-223.

Latour, B. (2005) *Reassembling the Social. An Introduction to Actor-Network-Theory,* Oxford: Oxford University Press.

Lavenex, S. (2006) 'Shifting up and out: the foreign policy of European immigration control', *West European Politics*, vol. 29, nr. 2: 329-350.

Leonard, S. (2010) 'The Use and Effectiveness of Migration Controls as a Counter-Terrorism Instrument in the European Union', *Central European Journal of International and Security Studies*, vol. 4, nr. 1: 32-50.

Liberatore, A. (2005) *Balancing security and democracy: the politics of Biometric Identification in the European Union*. EUI Working Papers. RSCAS no. 2005/30.

Lieber, H. (2010) 'The European Commission's new justice portfolio: Opportunities, goals and challenges', pp. 18-22 in: E. Guild, S. Carrera & A. Eggenschwiler (red.) *The Area of Freedom, Security and Justice ten years on. Successes and future challenges under the Stockholm Programme,* Brussel: CEPS.

Lyon, D. (2003) *Surveillance after September 11*. Cambridge: Polity Press.

Lyon, D. (2009) *Identifying citizens. ID Cards as Surveillance.* Cambridge: Polity Press.

Lyon, D. & C. Bennett (2008) 'Playing the identity card: understanding the significance of identity card systems', pp. 3-20 in: C. Bennett & D. Lyon (red.) *Playing the identity card. Surveillance, security and identification in global perspective.* London: Routledge.

Mathiesen, T. (2001) 'On globalization of control: towards an integrated surveillance system in Europe, in: *Social change and crime in the Scandinavian and Baltic Region*. Rapport från NSFKS 43. forskarseminarium, Riga 2001**.** http://www.nsfk.org/downloads/seminarreports/researchsem_no43.pdf

Mitsilegas, V., J. Monar, W. Rees (2003) *The European Union and internal security. Guardian of the people?* Houdmills, Basingstoke, Hampshire: Palgrave.

Mitsilegas, V. (2009) 'The Borders Paradox. The Surveillance of Movement in a Union without Internal Frontiers', pp. 33-64 in H. Lindahl (red.) *A Right to Inclusion and Exclusion? Normative Faultlines of the EU's Area of Freedom, Security and Justice*, Oxford: Hart Publishing.

Monar, J. (2008) 'Justice and Home Affairs', *Journal of Common Market Studies. Annual Review.* Vol. 46: 143-162.

Monar, J. (2010) 'Justice and Home Affairs', *Journal of Common Market Studies. Annual Review.* Vol. 48: 109-126.

Nationale Ombudsman (2010) *Toegang verboden. Onderzoek naar de opname van vreemdelingen in het Schengen Informatie Systeem en de informatievoorziening hierover.* Rapport 2010/115, 17 juni 2010.

Peers, S. (2000) *EU justice and home affairs law*. Harlow: Longman.

Ploeg, I. van der & I. Sprenkels (2009) 'Migratie en het machine-leesbare lichaam: identificatie en biometrie', in: H. Dijstelbloem en A. Meijer (red.) *De Migratiemachine. De rol van technologie in het migratiebeleid.* Amsterdam: Van Gennep.

Salter, M. (2008) 'Imagining numbers: Risk, quantification and aviation security', *Security Dialogue*, vol. 39, nr. 2-3: 243-266.

Snel, E. et al. (2007) *Migration and migration policies 2005. Dutch SOPEMI report 2005*. Rotterdam: RISBO.

Snijder, M. (2010) *Het biometrische paspoort in Nederland: crash of zachte landing?* WRR-webpublicaties nr. 51. Den Haag: WRR.

Stanton, J. (2008) 'ICAO and the biometric RFID passport. History and analysis', pp. 253-267 in: C. Bennett & D. Lyon (red.) *Playing the identity card. Surveillance, security and identification in global perspective.* London: Routledge.

Stevens, B. (2004) 'The emerging security economy: an introduction', in: OECD, *The security Economy*. Paris: OECD.

Torpey, J. (2000) *The invention of the passport; surveillance, citizenship and the state.* Cambridge: Cambridge University Press.

Torpey, J. (2001) 'The great war and the birth of the modern passport system', pp. 256-270 in J. Caplan & J. Torpey (red.) *Documenting individual identity. The development of state practices in the modern world.* Princeton and Oxford: Princeton University Press.

UNWTO (2007) *Tourism Market Trends 2006 edition*. Madrid: UNWTO.

UNWTO (2009) *Tourism highlights 2009 edition*. Madrid: UNWTO.

Wolf, K. (1999) 'The new *Raison d'État* as a problem for democracy in World society', *European Journal of International Relations*, vol. 5, nr. 3: 333-363.

WRR (2003) *Slagvaardigheid in de Europabrede Unie*. WRR-rapporten aan de Regering nr. 65. Den Haag: Sdu.

Zolberg, A. (2002) 'Guarding the Gates', on-line paper at http://www.newschool.edu/icmec/guardingthegates.html

8 JEUGDZORG VIA SYSTEMEN. DE VERWIJSINDEX RISICOJONGEREN ALS SPIN IN EEN DIGITAAL VANGNET

Esther Keymolen en Corien Prins

8.1 INLEIDING

"Door de komst van de verwijsindex is een proces van bewustwording in gang gezet over de noodzaak van (vroeg)signalering, de noodzaak tot samenwerking en de noodzaak tot het uitwisselen van informatie."

(Tweede Kamer 2008/09: 31 855)

In een notendop verwoordt het voorgaande citaat de ambities, maar zeker ook de beleidsovertuiging, die ten grondslag liggen aan het initiatief om met behulp van digitalisering een verbeteringsslag door te voeren in het jeugdbeleid. Naast de overtuiging dat technologie – hier de verwijsindex – daadwerkelijk een bewustwordingsproces in gang heeft kunnen zetten, spreekt uit het citaat de noodzaak tot 1) proactief signaleren en handelen en 2) meer uitwisseling van informatie tussen instanties en beleidsdomeinen om samenwerking te verbeteren. Sinds de landelijke en politieke ophef over het Maasmeisje en de kleuter Savannah is de roep vanuit zowel de samenleving als de politiek om een stringenter, efficiënter en effectiever jeugdbeleid groot. Gestroomlijnde communicatie tussen de verschillende betrokken instanties en meer duidelijkheid over verantwoordelijkheden binnen de zorgketen vormen onlosmakelijke onderdelen van het streven kinderen niet langer uit het oog te verliezen en tragedies in de jeugdzorg te voorkomen. Digitalisering is hierbij een belangrijk instrument: verschillende registratie- en informatie-uitwisselingssystemen worden als hulpmiddelen voor betere communicatie en vroegtijdig signaleren naar voren geschoven. De initiatieven stralen de overtuiging uit dat met technische maatregelen een inhoudelijk vraagstuk geadresseerd kan worden. Naast de in het voorgaande citaat genoemde verwijsindex is het bekendste andere voorbeeld hiervan het Elektronisch Kinddossier (EKD).

Met 'de verwijsindex' wordt gedoeld op de Verwijsindex Risicojongeren, een initiatief waarmee de Tweede Kamer aan de vooravond van het zomerreces 2009 in grote meerderheid akkoord ging. Ruim een half jaar later (op 2 februari 2010) stemden vrijwel alle fracties in de Eerste Kamer voor het wetsvoorstel. Daarmee werd, via een aanpassing van de Wet op de jeugdzorg (Wjz), per 1 augustus 2010 formeel voorzien in de wettelijke grondslag voor de inzet van de verwijsindex.[1] Behalve dat de regeling de grondslag biedt voor de applicatie, realiseert het een

verplichting voor gemeenten om te bevorderen dat alle in hun gemeente werkzame instanties en zelfstandige professionals worden aangesloten op de verwijsindex. Met deze wettelijke opdracht krijgen gemeenten er een specifieke preventieve taak bij, namelijk hulp aan jeugdigen met problemen op het terrein van opgroeien en opvoeden. Overigens was de nieuwe wet voor een belangrijk deel niet meer dan een formalisering van een reeds ontwikkelde praktijk: nog voordat de wet bij Koninklijk Besluit in werking trad, beschikten al zo'n 300 gemeenten over een aansluiting op het systeem, waren bijna 130.000 meldingen gedaan en bedroeg het aantal matches ruim 23.000 (Ministerie Jeugd en Gezin 2010b: 4). De minister sprak voorjaar 2010 de verwachting uit dat nog datzelfde jaar de landelijke dekking van de verwijsindex een feit zou kunnen zijn.

Wat hierna volgt is een analyse van de belangrijkste kenmerken, factoren en omstandigheden die samenhangen met de plannen voor, het opzetten en implementeren van en de omgang met deze verwijsindex. Alhoewel de analyse zich primair richt op de verwijsindex, komen ook andere ICT-initiatieven binnen de jeugdzorg in beeld. Dat de verwijsindex de rode draad vormt in het bredere betoog over digitalisering in de jeugdzorg, heeft te maken met een aantal overwegingen. Een eerste reden is dat de verwijsindex kenmerken vertoont van een 'spin in het web' en daarmee inzicht biedt in de wijze en mate waarop de belangrijkste ICT-projecten binnen de jeugdzorg al dan niet met elkaar samenhangen. Bovendien zal uit de bespreking duidelijk worden dat het initiatief voor de verwijsindex veel ruimer en daarmee in diverse opzichten ook omvattender is dan andere applicaties. Ten slotte toont zich juist bij het initiatief voor de verwijsindex de interactie tussen plannen en ambities op rijksniveau enerzijds en lokaal (provinciaal en gemeentelijk) niveau anderzijds. In deze verkenning zal specifiek op de dynamiek tussen rijksniveau en lokaal niveau worden ingegaan. Daarbij zal onder meer duidelijk worden dat de Haagse – tekentafel – wereld in vele opzichten ver verwijderd staat van de lokale realiteit.

8.2 KORTE SCHETS VERWIJSINDEX EN CONTEXT

Bij een schets van 'het hoe en waarom' van de verwijsindex is het van belang scherp voor ogen te houden dat het initiatief van de verwijsindex niet alleen een landelijke variant kent, maar ook vele tientallen lokale en regionale. Het landelijk systeem fungeert als een paraplu over alle lokale systemen, om daarmee een gestandaardiseerde uitwisseling tussen de onderliggende lokale systemen te realiseren en de signalering van risicojongeren 'dekkend' voor het gehele land te hebben. Zoals lopende het betoog duidelijk zal worden, wijkt de wijze waarop de lokale en regionale signaleringssystemen vorm en inhoud krijgen in vele opzichten af van de op centraal niveau gestelde ambities. In het onderstaande starten we met een bespreking van het landelijke paraplusysteem aan de hand van de parlementaire stukken behorende bij het wetsvoorstel Verwijsindex Risicojongeren

(31 855) en documenten die werden opgesteld naar aanleiding van de proeven met het systeem, om vervolgens in te gaan op de uitwerking op lokaal niveau.

8.2.1 MELDEN VAN RISICO, NIET INHOUD

De landelijke verwijsindex faciliteert risicomeldingen van jeugdigen tot 23 jaar. Het gaat daarbij om jeugdigen bij wie zich zodanige problemen voordoen dat hun persoonlijke ontwikkeling wordt bedreigd en zij buiten de maatschappij dreigen te vallen. De gedachte achter het initiatief is dat hulpverlenende instanties van elkaar vaak niet weten dat ze met dezelfde jongere aan het werk zijn, waardoor de hulp onderling niet goed afgestemd kan worden. Via de inzet van het systeem beogen bestuurders en uitvoerende instanties dit veelal slepende probleem aan te pakken. Ook kan het verzamelen van risicosignalen uit verschillende hoeken aan het licht brengen hoe ernstig de problematiek van een jeugdige werkelijk is en kan gericht optreden hierdoor eerder plaatsvinden.

Aan de verwijsindex wordt uitsluitend doorgegeven dát er een melding is gedaan. Het adres en de geboortedatum van de jeugdige, de datum van de melding samen met de identificatiegegevens en contactgegevens van de meldende instantie worden daartoe in het systeem geregistreerd. Pas wanneer er twee of meerdere signalen over een en dezelfde persoon zijn afgegeven in het systeem, wordt er een verbinding gelegd tussen de verschillende meldende instanties. Er is dan sprake van een *match*. Dus: een school doet een melding aan de verwijsindex over een bepaalde jeugdige, waarna de school via de verwijsindex wordt geïnformeerd dat andere professionals ook al bij de zorg rondom deze jeugdige betrokken zijn.

Professionals krijgen geen inzage in achterliggende kenmerken van de andere meldingen. Zij krijgen alleen een signaal dat ook een andere professional dezelfde jeugdige heeft gemeld. Bij dat signaal is niet aangegeven om welk risico het gaat. Daarvoor moeten de professionals in persoon contact met elkaar opnemen. Of er op dat moment verdere inhoudelijke gegevens mondeling of schriftelijk mogen worden uitgewisseld is afhankelijk van het voor de betrokken professionals geldende wettelijk regime (Wet bescherming persoonsgegevens; Wet geneeskundige behandelingsovereenkomst, enz.). In tegenstelling tot initiatieven gericht op digitalisering van dossiers (zoals het Elektronisch Kinddossier (EKD) en Elektronisch Patiëntendossier (EPD)) worden dus geen dossier- of inhoudelijke gegevens met tussenkomst van de landelijke verwijsindex uitgewisseld. Natuurlijk kan – zoals door de minister ook werd erkend bij de parlementaire behandeling – op basis van de gegevens over het type afzender van een risicomelding (jeugdpsychiater, schuldhulpverlening, functionaris schoolverzuim, enz.) wel indirect het een en ander aan inhoudelijke informatie worden afgeleid.

8.2.2 WANNEER MAG MEN MELDEN?

Een meldingsbevoegde professional kan uitsluitend een jeugdige aan de verwijsindex melden als hij een redelijk vermoeden heeft dat een of meer van de in artikel 2j van de Wet op de jeugdzorg limitatief opgesomde risico's aanwezig is, waardoor de jeugdige in zijn ontwikkeling naar volwassenheid wordt belemmerd. De meldingsbevoegde dient hierbij te allen tijde een zorgvuldige afweging te maken alvorens een jeugdige aan de verwijsindex te melden, waarbij alle bekende beïnvloedende omstandigheden moeten worden gewogen. Een en ander betekent dat het antwoord op de vraag wanneer mag worden gemeld wordt bepaald door 1) aanwezigheid van een gespecificeerd risico; 2) een zorgvuldige afweging; en 3) een redelijk vermoeden. Geen beperkend criterium is het bestaan van een behandelrelatie: de professional mag zoals we later in dit betoog nader zullen bespreken, ook een risico melden waarover hij professioneel gezien verder 'niet gaat', mits hij op basis van de feiten tot een redelijk vermoeden is gekomen dat het betreffende probleem speelt.

Gemeenten is het niet toegestaan eigenstandig andere risico's te benoemen dan degene die in de wet genoemd staan. Andere risico's mogen dus niet geformuleerd worden in bijvoorbeeld lokale samenwerkingsconvenanten. Wat wel mogelijk – en naar de mening van de minister zelfs wenselijk – is, is dat beroepsgroepen de vastgestelde meldcriteria verder uitwerken en nader inkleuren voor hun specifieke werkveld. Om hulpverleners hierbij te ondersteunen publiceerde het ministerie op 6 april 2009 de handreiking 'meldcriteria'.[2] Bij de totstandkoming van deze handreiking zijn de ketenpartners nauw betrokken geweest. Door concrete situaties te beschrijven beoogt de handreiking een denkrichting voor de professional te bieden bij de afweging een jeugdige aan de verwijsindex te melden. Expliciet is beoogd dat de handreiking wordt doorontwikkeld aan de hand van de nadere inkleuring die door professionals en beroepsgroepen wordt gegeven aan de meldcriteria: "De handreiking 'meldcriteria' is dus niet statisch, maar dynamisch en zal voortdurend verder worden ontwikkeld, geïnterpreteerd en ingekleurd. Omdat de ontwikkelingen in de brede jeugdketen niet stil staan, kan doorontwikkeling van de meldcriteria door afzonderlijke beroepsgroepen enkel worden toegejuicht."[3]

Artikel 2j

De in artikel 2j limitatief opgesomde risico's zijn breed geformuleerd en strekken zich uit van geestelijk, lichamelijk of seksueel geweld, veelvuldig schoolverzuim tot tienermoederschap. Dat is om twee redenen gedaan, aldus de parlementaire stukken: "Ten eerste laat de brede formulering de verschillende beroepsgroepen, die met de verwijsindex te maken krijgen, de ruimte voor interpretatie, zodat de uiteindelijke afweging een jeugdige te melden wordt gemaakt door een professional die dicht bij de jeugdige staat. Ten tweede biedt de brede formulering de mogelijkheid nu nog niet als zodanig geïdentificeerde risico's in de toekomst te herken-

nen in één van de in artikel 2j opgesomde risico's."[4] Het wekt geen verwondering dat zowel de Raad van State als enkele fracties in de Tweede Kamer kritiek hebben geuit op de brede formulering.[5] Eenduidig, meetbaar en herleidbaar: daaraan moeten volgens het Kamerlid Dezentjé Hamming de criteria voor het melden van risico's in de verwijsindex voldoen.[6] De risico's zijn volgens haar nu te vaag geformuleerd. Diverse Kamerleden sloten zich daarbij aan en dienden moties in ter nadere afbakening van de criteria, mede bedoeld om op landelijk niveau meer sturing te geven aan de nadere ontwikkeling van criteria op lokaal niveau.[7]

Een omstreden risico dat opgenomen is in deze lijst heeft betrekking op etniciteit. In het artikel 2j wordt vastgesteld dat 'als de jeugdige bloot staat aan risico's die in bepaalde etnische groepen onevenredig vaak voorkomen' dit een reden voor melden is. Deze specifieke regeling ontbrak in het oorspronkelijke wetsvoorstel, maar is toegevoegd na een motie vanuit de Tweede Kamer. Hiermee is er een opening gekomen die waarschijnlijk strijdig is met het non-discriminatieverbod, zoals neergelegd in richtlijn 2000/43/EG. Deze verplicht lidstaten maatregelen te nemen tegen ongeoorloofd direct en indirect onderscheid op grond van ras of etnische afstamming, onder meer op het terrein van de sociale bescherming. Maatregelen zijn alleen dan toegestaan wanneer ze objectief worden gerechtvaardigd door een legitiem doel en ze voor het bereiken van dat doel passend en noodzakelijk zijn. Bij een vermoeden van discriminatie moet conform artikel 8 richtlijn zijn aan te tonen dat het beginsel van gelijke bescherming niet is geschonden. Zonder enige inhoudelijke discussie over de verhouding tot deze en andere discriminatieverboden, heeft de Tweede Kamer de voornoemde motie echter aangenomen.

Bovendien zijn relevante instanties, zoals het College bescherming persoonsgegevens (CBP) niet in de gelegenheid gesteld te adviseren toen de minister besloot de motie op te volgen. De minister vond dat niet nodig. Deze opstelling heeft waarschijnlijk alles te maken met zijn (ook in de MvA te vinden) opvatting dat er in het geval van de verwijsindex geen sprake is van registratie op grond van etniciteit. Maar welke hulpverlener zal een signaal afgeven zonder de aanleiding hiervoor gedocumenteerd te hebben (en dus gegevens over etniciteit te registreren)? Welke professional zal, wanneer hij door een derde op de hoogte wordt gebracht van de (etnisch gerelateerde) problemen, dit vervolgens niet ook weer in zijn digitale dossier aantekenen? Zorgvuldige hulpverlening verlangt immers goede documentatie. En daarmee is de feitelijke registratie van gegevens over etnische herkomst door een bont gezelschap van organisaties (in sommige lokale verwijssystemen participeren meer dan 40 instanties) een feit (Prins 2010).

8.2.3 VAN PROEFTUIN NAAR WET

Het wetgevingstraject rondom de landelijke verwijsindex vormde niet het vertrekpunt voor het initiatief. In feite is de Wet Verwijsindex Risicojongeren het sluit-

stuk van een traject dat in oktober 2007 een aanvang nam via een zogenaamde proeftuin. Diverse gemeenten experimenteerden in deze proeftuin met het systeem. Medio 2008 waren na een klein jaar werken in onder andere Rotterdam, Almere en Gouda, ruim 43.000 meldingen aan het systeem gedaan, die meer dan 6.000 matchen opleverden. In mei 2009 was het aantal meldingen ruim 67.000, waarvan er meer dan 10.000 resulteerden in een match. Ongeveer honderd gemeenten waren op dat moment aangesloten bij de proeftuin. In december 2008 vond een eerste evaluatie plaats waaruit bleek dat het draagvlak voor de verwijsindex groot was. Wel kwam een aantal aandachtspunten naar voren. Deze sloegen terug op zaken als privacy, de rechten van de jeugdige en diens ouders, de vertaalslag naar de werkvloer waar daadwerkelijk moet worden gewerkt met de verwijsindex en technische problemen bij de lokale systemen.

De minister liet naar aanleiding van de evaluatie weten een aantal acties in gang te hebben gezet om de aandachtspunten aan te pakken (waaronder: het laten ontwikkelen van een privacywegwijzer die professionals inzicht biedt welke informatie met wie mag worden uitgewisseld; het verstrekken van nadere informatie over de rechten van de jeugdige). De privacywegwijzer is inmiddels als internettoepassing voor een beperkt aantal betrokkenen (Bureau Jeugdzorg en de Raad voor de Kinderbescherming) beschikbaar (Verwijsindex 2010). We zien dus dat technologie hier wordt ingezet om op laagdrempelige, eenduidige en breed beschikbare wijze de professionals bij hun werkzaamheden te ondersteunen.

Behalve experimenteren in de proeftuin is tijdens de opstartfase van het project ook gewerkt aan een nadere uitwerking van de criteria voor het melden van een risico. Op 6 april 2009 presenteerde de minister voor Jeugd en Gezin de eerdergenoemde Handreiking meldcriteria, opgesteld in overleg met diverse betrokkenen (waaronder brancheorganisaties als GGZ Nederland en de Landelijke Huisartsen Vereniging). Deze criteria, verdeeld over vijf domeinen: materiële omstandigheden, gezondheid, opvoeding en gezinsrelaties, onderwijs en werk, en sociale omgeving buiten het gezin en school, zijn voor iedereen te raadplegen op de website www.meldcriteria.nl. Deze meldcriteria zijn geen uitgewerkte risicoprofielen, maar vormen slechts een leidraad voor de lokale instanties om hun eigen meldingsbeleid vorm te geven.

8.2.4 IEDERE LOKALE CONTEXT EEN EIGEN SYSTEEM

Zoals we hiervoor al aangaven, kent de verwijsindex zowel een landelijke als een lokale variant. De vanuit het projectministerie Jeugd en Gezin geïnitieerde Verwijsindex Risicojongeren (VIR) beoogt op landelijk niveau op gestandaardiseerde wijze signaleringsinformatie uit te wisselen tussen de verschillende gemeentelijke en lokale verwijssystemen die daar reeds zijn of worden ingericht. Uit de brief over de VIR en het Elektronisch Kinddossier die toenmalig staatssecretaris Ross

eind 2005 naar de Tweede Kamer stuurde, vallen grofweg drie argumenten op te maken voor het invoeren van een Verwijsindex Risicojongeren (Ministerie voor Jeugd en Gezin 2005). Ten eerste weten instanties vaak niet van elkaar dat ze met dezelfde jongere aan het werk zijn waardoor de hulpverlening niet goed op elkaar wordt afgestemd. De tragedie van 'het Maasmeisje' is een pijnlijke illustratie van de desastreuze gevolgen die voortvloeien uit een gebrek aan overzicht van en coördinatie tussen hulpverlenende instanties. Ten tweede krijgen hulpverleners door het verzamelen van diverse risicosignalen een vollediger beeld van de ernst en complexiteit van de problematiek waarmee de jeugdige te maken heeft. Dit gelaagde beeld maakt het mogelijk vroegtijdig in te grijpen. Ten slotte blijkt, zoals eerder gemeld, dat probleemjongeren vaak verhuizen waardoor de continuïteit van de zorg bedreigd wordt. Een VIR op landelijk niveau zou dit probleem kunnen ondervangen. De regering ziet het als haar taak om jeugdigen met problemen actief en tijdig te helpen.

De gedachte achter de aanvullende verwijssystemen op regionaal en gemeentelijk niveau is dat de lokale systemen vorm kunnen krijgen op basis van de vragen en behoeften die door het plaatselijke bestuur aangedragen worden. Wat een speerpunt is in de jeugdzorg van een grote stad hoeft dit niet te zijn op het platteland. Bovendien was er al een aantal gemeenten en regio's dat – alvorens sprake was van een landelijke verwijsindex – zelf reeds een lokale index had ontworpen en in werking had genomen. Deze lokale indexen terzijde schuiven en opnieuw beginnen bleek niet opportuun. Voor de gemeenten en de betrokken jeugdzorginstanties werd er dan ook een duidelijke opening geboden om de bestaande signaleringssystemen te handhaven en naar eigen inzicht en ervaring verder vorm te geven. Zo kunnen er naast de basismodule waarin signaleren, matchen en aansluiten op het landelijk systeem mogelijk is, ook aanvullende lokale behoeften worden gerealiseerd. De lokale beheersorganisatie Multisignaal, waarvan tal van gemeenten deel uitmaken, noemt in dit verband: het attenderen van mogelijke partners op aankomende acties betreffende een jeugdige, het samenstellen van groepen zoals gezinnen of hangjongeren of de regie bij een casus nader regelen (Multisignaal 2010). Zoals we hierna zullen zien, zijn de lokale signaleringssystemen dan ook vaak uitgebreider dan het landelijk initiatief. Uitgebreider in zowel functionaliteit als ook het type informatie dat wordt gegenereerd. Alvorens overigens aangesloten te kunnen worden op de landelijke verwijsindex moet een lokaal systeem gecertificeerd zijn, zoals de systemen Multisignaal, Zorg voor Jeugd en VIS2 dat zijn. Deze certificatie behelst voornamelijk het voldoen aan technische vereisten.

De praktijk laat kortom een kleurrijk digitaal landschap zien waarin elke gemeente vanuit haar eigen behoeften en doelstellingen een lokaal verwijssysteem opbouwt en inkleurt. Inkleuren geeft hierbij mooi weer dat er ook niet altijd uitsluitend uit het niets een systeem ontwikkeld wordt. Vaak wordt een al bestaand systeem

aangepast of worden reeds ontwikkelde modulen en systemen aangehaakt op het basissysteem.

8.2.5 AMBITIES OP RIJKSNIVEAU: PREVENTIEF INGRIJPEN DOOR GESTROOMLIJNDE INFORMATIE-UITWISSELING

Preventie

Op rijksniveau wordt met het verzamelen en uitwisselen van risicosignalen expliciet beoogd in een vroeg stadium de ernst van de problematiek van jeugdigen in beeld te brengen, waardoor optreden ook in een vroeg stadium plaats kan vinden. Kortom, de verwijsindex moet preventief handelen mogelijk maken, zodat via een vroegtijdige en onderlinge afstemming tussen hulpverleners jeugdigen tijdig de passende hulp, zorg of bijsturing kan worden gegeven. In de beleidsagenda 2009 van het programmaministerie valt de VIR dan ook onder de doelstelling 'omslag naar preventie'. Door het vroeg signaleren van problemen door middel van een verbeterde informatie-uitwisseling wil het kabinet ernstige opvoedingsproblemen en misstanden waarbij jongeren betrokken zijn voorkomen (Ministerie voor Jeugd en Gezin 2008a: 15). Binnen het beleid van de overheid (zoals onder meer neergelegd in de ambitie 'Veiligheid Begint Bij Voorkomen') zijn preventie, bestuurlijke en strafrechtelijke handhaving en nazorg daarbij de kernelementen (Kamerstukken II 2007/08a). De noodzaak tot preventief optreden wordt door het kabinet met diverse argumenten onderbouwd. Het is de taak van de overheid burgers veiligheid te bieden. 'Veiligheid' (in de zin van veilig opgroeien) en 'voorkomen' (in de zin van een preventieve aanpak) zijn als belangrijke aanknopingspunten ook terug te vinden in het beleidsprogramma van het ministerie voor Jeugd en Gezin.

Vanuit een juridisch perspectief wordt de basis voor de taakopvatting onder meer gevonden in het leerstuk van verplichtingen die uit vrijheidsrechten voortvloeien. Met andere woorden, de fundamentele en in het Europees Verdrag voor de Rechten van de Mens (EVRM) verankerde vrijheidsrechten verlangen van de overheid dat ze actief zorg draagt voor een maatschappij waarin burgers zich vrij voelen in hun handelen en aldus geen bedreiging ervaren vanuit bijvoorbeeld criminaliteit, terrorisme en verstoring van de openbare orde. Illustratief is de volgende opmerking in de parlementaire stukken bij de verwijsindex: "Volgens het EHRM mag van de autoriteiten worden verwacht dat informatie met betrekking tot de verschillende problemen bij elkaar wordt gebracht. Uit de overweging van het EHRM blijkt dat voortschrijdend wetenschappelijk inzicht de aansprakelijkheid van de staat voor tekortkomingen in de kinderbescherming kan verhogen."[8] Hoe ruim deze taakopvatting – en daarmee de reikwijdte van preventief handelen – is, wordt duidelijk als we de invulling door de regering van het begrip gezondheid bekijken: "Voor de invulling van het begrip gezondheid sluit het voorstel aan bij de definitie van de wereldgezondheidsorganisatie: Gezondheid is de toestand van volledig lichamelijk, geestelijk en maatschappelijk welzijn en niet slechts de afwezigheid

van ziekte of andere lichamelijke gebreken. Het gaat dus om de kwaliteit van leven in het algemeen, waarbij ook een rol speelt of de jeugdige voldoende kansen krijgt in de maatschappij, bijvoorbeeld voor het volgen van een opleiding of het hebben van een baan. Het hoeft dus niet per definitie te gaan om een bedreiging van het leven en de veiligheid van een jeugdige om aan het criterium van noodzakelijkheid in een democratische samenleving te kunnen beantwoorden, maar ook, of juist vooral ook om de kwaliteit van leven in ruime zin."

Efficiënte informatie-uitwisseling

De inzet op preventief en vroegtijdig ingrijpen in de jeugdzorg moet mogelijk worden gemaakt door een gestroomlijnde informatie-uitwisseling tussen hulpverleners. Zij moeten effectief kunnen werken en meer duidelijkheid hebben over wat te doen bij risicokinderen. Trefwoorden die in de parlementaire stukken worden gehanteerd zijn: snel, eerder, beter, duidelijk. In de Nota naar aanleiding van het verslag merkt de minister voor Jeugd en Gezin onder meer op: "Met de verwijsindex krijgen de professionals in het veld een instrument in handen om snel op de hoogte te worden gebracht van elkaars betrokkenheid bij een jeugdige.

Op die manier krijgen jeugdigen die in de problemen zitten eerder en beter afgestemde hulp, zorg of bijsturing. Voor de professionals betekent de komst van de verwijsindex ook dat er meer duidelijkheid komt op het punt van risicosignalering."[9] En: "Door het wetsvoorstel verwijsindex risico's jeugdigen is er straks een duidelijk kader voor het doen van meldingen. Deze duidelijkheid ontbreekt op dit moment bij veel professionals. Door het instellen van de verwijsindex wordt het risico dat belangrijke waarnemingen van professionals uitsluitend terechtkomen in een dossier en er verder niets mee gebeurt dus kleiner."[10] De doelstelling aan professionals meer duidelijkheid (en via het wetsvoorstel ook rechtszekerheid) te bieden, beoogt te voorkomen dat ten onrechte geen melding van risico's wordt gedaan. De minister merkt in dit verband op dat door de bevoegdheid tot melden te expliciteren, er voor de professionals een einde komt aan de onzekerheid, namelijk de vraag of het wel of niet is toegestaan om bepaalde risico's te melden. Bovendien wil de regeling verandering brengen in de positie van geheimhouders (bijv. artsen). Zonder een wettelijk vastgelegd meldrecht zouden zij zich hier niet op kunnen beroepen, wat betekent dat ze voor het doen van een melding toestemming moeten vragen aan de jeugdige of zijn ouders, of zich in een uiterste geval op een conflict van plichten moeten beroepen.

Om de gestroomlijnde informatie-uitwisseling tot stand te brengen is op rijksniveau gekozen voor een kaal systeem. Er behoeft immers uitsluitend te worden gemeld dat er een melding is. Alle verdere relevante informatie behoeft pas op het persoonlijker niveau tussen de betrokken professionals uitgewisseld te worden, bijvoorbeeld via een gesprek of telefonische bespreking. Ondanks de vraag van onder meer de vier grote steden, Rotterdam, Amsterdam, Den Haag en Utrecht,

om de verwijsindex uit te breiden, bijvoorbeeld door een koppeling te maken naar het Elektronisch Kinddossier (wethouders Jeugd van Amsterdam, Utrecht, Rotterdam en Den Haag 2007), werd dit voorstel tot uitbreiding van de VIR door de betrokken minister dan ook afgewezen. Uit onderzoek naar de gevolgen van een dergelijke koppeling werden diverse privacybezwaren ingebracht. Tevens werd vastgesteld dat de werkvloer nog niet toe was aan een integratie van de verschillende middelen en systemen (Ministerie voor Jeugd en Gezin 2008b). Verder is handhaving en openbare orde problematiek expliciet buiten de doelstelling van de verwijsindex gehouden (Nota naar aanleiding van het verslag). Zowel het College bescherming persoonsgegevens als de Raad van State hebben in hun adviezen aangegeven dat de verwijsindex niet uitgebreid diende te worden naar het domein van de openbare orde.

8.2.6 EEN DIVERS PALET AAN AMBITIES OP LOKAAL NIVEAU

Hoe anders is het als we kijken naar de ambities op lokaal niveau. Op lokaal niveau is het expliciet de bedoeling de verwijssystemen aan te passen aan de behoeften van de plaatselijke context. Het is dan ook niet zo verrassend dat behalve de rijksdoelstellingen van preventief en vroegtijdig ingrijpen via een gestroomlijnde informatie-uitwisseling op lokaal niveau tal van andere ambities vorm krijgen. Zo liggen de doelstellingen van SISA – wat staat voor signaleren en samenwerken – het lokale signaleringssysteem van onder andere Rotterdam, met name op het organisatorisch niveau (Keymolen & Broeders 2010a: 74). Op de website van SISA staan vier doelstellingen. Ten eerste wil men het beleid binnen organisaties verbeteren. Ten tweede zet men in op een sluitende aanpak tussen verschillende organisaties. Ten derde moeten op (deel)gemeentelijk niveau de aanpak en samenwerking sluitend worden. Als laatste wil men de methoden om hardnekkige problematiek aan te pakken verder ontwikkelen.[11] Bij Zorg voor Jeugd, het lokale signaleringssysteem van onder meer Noord-Brabant, worden maar liefst zes kernfuncties genoemd: signaleren, ketenregistraties, berichtenuitwisseling, zorgcoördinatie, rapportage en archivering. Daarnaast beschikt het systeem ook over de nodige beheersfuncties. Ondanks de verschillende ambities tussen de regio's zijn er wel degelijk verscheidene zwaartepunten aan te wijzen die op lokaal niveau bepalend zijn voor de inrichting van de verwijssystemen.

Een uitgebreid net van hulpverleners

De instanties die aan de landelijke verwijsindex mogen melden zijn bij Besluit van 13 juli 2010 vastgesteld.[12] Dit zijn instanties die werkzaam zijn in de domeinen jeugdzorg, de jeugdgezondheidszorg, onderwijs, de maatschappelijke ondersteuning, werk en inkomen en politie en justitie. Het gaat hierbij met name om Bureaus Jeugdzorg, Jeugd-GGZ, GGD'en, consultatiebureaus, scholen, regionale meld- en coördinatiepunten, leerplichtambtenaren, MEE-organisaties[13], instanties voor sociaal maatschappelijk werk, schuldhulpverlening, de politie, bureaus halt,

de raad voor de kinderbescherming.[14] Naast deze partijen zijn er op lokaal niveau echter ook andere actoren betrokken, zoals peuterspeelzalen en verloskundigen, die wel risicosignalen uitzenden in het lokaal systeem, maar niet meldingsbevoegd zijn voor het landelijke systeem.[15] Deze plaatselijke actoren worden echter op lokaal niveau aangemerkt als noodzakelijk voor een sluitende jeugdhulpverlening. Hun signalen worden dus wel op lokaal niveau verwerkt, maar gaan niet de nationale index in. Dit betekent dat op basis van hun signalen er geen matchen kunnen ontstaan op interregionaal niveau, maar wel binnen het lokale convenantgebied. Op lokaal niveau ontstaat er dus een veel omvangrijker netwerk van aan elkaar verbonden hulpverleners die de jeugdige op het netvlies krijgen. De verschillende instanties worden als het ware elkaars *deputy sherrifs* (Torpey 2000; Lahav & Guiraudon 2000). Hun observaties en acties krijgen gewicht buiten het eigen professionele domein en ze worden verantwoordelijk gemaakt voor zaken die buiten het eigen beleidsveld liggen (zie ook Garland 2001). Hoewel kinderen en jongeren natuurlijk altijd al door verschillende actoren in de gaten worden gehouden, transformeert de lokale index deze 'analoge ogen' in 'digitale ogen' waardoor datgene wat gezien wordt door één, ook bruikbaar is voor anderen (Keymolen & Broeders 2010b: 13).

Een uitgebreide functionaliteit

Naast de 'kale' signaal- en meldfunctie van de landelijke verwijsindex bestaan er op lokaal niveau ook tal van andere functionaliteiten. Zo wordt in het lokale systeem Zorg voor Jeugd, dat in Noord-Brabant, Groningen en de Drechtsteden wordt gebruikt, ook aan ketenregistratie gedaan. Alle jeugdigen die aankloppen bij een instantie met een hulpvraag welke voldoet aan de risico's zoals ze zijn omschreven in het eerder besproken artikel 2j, worden in het systeem geregistreerd. Hierdoor kan er in kaart worden gebracht hoeveel jeugdigen in de regio hulpzoekend zijn en bij wie zij in eerste instantie terechtkomen. Ook maakt ketenregistratie het mogelijk een completer beeld te verkrijgen van het hulptraject dat een jeugdige doorloopt. "De instellingen die bij een bepaalde jeugdige zijn betrokken, worden automatisch via een mailbericht geïnformeerd als dezelfde jeugdige door een nieuwe, nog niet eerder betrokken instelling, wordt geregistreerd. Daarmee hebben de instellingen en hulpverleners continu inzicht in de instellingen die contact hebben met de jeugdige en wordt ketenregistratie opgebouwd."[16]

Een weer andere uitbreiding van de functionaliteit treffen we in Rotterdam aan. In SISA, het lokale systeem van onder meer deze stad, kent men namelijk de mogelijkheid van het afgeven van presignalen ofwel niet-pluis-signalen. De presignalen worden gebruikt in de lokale index om eventuele zorgen met andere hulpverleners over een bepaalde jeugdige te delen. Wanneer een professional een presignaal invoert in de lokale index, ontvangt hij een e-mailbericht met daarin een overzicht van al de mogelijk aanwezige presignalen, signalen en matchen over de desbetreffende jeugdige.[17] Deze presignalen zijn niet gebaseerd op een risicoprofiel, leiden

niet tot een match en worden dus ook niet naar de landelijke verwijsindex gestuurd waar alleen risicosignalen die voldoen aan de in de wet vastgelegde eisen in terecht mogen komen.[18] Omdat een presignaal dus niet tot een match kan leiden, hoeven kinderen en ouders hiervan ook niet op de hoogte te worden gebracht, wat bij een 'echte' match wel het geval is. Met dit systeem van presignalen ontstaat op lokaal niveau een subsysteem onder de nationale Verwijsindex Risicojongeren met een eigen werking en doelstelling (Keymolen & Broeders 2010b).

Genereren managementinformatie

Geen expliciete doelstelling op rijksniveau, maar wel op lokaal niveau is het genereren van managementinformatie met behulp van de verwijsindex. Zowel professionals kunnen via deze functionaliteit hun eigen statistieken genereren en zo een overzicht verkrijgen van de *caseload*, aantal afgegeven signalen en matchen, alsook toezichthouders kunnen via tal van statistieken het reilen en zeilen in de lokale index controleren. Zo worden op basis van door het systeem gegenereerde gegevens in de regio Rotterdam de wethouder en het college ingelicht over de stand van zaken binnen de jeugdzorg. Er kan hierbij uitgesplitst worden hoeveel signalen per deelgemeente worden afgegeven en door welke instantie dit gebeurt, of het om een jongen of meisje gaat en in welke leeftijdscategorie die zich bevindt. Het systeem is dan ook zodanig ingericht dat het een expliciet doel is om op basis van de gegenereerde data beleidsadviezen te kunnen geven. De aangeleverde statistieken maken het immers mogelijk om als het ware toezicht te houden op de aangesloten instanties en hun meldgedrag. Dit toont zich bijvoorbeeld in de Rapportage SISA 2de kwartaal 2010 waar er wordt opgemerkt dat het Centrum voor Jeugd en Gezin een daling laat zien in het aantal afgegeven signalen ten opzichte van het eerste kwartaal. Men geeft aan: "Op dit moment wordt bekeken waar die daling vandaan komt."[19] De stroom aan statistieken die het systeem aanlevert maakt een continue monitoring en evaluatie van het werkveld mogelijk.

Een adequate informatievoorziening vormt, zoals we hiervoor al opmerkten, bij de jeugdzorg een slepend probleem. Niet alleen de tragische gebeurtenissen binnen de jeugdzorg van enkele jaren geleden, maar ook onderzoek illustreert de problemen. Zo concluderen onderzoekers van het Nederlands Instituut voor Zorg en Welzijn (NIZW) in 2004 dat het niet eenvoudig is valide en betrouwbare conclusies te trekken over de jeugdzorg in ons land, omdat er sprake is van een duidelijk informatietekort (De Graaf et al. 2005). Als reden hiervoor wordt gewezen op het gebrek aan samenhang tussen de deelsectoren binnen de jeugdzorg, met als gevolg dat er met een diversiteit aan systemen en indelingen wordt gewerkt. Bovendien registreren veel instellingen in de jeugdzorg gebrekkig dan wel leveren zij gegevens moeizaam aan andere betrokken instellingen aan. Het gevolg van dit informatietekort is dat de validiteit en betrouwbaarheid van de gegevens over problemen van jeugdigen nogal problematisch is, aldus het rapport. In een rapport van het Wetenschappelijk Instituut voor het CDA wordt de gebrek-

kige informatievoorziening in verband gebracht met de grote onevenwichtigheid die er in de jeugdzorg is in aandacht (en dus middelen) voor bepaalde leeftijdsgroepen. Een betere informatievoorziening binnen de jeugdzorg biedt mogelijkheden meer zicht te krijgen op de mogelijke scheefgroei, de consequenties daarvan en de eventuele noodzaak tot een bijstelling (De Graaf et al. 2005: 72). Het wekt aldus geen verwondering dat bij de introductie van niet alleen de verwijsindex, maar ook andere projecten een direct verband wordt gelegd met het probleem van de gebrekkige informatievoorziening. De meerwaarde van juist de technologische dimensie aan een beter gestroomlijnd informatiebeleid wordt gezien in de noodzaak te werken volgens vastgelegde protocollen, waarbij geautomatiseerde verificatie een belangrijke functie heeft in het opschonen van gegevens.

Systeembeslissingen

Wanneer er in de Verwijsindex Risicojongeren een match plaatsvindt, wordt er door de index een e-mailbericht verstuurd naar de betrokken hulpverleners. Het systeem controleert echter niet of en hoe de hulpverleners met elkaar contact opnemen. Bij verschillende lokale systemen zien we dat taken die van oudsher werden uitgevoerd door de professionals, bijvoorbeeld op het vlak van management en toezicht, overgenomen worden door het systeem (Keymolen & Broeders 2010a). Zo stuurt het lokale SISA-systeem automatisch een brief naar de ouders of jongere wanneer er een match in het systeem heeft plaatsgevonden. Ook bewaakt SISA de voortgang van het zorgproces en kan het eventueel rappels sturen naar de desbetreffende instanties (SISA 2009). In het Zorg voor Jeugd-systeem zijn alle mogelijke regionale samenwerkingsverbanden in kaart gebracht en wordt bij een match automatisch door het systeem een hoofdregisseur aangewezen die verantwoordelijk is voor de coördinatie van de zorg. Deze tendens van een systeem dat steeds meer sturend wordt, duiden Bovens & Zouridis (2002) met de term *system-level bureaucracy*. De ICT en de automatische beslissingen die het systeem neemt, worden in toenemende mate bepalend voor de wijze waarop samenwerking en toezicht plaatsvindt (Keymolen & Broeders 2010a).

8.3 DE ACTOREN IN BEELD

Het rijkgeschakeerde landschap aan systemen, hun gebruikers en de daarvoor verantwoordelijken resulteert in een breed palet aan organisaties en personen die op de een of andere wijze allemaal hun rol spelen dan wel (direct of indirect) met de applicatie te maken hebben. In het onderstaande komen de meest relevante partijen in beeld. Zoals eerder aangegeven, ligt een primaire doelstelling van de verwijsindex op het terrein van de gezondheid in ruime zin (zorg, hulp en bijsturing voor jeugdigen). Dat impliceert een evenzeer ruim bereik van relevante beleidsdomeinen, wat vervolgens een bont gezelschap van meldende instanties aan boord haalt. Wie de parlementaire stukken over de proeftuin erop naleest, ontwaart een groot aantal domeinen van waaruit direct dan wel indirect signalen

worden uitgewisseld: jeugdzorg, jeugdgezondheidszorg, gezondheidszorg, onderwijs, maatschappelijke ondersteuning, werk en inkomen, politie en justitie. Op het concretere niveau van actoren gaat het om de in subparagraaf 8.2.6 genoemde instellingen en organisaties als Bureaus Jeugdzorg, de GGD, consultatiebureaus, MEE-organisaties, instanties voor sociaal-maatschappelijk werk, de politie, bureaus halt, de raad voor de kinderbescherming, scholen, schoolartsen, regionale meld- en coördinatiepunten en leerplichtambtenaren.

Kenmerkend voor de ontwikkeling van de verwijsindex zijn in ieder geval twee zaken: 1) iedere gemeente en/of regio trekt min of meer zijn eigen plan, en 2) van meet af aan is sprake van nauwe samenwerking tussen lokale beleidsmakers enerzijds en leveranciers en ontwikkelaars van systemen anderzijds. Laten we vanuit deze vaststellingen daarom beginnen met de actor die in diverse opzichten leidend is bij het initiatief en de verdere ontwikkeling en inzet van het systeem: de gemeenten (soms regio en/of provincie).

8.3.1 GEMEENTEN

De prominente rol die bij de verwijsindex aan het lokaal bestuur is toebedeeld krijgt op meerdere fronten gestalte. Gemeenten moeten zelf keuzes maken wat betreft leverancier en inrichting van het systeem. Daarnaast zijn ze ook grotendeels vrij bij de keuzes rondom de doelstellingen en reikwijdte van het systeem. Leidende overweging is dat daarmee de gemeenten en regionale samenwerkingsverbanden beter kunnen inspelen op lokale noden en aldus kunnen kiezen voor de best daartoe geëquipeerde systemen. Illustratief is de volgende opmerking van minister Rouvoet in een landelijk dagblad: "Met Leonard Geluk (voormalig CDA-wethouder Jeugd in Rotterdam) heb ik al lang afspraken gemaakt: hij heeft veel meer ruimte om dingen in zijn eigen gemeente te doen. Als Lodewijk Asscher (PvdA-wethouder Jeugd in Amsterdam) dat ook wil, laat hem maar langskomen" (*de Volkskrant*, 15 januari 2009). Bekende lokale initiatieven zijn het al eerder genoemde SISA in de stadsregio Rotterdam en Zorg voor Jeugd in Noord-Brabant, maar ook het Matchpoint-initiatief in de regio Amsterdam (Dienst Maatschappelijke Ontwikkeling 2010). Illustratief voor de lokale overwegingen is de opmerking die door de verantwoordelijken voor Matchpoint wordt gemaakt: "Amsterdam heeft ervoor gekozen zelf een verwijsindex te ontwikkelen, omdat de VIR vooral een landelijke basisvoorziening en 'ruggengraat' voor risicosignalering levert. De VIR ondersteunt geen ketenregie en is niet ontwikkeld om tegemoet te komen aan de wensen en afspraken van lokale samenwerkingsverbanden" (Dienst Maatschappelijke Ontwikkeling 2010).

Kijken we wat scherper naar de verschillende rollen die gemeenten bij de lokale verwijsindex spelen, dan zien we dat zij opereren als 1) verantwoordelijke en regievoerder, 2) opdrachtgever en risicodragend ondernemer, en 3) beheerder. Bij

deze laatste rol gaat het primair om functioneel beheer, waarmee een nadere bespreking in deze studie minder relevant is. Een nadere uiteenzetting over de rollen van verantwoordelijke respectievelijk risicodragend ondernemer is dat daarentegen wel.

Rol van verantwoordelijke en regievoerder

De rol van verantwoordelijke ligt op het bordje van de gemeente, omdat die in de wet verantwoordelijk wordt gehouden voor het organiseren van de samenwerking tussen alle partijen in de jeugdketen. Daarmee ligt bij de gemeente ook de uiteindelijke verantwoordelijkheid voor de feitelijke inzet van het verwijssysteem. Aldus is het college van burgemeester en wethouders verantwoordelijk voor het aangaan en nakomen van de afspraken over de samenwerking tussen het college enerzijds en de meldingsbevoegde instanties anderzijds. In de wet wordt opgemerkt dat dit op een concreet niveau bijvoorbeeld betekent dat de gemeente erop moet toezien dat protocollen worden opgesteld over de handelwijze in geval van een match. Deze en diverse andere uitvoeringskwesties die de samenwerking raken, moeten worden vastgelegd in een samenwerkingsconvenant tussen alle betrokken partijen**.** Het is aan de gemeente hierin het voortouw te nemen, aldus de parlementaire stukken. De praktische invulling is belegd via de functie van de gemeentelijk convenantbeheerder.

Behalve deze convenantbeheerder verlangt de wet van de gemeente dat ze voorziet in de functie van gemeentelijke regievoerder. Deze heeft de verantwoordelijkheid om na te gaan of er na een match door de betrokken professionals ook daadwerkelijk contact wordt gelegd, of deze personen (vervolg)afspraken maken hoe verder te handelen en erop toe te zien dat die stappen ook worden gezet. Kortom, de regievoerder bewaakt of er opvolging wordt gegeven aan signalen en 'controleert' daarmee het handelen van professionals. Waar in de praktijk de regiefunctie wordt belegd (bij een bestaande, bij de zorg voor de jeugdige betrokken instantie dan wel bij een aparte functionaris) en hoe wordt gerapporteerd is aan de gemeente. In Rotterdam bijvoorbeeld wordt per kwartaal een memo naar de verantwoordelijke wethouder en het college gestuurd, met daarin een overzicht van het aantal signalen en matches, uitgesplitst naar meldende instanties maar ook naar jeugdige (man, vrouw, leeftijd, …).

Rol van opdrachtgever en risicovol ondernemer

Hiernaast heeft de gemeente de rol van initiatiefnemer, opdrachtgever of zo men wil risicodragend ondernemer. In de discussie over de inzet van technologie door de overheid blijft het punt van het opdrachtgeverschap en daarmee vaak ook eigenaarschap van de ontwikkelde en gebruikte systemen vaak onderbelicht. Maar in diverse situaties, waaronder bij de lokale verwijssystemen, zien we dat een overheidsinstantie niet alleen gebruiker van een systeem is, maar ook initiatiefnemer, financier en aldus eigenaar van de applicatie. Dat brengt specifieke uitdagingen en

dilemma's rondom opdrachtgeverschap met zich mee. Om deze uitdaging aan te gaan heeft een aantal gemeenten, waaronder Rotterdam, in een vroeg stadium de krachten gebundeld en Multisignaal opgericht, een naamloze vennootschap die de exploitatie en het beheer van de verschillende systemen verzorgt. Multisignaal staat onder toezicht van een raad van advies, heeft de exclusieve opdracht risicosignalering voor gemeenten te verzorgen, deze taken uit te voeren zonder winstoogmerk en de deelnemende gemeenten jaarlijks inzicht in de exploitatie te verschaffen (Multisignaal 2010). Door op deze manier ontwikkelde kennis en technologie met elkaar te delen beogen de gemeenten de beheers- en ontwikkelkosten laag te houden. Elke gemeente hoeft nu immers niet zelf het wiel uit te vinden. Bijkomend voordeel is dat men door het delen van de kosten ook voor de langere termijn de doorontwikkeling en het onderhoud hoopt te waarborgen. Ten slotte beoogt de samenwerking de flexibiliteit te garanderen: er is een basismodule die de noodzakelijke basisfunctionaliteit bezit, maar daarbovenop staat het een gemeente vrij een op de plaatselijke context toegespitste uitbreiding te laten ontwikkelen.

Dat de rol van risicodragende ondernemer overigens ook heel anders kan uitpakken blijkt uit de historie van het KIDOS-systeem. Alhoewel KIDOS geen verwijsindex is, maar een Elektronisch Kinddossier (EKD), is een en ander wel illustratief voor de complexiteit van het opdrachtgeverschap door een publieke instantie. Op de markt voor de EKD-applicaties waren ten tijde van de discussie drie systemen beschikbaar: OpenCare, mlCAS en KIDOS. Van de twee eerste lag het eigenaarschap bij commerciële partijen, bij de laatstgenoemde lag dat bij twee grote GGD'en (Rotterdam-Rijnmond en Amsterdam). Dit eigenaarschap van de beide GGD'en bleek problematisch, omdat politieke wensen en keuzes aangaande financiële belangen niet strookten met beleidsinhoudelijke belangen rondom jeugdzorg. De lokale politiek in (de stadsregio) Rotterdam uitte namelijk de ambitie over te gaan tot meer integratie van alle bij jeugdigen betrokken uitvoeringsinstanties (jeugdgezondheidszorg, Bureau Jeugdzorg, maar ook scholen en justitie) ten behoeve van een brede vroege signalering, centrale registratie van knelpunten en koppeling en coördinatie van acties van verschillende hulpverleners. Daarmee was het dossier niet langer een puur medisch dossier, maar een 'breed EKD'.

Deze ambitie had tegelijkertijd ook consequenties voor de noodzakelijke verdere ontwikkeling van het gebruikte systeem, onder meer ten aanzien van functionaliteit en rechtenbeheer, wat financieel het nodige betekende. Om de kosten te delen zocht de gemeente daarom partners en trachtte andere instellingen over te halen voor het KIDOS-systeem te kiezen. Maar juist de inhoudelijke keuze voor een verdere ontwikkeling naar een breed EKD bleek voor sommige van deze instellingen een stap te ver. De consequentie van het feit dat het eigenaarschap bij de publieke instellingen zelf lag en er dus geen sprake was van een klant-leverancierrelatie (waar de publieke instellingen puur gebruiker zijn), compliceerde met

andere woorden ook de keuzes rondom inhoudelijke beleidsambities. In het geval van de gemeente Rotterdam bleek het erin te resulteren dat men niet tot een eenduidige visie op de scenario's voor deze verdere ontwikkeling kon komen: wordt het een systeem dat de bedrijfsvoering binnen de jeugdketen optimaal ondersteunt en het productieverlies zo klein mogelijk maakt of wordt het een systeem dat ketensamenwerking, integrale dienstverlening en vroege signalering optimaal ondersteunt? De keuze leek in Rotterdam in belangrijke mate te worden gestuurd door politieke overwegingen ten aanzien van de ambities en inzet op het terrein van de jeugdzorg (breed en omvattende zorg). Overwegingen die zich niet per definitie goed verhouden met de zekerheid die men zou zoeken vanuit een bedrijfsmatige optiek (zoals te nemen financiële risico's) en het belang van eigenaarschap.[20]

8.3.2 HET MINISTERIE

De andere grote speler in dit dossier is het programmaministerie voor Jeugd en Gezin. Zo wordt het initiatief voor de verwijsindex geïntroduceerd in het beleidsprogramma 'Alle kansen voor alle kinderen' en presenteert het departement de applicatie in de beleidsagenda 2010 als instrument in de ambitie om te komen tot een 'omslag naar preventie'. Via het in een vroeg stadium signaleren van problemen door middel van een verbeterde informatie-uitwisseling wilde het kabinet Balkenende IV zich richten op het voorkomen van ernstige opvoedingsproblemen en misstanden waarbij jeugdigen betrokken zijn (Ministerie voor Jeugd en Gezin 2009: 15). Op diverse plaatsen in deze studie staan wij nader stil bij de rol van het programmaministerie en daarmee ook de verhouding tussen de twee belangrijke actoren, lokale overheid en rijksoverheid. Hier stippen we slechts kort een punt aan dat van belang is met het oog op de kwestie van goed opdrachtgeverschap, meer in het bijzonder het beheer van de landelijke verwijsindex. De gekozen constructie voor het beheer is illustratief voor de beleidsoverstijgende complexiteit die de verwijsindex oproept. De verschillende beheersfuncties zijn uiteindelijk belegd bij een uitvoeringsorganisatie en agentschap van het ministerie van VWS: het Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG). Ondanks deze organisatorische inbedding binnen het zorgdomein, wordt het beheer uitgevoerd onder de uiteindelijke verantwoordelijkheid van de minister voor Jeugd en Gezin. In eerste instantie lag het beheer bij ICTU, de interdepartementale uitvoeringsorganisatie van de overheid op het terrein van ICT. Deze keuze was ingegeven door het feit dat de ontwikkeling en eerste uitrol van de verwijsindex ook bij het ICTU was neergelegd. Toen een structurele beheersoplossing aan de orde was, viel de keuze op het CIBG. Het belangrijkste motief hierbij vormde de ervaring van deze organisatie met het beheren van andere systemen in de zorg (BIG-register, Uziregister, donorregister, toelating zorginstellingen, en de sectorale Berichten Voorziening in de Zorg (SBVZ)).

8.3.3 LEVERANCIERS

Een partij die formeel bestuurlijk geen betrokkenheid heeft, maar waarvan de invloed zeker niet onderkend mag worden, is de ICT-markt. Lang niet alle gemeenten lijken te beschikken over de noodzakelijke kennis voor het ontwikkelen van complexe digitale systemen, zoals een verwijsindex. Datzelfde geldt voor een groot deel van de lokale organisaties in de jeugdzorg. In de praktijk van alledag zien publieke instanties zich vaak genoodzaakt de ontwikkeling van digitale systemen aan een externe organisatie over te laten, veelal een private partij. Zo domineren grote bedrijven als Centric en Getronics PinkRoccade de markt van de gemeentelijke softwareapplicaties (Van der Hof et al. 2009: 47). Maar behalve de technische realisatie van de digitale systemen, verlangt de implementatie van de systemen een gespecialiseerde deskundigheid. De praktijk laat zien dat deze over het algemeen wordt geleverd door een diversiteit aan consultants en adviesbureaus. Aldus ontstaan op lokaal niveau samenwerkingsvormen waarin niet alleen organisaties met een publieke taak participeren, maar ook (dikwijls primair economisch gemotiveerde) bedrijven en adviesbureaus. Technologie dwingt als het ware tot arrangementen van publiek-private samenwerking.

Wat verder opvalt is dat op lokaal niveau de betrokkenen die (mede) het initiatief nemen tot het opzetten en bij gemeenten introduceren van verwijssystemen (bijvoorbeeld een verantwoordelijk beleidsambtenaar) soms – nauwe – banden hebben met aanbieders en bouwers van systemen (private partijen). Soms zelfs blijken de actoren in één persoon verenigd. Hiermee ontstaan situaties waarin private partijen – mede onder invloed van een gebrek aan kennis bij lokale bestuurders – de inrichting van het verwijssysteem en daarmee keuzes over de reikwijdte van de informatie-uitwisseling (kunnen) bepalen. En dat doet de vraag rijzen wie binnen dergelijke samenwerkingsverbanden de functionaliteit van het systeem bepaalt, wie vaststelt welke voor de jeugdzorg relevante instellingen toegang tot het systeem krijgen en wie de beslissende stem heeft bij de afspraken welke gegevens onder welke voorwaarden in het systeem worden ingebracht en uitgewisseld. Een gesprekspartner die betrokken is bij dit soort processen gaf aan dat systeembouwers vaak ook met een kant-en-klaarproduct naar de gemeente en instellingen stappen, waarbij het systeem kan worden uitgebouwd met, wederom reeds vooraf, vastgestelde opties.

8.3.4 INSTANTIES EN HUN PROFESSIONALS: WIE MOGEN (MAAR MOETEN NIET) MELDEN?

Belangrijk voor het feitelijk functioneren van de verwijsindex zijn natuurlijk ook de professionals die via het systeem een melding doen. Wie meldingsbevoegd is, is – zoals eerder aangegeven – vastgesteld bij Besluit van 13 juli 2010 tot wijziging van het uitvoeringsbesluit Wet op de jeugdzorg.[21] Overigens benoemt dit besluit

uitsluitend categorieën van instanties (dus geen concrete professionals) en stelt het eisen aan deze instanties. Het is aan deze organisaties zelf om vervolgens vast te stellen welke professionals (natuurlijke personen) meldingsbevoegd worden. Om daadwerkelijk aan het systeem een melding af te mogen geven behoeft de professional geen (behandel)relatie te hebben met de jeugdige. De wet stelt als voorwaarde dat de professional op basis van feiten tot de conclusie moet komen dat een jeugdige een in de wet genoemd risico loopt. Concreet betekent dit dat instanties en professionals meldingsbevoegd zijn die niet een relatie met de jeugdige, maar met een van diens ouders hebben. In de parlementaire stukken worden als illustraties genoemd de instantie die schuldhulpverlening aan de ouders biedt en de professional die een ouder met psychiatrische problemen onder behandeling heeft. Op het lokale systeemniveau vertaalt zich deze situatie in de mogelijkheid om relaties aan te vinken. Zo kan een hulpverlener op naam van een jeugdige melden dat de ouders van die jeugdige problemen hebben, zoals drugsproblematiek, waardoor de jeugdige zelf ook risico loopt (Zorg voor Jeugd-systeem). De jeugdige wordt dan via de band van de ouders in beeld gebracht. De KNMG heeft laten weten deze ruime interpretatie van het meldrecht niet te zullen volgen, maar haar leden te adviseren alleen een melding te doen als deze voortkomt vanuit de eigen expertise (KNMG 2010). De minister sprak in een reactie op deze beperkte uitleg van "een gemiste kans" en deze "te betreuren" (Ministerie Jeugd en Gezin 2010a: 4).

Een aangewezen instantie is (vooralsnog) niet verplicht mee te werken aan de verwijsindex. De minister merkt hierover op: "Mocht een instantie niet mee willen doen, dan zal de gemeente haar uiterste best doen om een dergelijke instantie bij de samenwerking te betrekken, maar als de wil tot samenwerking niet aanwezig is, is het beter dat een dergelijke instantie vooralsnog niet deelneemt aan de samenwerking. Op gezette tijden zal de gemeente opnieuw proberen om deze instantie bij de samenwerking te betrekken. Dwang, bijvoorbeeld in de vorm van een wettelijke verplichting om aan te sluiten op de verwijsindex, zal hier niet helpen, aangezien het met onwillenden kwaad kersen eten is, en men altijd wel een weg zal vinden om zich aan de verplichtingen te onttrekken. Daarom is er ook geen meldingsplicht omdat 'meedoen' dan een loos begrip is. Overigens is er vooralsnog geen reden om aan te nemen dat er instanties zijn die niet positief tegenover de verwijsindex staan."[22] Over de medewerking van een individuele professional wordt opgemerkt: de in "het wetsvoorstel opgenomen regeling maakt het strikt genomen niet mogelijk om een professional die 'het hele concept van de verwijsindex onwenselijk vindt' te dwingen om een jeugdige aan de verwijsindex te melden."

Sturen op gebruik verwijsindex

Tegelijkertijd blijkt in de praktijk van alledag wel degelijk direct dan wel indirect te worden gestuurd op deelname van professionals. Subsidieverstrekking blijkt

een eerste instrument waarmee de overheid poogt in te grijpen in de handelingsruimte van professionals. Zo werden in de gemeente Rotterdam de regelingen zodanig aangepast dat organisaties die een subsidie van de gemeente wensen te ontvangen zich hebben aan te sluiten op de verwijsindex SISA om voor de betreffende subsidie in aanmerking te komen. "Dit heeft inmiddels geleid tot 34 nieuw aangesloten organisaties op SISA", aldus de SISA-rapportage aan de wethouder over het eerste kwartaal 2010.[23] Sturen op het gebruik van een applicatie via de band van een subsidie is overigens ook populair bij andere initiatieven. Zo moesten artsen voor juli 2010 kenbaar maken aan te sluiten op het landelijk schakelpunt van het Elektronisch Patiëntendossier (EPD) wilden ze gebruik kunnen maken van een eenmalige subsidieregeling.

Ook langs andere wegen wordt de professional gestuurd in het gebruik van de verwijsindex. Zo stelde de minister bij de behandeling van het wetsvoorstel voor de verwijsindex: "Een professional die namelijk werkzaam is voor een instantie die samenwerkingsafspraken met de gemeente heeft gemaakt – en de meerderheid van de betrokken professionals valt daaronder –, zal zich hebben te houden aan die afspraken. Verder zal hij gehouden zijn aan de werkafspraken en werkinstructies (bijvoorbeeld protocollen) die binnen die instantie zijn gemaakt over het werken met de verwijsindex en het samenwerken met andere instanties en professionals. De instantie waarvoor hij werkzaam is, is immers zijn werkgever of opdrachtgever, en op basis van die relatie staat het de professional niet vrij om zelf te bepalen of hij wil werken met de verwijsindex of niet. Ik ben, met andere woorden, van mening dat het feit dat een professional die onderdeel uitmaakt van een instantie die 'ja' heeft gezegd tegen de gemeentelijke samenwerkingsafspraken, een goede waarborg is voor een positieve houding van die professional over de verwijsindex. Daarom hecht ik ook zeer aan de inbedding van de verwijsindex in die samenwerkingsafspraken. Daarmee is ook gezegd dat het meldrecht 'niet vrijblijvend' is. Iets anders ligt het voor professionals die niet werkzaam zijn voor een instantie. Het gaat hier om een kleine groep, individueel werkende professionals." Bij de latere analyse van het beginsel 'keuzevrijheid' zal nader op de medewerking van professionals en de implicaties voor de professionele autonomie in worden gegaan.

Zowel care als control

Kenmerkend voor de verwijsindex is dat het actoren uit verschillende beleidstereinen bij elkaar brengt en wel dat van zorg en controle. Alhoewel de meerderheid van de betrokken professionals binnen de (jeugd)zorg werkzaam is, is de verwijsindex ook uitdrukkelijk een instrument voor professionals die primair een controlerende taak hebben. Concreet betreft het hier de politie. De politie wordt gezien als een 'belangrijke signaleerder die in de uitoefening van haar taken bevoegdheden soms meer kan waarnemen dan andere professionals'.[24] Op twee manieren kan de politie een jeugdige melden aan de verwijsindex. De regionale politiekorpsen kunnen meldingsbevoegde functionarissen aanwijzen en zo direct

melden aan de verwijsindex of men meldt indirect via de landelijke samenwerking tussen de politieregio's en de Bureaus Jeugdzorg. Deze laatste manier van melden is gebaseerd op het werkproces Vroegtijdig Signaleren en Doorverwijzen van de politie. In de parlementaire stukken valt hierover te lezen: "Dit werkproces wordt ondersteund door een zorgformulier dat door de politie wordt ingevuld en voor risicotaxatie aan Bureau Jeugdzorg wordt voorgelegd. Bureau Jeugdzorg besluit na risicotaxatie of de melding van de politie moet worden doorgemeld aan de verwijsindex. Daarbij is afgesproken dat altijd herkenbaar blijft dat de politie de oorspronkelijke melder is en dat de werkprocessen tussen de politie en Bureau Jeugdzorg, de formele melder, op adequate wijze worden uitgevoerd zodat er geen meldingen verloren gaan. In de loop van 2009 zullen de zorgformulieren van de politie door middel van elektronisch berichtenverkeer bij de Bureaus Jeugdzorg binnenkomen en zal ook de terugmelding elektronisch kunnen gebeuren. Dit werkproces van melden van de politie aan de verwijsindex via Bureau Jeugdzorg zal worden gemonitord om vast te kunnen stellen hoe dit verloopt." Het Korpsbeheerdersberaad heeft aangegeven een voorkeur te hebben voor de indirecte melding, omdat dit "als meest efficiënte wijze wordt beschouwd en momenteel door de meeste politiekorpsen wordt gehanteerd. Op dit moment melden 6 korpsen direct aan de verwijsindex en 19 korpsen melden indirect" (Staatsblad 2010, 302: 16). Overigens mag een Bureau Jeugdzorg in de melding niet aangeven dat het verzoek afkomstig is van de politie. Volgens het CBP is dit strijdig met artikel 11 Wbp en moet worden voorkomen dat de melding wordt geassocieerd met de politie: "Hierdoor kan immers het vermoeden ontstaan dat een jeugdige wordt verdacht van het plegen van strafbare feiten" (CBP 2009: 3). Vermeldenswaard is hier ten slotte nog dat het niet-direct melden door de politie bij de lokale systemen in ieder geval in de praktijk niet lijkt te betekenen dat de politie niet op de hoogte wordt gehouden van risicomeldingen. Zo wordt bij Zorg voor Jeugd de politie na een (indirecte) melding op de hoogte gehouden van latere meldingen door andere instanties, een praktijk waar vanuit juridisch perspectief door adviseurs vraagtekens bij worden geplaatst (Holla et al. 2008).

Dat de verwijsindex niet alleen dienstbaar is aan zorg maar ook aan controle, betekent overigens niet dat de deur wagenwijd open is gezet en bijvoorbeeld ook de handhaving van de openbare orde binnenboord is gehaald. De burgemeester is niet meldingsbevoegd, juist omdat de verwijsindex niet is beoogd voor het handhaven van de openbare orde. Ook het Openbaar Ministerie neemt geen deel aan de verwijsindex, omdat – zo valt te lezen in de nota naar aanleiding van het verslag – door partijen werd geconcludeerd dat de betrokkenheid van het OM "de toets der noodzakelijkheid niet kan doorstaan". Belangrijkste overweging hierbij was dat deze instantie zich aan het einde van de jeugdketen bevindt en de rol in de samenwerking met andere actoren op dit terrein zeer beperkt is. Tenslotte werd na overleg met de Antillianengemeenten vastgesteld dat de daar werkzame Antillencoördinatoren niet vanuit deze functie meldingsbevoegd worden. Als reden wordt

genoemd dat professionals die deelnemen aan de huidige overleggremia voor Antillianen ieder afzonderlijk al meldingsbevoegd zullen zijn voor de verwijsindex, waardoor zij op basis van deze bevoegdheid meldingen kunnen doen en een aparte tussenstap via de Antillianencoördinator niet als noodzakelijk wordt ervaren. Toch zijn er drie gemeenten (Rotterdam, Eindhoven en Nijmegen) die hun Antillianencoördinator wel als meldingsbevoegd wensen aan te merken. Gegeven niet alleen dit verschil in opvatting, maar zeker ook de eerdere felle (politieke) discussie over de Verwijsindex Antillianen (Janssen 2008; Brouwer & Houtzager 2009), is het opvallend dat het Uitvoeringsbesluit uitgebreid aandacht besteedt aan de mogelijkheid tot melding door doelgroepcoördinatoren voor tienermoeders, zwerfjongeren, hangjongeren en verslaafde jongeren. Met geen woord wordt echter gerept over de doelgroepcoördinatoren voor Antillianen (Staatsblad 2010, 302: 14-15).

8.3.5 TOEZICHTHOUDER EN HELPDESK

Het College bescherming persoonsgegevens (CBP) houdt op grond van de Wet bescherming persoonsgegevens (Wbp) toezicht op de verwerking van de persoonsgegevens via de verwijsindex. Eerder al was het college via de taak van wetgevingsadvisering betrokken bij het ontwikkeltraject van de verwijsindex. Verder heeft het CBP formeel een adviestaak: gemeenten kunnen bij het college aankloppen met vragen over de interpretatie van de wetgeving in het licht van de verwijsindex. De realiteit ziet er echter wat betreft zowel toezicht als advisering nogal anders uit. Allereerst blijkt – afgaand op verslagen en openbare informatieverstrekking vanuit het CBP – de bemoeienis en het toezicht in de dagelijkse praktijk vrijwel beperkt tot rijksniveau, onder meer omdat het CBP niet over de middelen beschikt om actief toezicht te houden op het scala aan verschillende lokale initiatieven. Zo heeft het CBP tot op heden geen concrete actie ondernomen naar aanleiding van de praktijk in Rotterdam om in het SISA-systeem te werken met presignalen ofwel niet-pluis-signalen, terwijl deze praktijk in diverse opzichten niet te verenigen lijkt met wettelijke regelingen.

Gemeenten op hun beurt hebben het gevoel bij het CBP voor een gesloten deur te staan. De gesprekken met betrokkenen op lokaal niveau geven de indruk dat de beleidsregels die het college voor de adviseringstaak hanteert, een barrière opwerpen om met concrete vragen over privacyimplicaties bij de omgang met de verwijsindex naar het CBP te stappen. Als alternatief kunnen gemeenten en andere gegevensverwerkers aankloppen bij de helpdesk privacy van het ministerie van Justitie. Deze Helpdesk Privacy Jeugd en Gezin (HPJG) geeft advies en informatie over privacy en gegevensuitwisseling aan instanties en (beroeps)krachten die actief zijn op het terrein van de jeugd (0 tot 23 jaar) (Ministerie van Justitie 2010). De helpdesk werd opgezet als samenwerking tussen drie verschillende ministeries, destijds waren dat: het ministerie van Justitie, het ministerie van Onderwijs,

Cultuur en Wetenschap, het ministerie van Volksgezondheid, Welzijn en Sport (Programmaministerie voor Jeugd en Gezin). Naast het informeren en beantwoorden van vragen tracht de helpdesk de signalen van het werkterrein samen te brengen en te analyseren om zo te bekijken of er een bijstelling van de huidige wetgeving mogelijk is. De geluiden over het werk van de helpdesk zijn wisselend. Sommige instanties zijn positief. Andere betrokkenen zijn dat minder, zoals een gemeentelijk coördinator die de ervaring had dat er soms laat, niet of tegenstrijdige antwoorden gegeven worden vanuit de helpdesk en zich dan ook genoodzaakt zag extern juridisch advies in te winnen.

8.4 SYSTEMEN EN TENDENSEN BIJ DIGITALISERING IN DE JEUGDZORG

8.4.1 OVERIGE INITIATIEVEN

De verwijsindex is zeker niet het enige initiatief binnen de jeugdzorg waar de nieuwe mogelijkheden van digitalisering worden benut. Vele andere systemen lijken als paddenstoelen uit de grond te schieten. De populariteit van de inzet van ICT binnen de jeugdzorg is overigens niet alleen kenmerkend voor ons land. Initiatieven en systemen soortgelijk aan die hierna worden besproken treffen we bijvoorbeeld al langer in het Verenigd Koninkrijk aan (Garrett 2005; Parton 2008).

Vanuit de groeiende populariteit van het koppelen van systemen waar ook diverse bij de verwijsindex betrokken actoren bij aanhaken, is het van belang om de verwante systemen goed op het netvlies te krijgen. In deze paragraaf zullen we daarom allereerst kort de belangrijkste andere initiatieven binnen de jeugdzorg presenteren, om vervolgens een aantal dominante tendensen, mede gefaciliteerd door deze systemen, te schetsen.

EKD

Allereerst is er natuurlijk het Elektronisch Kinddossier (EKD). In tegenstelling tot de landelijke verwijsindex is het EKD een systeem met inhoudelijke informatie. Het betreft, in eenvoudige bewoordingen, de digitale variant van het papieren medisch dossier dat met name verpleegsters en dokters gebruiken in de consultatiebureaus en bij de GGD. De beoogde doelstellingen rond het EKD kennen enige overeenkomst met die van de VIR. Evenals bij de VIR moet het EKD tot meer efficiëntie in informatie-uitwisseling leiden, een vroege signalering van risico's mogelijk maken en input leveren voor het verfijnen van de gezondheidszorg aan kinderen. In eerste instantie beoogde het ministerie het EKD landelijk op te zetten. Daarbij moest het systeem niet alleen de papieren dossiers van de instellingen in de jeugdgezondheidszorg vervangen, maar deze instellingen via een landelijke kop ook op basis van inhoudelijke informatie met elkaar laten communiceren. Een negatieve beslissing van de rechter over het aanbestedingstraject van een landelijk

EKD dwong de minister voor Jeugd en Gezin (2007a) ertoe de digitalisering toch op decentraal niveau te beleggen.[25] De instellingen in de jeugdgezondheidszorg dienden nu onder regie van de gemeenten een plan van aanpak op te stellen om eind 2009 te kunnen werken met digitale dossiers. Gemeenten kregen daartoe de bestuurlijke verantwoordelijkheid en kregen via de VNG een subsidie. De wettelijke basis voor het EKD vormt artikel 5 van de Wet publieke gezondheid, waarbij lid 3 de verplichting betreft om digitale dossiers bij te houden van patiënten in de jeugdgezondheidszorg.[26] Deze digitaliseringsplicht kreeg 1 juli 2010 kracht van wet. In de voortgangsrapportage over het programma Samenwerken Voor de Jeugd van 19 mei 2010 meldt de minister dat: "In februari 2010 had 95 procent van de JGZ-organisaties een pakket gekozen en is bezig met de implementatie. 40 procent van de JGZ-organisaties werkt al geheel of gedeeltelijk digitaal... Naar verwachting heeft 85 procent op 1 juli of direct na de zomervakantie de digitalisering gerealiseerd" (Ministerie voor Jeugd en Gezin 2010b:22).

Anders dan bij traditionele papieren dossiers die primair binnen de individuele organisaties worden opgesteld en gebruikt, hebben diverse gemeenten de ambitie om het EKD uit te bouwen tot een inhoudelijk digitaal dossier dat door meerdere organisaties wordt gevuld en gebruikt, een zogenaamd 'breed EKD'. Om "een volledig beeld" te verkrijgen van jongeren, zo bepleitten de verantwoordelijke wethouders van de vier grote gemeenten in een brief aan de minister, moet het EKD naast informatie uit het domein van de jeugdzorg ook relevante informatie bevatten vanuit het schoolmaatschappelijk werk, de Bureaus Jeugdzorg en de geestelijke jeugdgezondheidszorg. Ook moet bezien worden of een koppeling met de VIR mogelijk is (wethouders Jeugd van Amsterdam, Utrecht, Rotterdam en Den Haag 2007). Het KNMG reageerde afwijzend op het voorstel van de wethouders om het EKD breed toegankelijk te maken. Het EKD is een medisch dossier en heeft als doel te zorgen voor goede medische zorg, niet het vroegtijdig opsporen van risicosituaties, zo stelde de KNMG in een nieuwsbericht (KNMG 2009). Voor deze laatste doelstelling is de verwijsindex immers in het leven geroepen. Bij de parlementaire behandeling van het wetsvoorstel Verwijsindex Risicojongeren liet ook de minister weten dat het EKD enerzijds en de landelijke verwijsindex anderzijds zo verschillend van aard zijn dat het niet voor de hand ligt om de systemen te integreren. "Integratie zou in mijn ogen tot een geforceerde opeenstapeling leiden, waarvan het de vraag is of die een meerwaarde zou hebben voor de praktijk."[27] Wel is gegarandeerd dat de systemen naast elkaar kunnen werken en in de toekomst een koppeling gerealiseerd kan worden met het Elektronisch Patiëntendossier (EPD): "Zo is het ontwerp van de verwijsindex afgeleid van het EPD en is ook voorzien dat het EKD op termijn wordt gekoppeld aan het EPD.

Verder is het zo dat vanuit het domein jeugdgezondheidszorg meldingen aan de verwijsindex kunnen worden gedaan. De informatie uit het EKD zal dus heel vaak nodig zijn om tot een weloverwogen afweging te komen of een melding aan de

verwijsindex moet worden gedaan. Benadrukt zij dat het ook hier steeds om de professionele afweging gaat, het doen van een melding kan dus nooit automatisch volgen uit de informatie in het dossier. Ook nadat een melding is gedaan, ligt het voor de hand dat de jeugdarts dit aantekent in het EKD."[28] De relatie tussen de verwijsindex en het EKD betekent dus concreet dat medewerkers van de jeugdgezondheidszorg op grond van hun bevindingen een jeugdige aan de verwijsindex kunnen melden, waarbij ze deze melding noteren in het digitale dossier van de jeugdige, het EKD.

Hoewel het EKD nu dus niet wordt gekoppeld aan de VIR, worden sommige lokale signaleringssystemen, zo blijkt uit de informatiebrochure van InterAcces, de ICT-leverancier van onder meer het signaleringssysteem van Noord-Brabant, daartoe wel uitgerust. Kortom, wordt in de toekomst eenmaal het groene licht gegeven, dan is de koppeling eenvoudig te realiseren. In Rotterdam heeft men daar echter niet op gewacht. Op 14 september 2009 is daar de elektronische verbinding gelegd tussen het Elektronisch Kinddossier en SISA, het lokale signaleringssysteem van Rotterdam. Hoewel deze verbinding niet zo uitgebreid is als waarop Rotterdam in eerste instantie had ingezet (uiteindelijk werd besloten het EKD een puur medisch dossier te laten zijn en dus niet via de VIR toegankelijk te maken voor andere hulpverleners), kunnen de verpleegkundigen en artsen nu wel via het Elektronisch Kinddossier rechtstreeks hun signalen afgeven in SISA (Rapportage SISA-signaleringssysteem 3de kwartaal 2009).

Prokid

Behalve het EKD zijn er ook andere, sommige minder bekende, initiatieven. De belangrijkste daarvan is het Prokid-systeem. Dit is een signaleringsinstrument van de politie ten behoeve van het signaleren van kinderen jonger dan 12 jaar (12-minners), die op de een of andere wijze in relatie staan tot een strafbaar feit, zodat vroegtijdig kan worden gesignaleerd of het risico bestaat dat zij crimineel en probleemgedrag zullen ontwikkelen. Prokid is daarmee een bronsysteem van de politie met inhoudelijke informatie. Kinderen van 0 tot 12 jaar worden op basis van een risicotaxatie in een van de vier risicocategorieën die het Prokid-systeem kent opgenomen. De minst risicovolle categorie bevat kinderen van wie bekend is dat zij als getuige of slachtoffer bij een delict aanwezig waren. Dat zij een risico lopen wordt onder meer beargumenteerd met het feit dat kinderen jonger dan 12 jaar die slachtoffer of getuige waren van seksueel misbruik, een groter risico blijken te lopen om later gedrags- of sociale problemen te ontwikkelen. In de zwaarste risicocategorie worden kinderen geplaatst die zich meerdere keren schuldig hebben gemaakt aan onder meer zedendelicten, geweldpleging of overvallen. De politieregio meldde dat er in een jaar tijd 2.932 kinderen waren beoordeeld, van wie er 1.147 in de lichtste categorie kwamen (geen risico) en 113 in de zwaarste categorie vielen. Voor deze laatste groep startte Bureau Jeugdzorg acute hulp op (ministerie van BZK 2008). De risicotaxatie van het Prokid-systeem werkt op basis van twee bronnen van gege-

vens. Ten eerste wordt gebruikgemaakt van gedragsindicatoren waarvan wordt vermoed of vaststaat dat die tot criminele activiteiten kunnen leiden. Ten tweede kijkt men naar de gegevens die bekend zijn over de medebewoners op het woonadres van de 12-minner en beoordeelt of die aanleiding geven tot verhoogd risico op crimineel en probleemgedrag van de jongere.

Op basis van de combinatie van deze twee bronnen van gegevens – het kind zelf en zijn woonomgeving – wordt het ingedeeld in een van de eerdergenoemde risicocategorieën. In het proefjaar bleek tevens dat ongeveer 50 procent van de in Prokid opgenomen kinderen bekend was bij Bureau Jeugdzorg.[29]

Wetenschappers zijn verdeeld over de voorspellende waarde en validiteit van risicoanalyses, meer specifiek de analyses van jonge kinderen. Ten behoeve van het Prokid-initiatief deed de Radboud Universiteit Nijmegen onderzoek naar de voorspellende waarde van de gehanteerde methodiek. Afgezien van het complexe antwoord op de vraag naar de voorspellende waarde (Aarntzen-Tacken et al. 2008), is een opvallende conclusie in het rapport "dat recidive in het algemeen evengoed te voorspellen is op basis van woonadres of enkel individuele kindkenmerken, als op basis van de combinatie van woonadres en kindkenmerken" (Radboud Universiteit 2008: 70). Met andere woorden, de registratie binnen dit project zou zich ook kunnen beperken tot gegevens over woonadres en daarmee alle informatie over individuele kindkenmerken achterwege kunnen laten.

Evenals bij de verwijsindex, is ook bij Prokid gegevensuitwisseling in de keten van zorgpartners een belangrijk element: "Het signaleren en doorverwijzen naar de hulpverlening van risicojongeren onder de 12 jaar is een belangrijke taak van de politie. De zorg voor adequate hulpverlening ligt echter bij de partners. Het is de bedoeling om tot een effectieve ketensamenwerking te komen. Daartoe wordt een provinciebreed masterplan voorbereid. De inzet is het realiseren van interventiekansen met partners aan de vóórkant van de problematiek" (Politie Gelderland-Midden 2008). Het Prokid-project dat in Arnhem zo succesvol is gebleken, loopt nu als pilot ook in vier andere politieregio's om te onderzoeken of een landelijke uitrol wenselijk en haalbaar is. Nol Meulendijks, projectleider Vroegtijdig Ingrijpen bij het ministerie van Justitie zegt hierover in de nieuwsbrief programma Aanpak jeugdcriminaliteit (Ministerie van Justitie 2009: 6): "Voordat we het systeem landelijk invoeren moeten we weten of en zo ja hoeveel extra capaciteit en kwaliteit er nodig is bij de politie, bij de Bureaus Jeugdzorg, maatschappelijk werk, bij zorgaanbieders. Aanvankelijk kan Prokid ertoe leiden dat het aantal 12-minners dat geholpen moet worden toeneemt." In hetzelfde artikel stelt Meulendijk dat wanneer de "weeffoutjes" eruit zijn en men zicht heeft op de eventuele extra hulpvraag en de wijze waarop er samengewerkt kan worden, het Prokid-systeem zo snel mogelijk landelijk ingevoerd moet worden. "Ook

als de hulpverlening nog niet op pijl is. Prokid biedt in ieder geval zicht op de problemen. Doe je het niet, dan steek je je kop in het zand" (Ministerie van Justitie 2009: 7). Wat betreft de relatie met de landelijke verwijsindex geldt tot op bepaalde hoogte hetzelfde als bij het EKD: de gegevens van de jeugdigen die in Prokid zijn opgenomen worden niet in de verwijsindex opgenomen. Er is geen koppeling tussen beide systemen. Met andere woorden een melding in Prokid betekent niet dat er automatisch een melding aan de verwijsindex volgt. Een politieagent kan natuurlijk wel zowel in Prokid als ook in de verwijsindex een risicosignaal afgeven. De politieagent vormt dan het knooppunt tussen beide systemen.

Overige initiatieven van de overheid

Ten slotte gebruiken alle bij de jeugdzorg betrokken partijen diverse eigen systemen waarin informatie over kinderen en jeugdigen wordt geregistreerd en van waaruit de gegevens in voorkomende gevallen worden verstrekt aan andere instanties. Zo hebben scholen en gemeenten een leerplichtsysteem, werken schuldhulpverleningsinstanties met digitale dossiers, veiligheidshuizen met databanken, is er het systeem Jongeren in Beeld van sociale diensten, de diverse systemen die de gemeentelijke Centra voor Jeugd en Gezin opzetten, enzovoorts. Het valt buiten het bestek van deze paragraaf om al deze systemen individueel nader te duiden en te bespreken. Hier wordt volstaan met de opmerking dat we ervan uit mogen gaan dat alle professionals en andere relevante instanties die melden in de VIR en in de volgende paragraaf in beeld komen op z'n minst één, zo niet meerdere, systemen in gebruik hebben die informatie over jeugdigen bevatten en op basis waarvan ze noodzakelijke input leveren aan de werking van de verwijsindex. Daar waar dat relevant is zal het bestaan en gebruik van de systemen daarom in de onderstaande paragrafen worden meegenomen.

8.4.2 VERSCHUIVINGEN IN DE JEUGDZORG

Risico in kaart gebracht

Niet alleen de verwijsindex, maar ook het Prokid-initiatief zijn voorbeelden van de tendens om aan de hand van risicofactoren een beeld te creëren van jeugdigen, om vervolgens op basis van dit beeld voorspellingen over hun toekomst te doen en – waar noodzakelijk geacht – preventief op te treden. Een belangrijke vraag die in dit verband dan natuurlijk naar voren treedt is in hoeverre er inderdaad een wetenschappelijke onderbouwing bestaat voor mogelijke parallellen en samenhang tussen (ernstig) problematisch of crimineel gedrag van jeugdigen en omgevings- en persoonskenmerken. Een snelle blik op de literatuur laat hierover een nogal gevarieerd beeld aan opvattingen en bevindingen zien.

Voornamelijk gericht op potentieel delinquent gedrag concludeerde een onderzoek van het ministerie van Justitie uit 1996 naar de signaalwaarde van kinder-

delinquentie en probleemgedrag, op basis van longitudinale studies dat er "duidelijke, voorspellende factoren voor delinquentie zijn, die reeds op jonge leeftijd gesignaleerd kunnen worden" (Dienst Preventie, Jeugdbescherming en Reclassering 1996: 33). Deze factoren kunnen onderscheiden worden in individuele kindfactoren, factoren in de familie en omgevingsfactoren. Verder stelt de studie dat niet één signaal op zich, maar de combinatie van meerdere signalen de kans verhoogt op ernstig crimineel gedrag op latere leeftijd. Tenslotte is hier de volgende conclusie van belang: "Uit het onderzoek blijkt dat jeugdigen op diverse plaatsen signalen afgeven voor hun probleemgedrag dan wel de probleemsituatie waarin zij opgroeien. Knelpunt daarbij is dat er niet op één plaats een overzicht is van de diversiteit aan signalen. Daarnaast worden er ook signalen afgegeven door jeugdigen, die door een gebrek aan deskundigheid niet op hun waarde geschat worden. Tot slot is er sprake van informatie-uitwisselingsproblemen: de kennis is aanwezig, maar men wil, mag of kan die informatie niet aan derden verstrekken. Kortom: op diverse plaatsen liggen puzzelstukjes of zouden er kunnen liggen, maar niemand wordt in staat gesteld om de puzzel in elkaar te leggen. Bundeling van regie over informatie op één plaats zou een enorme stap in de goede richting zijn" (Dienst Preventie, Jeugdbescherming en Reclassering 1996: 61). De onderzoekers merken in een voetnoot bij de bovenstaande passage op dat het belangrijkste knelpunt hierbij "de Wet op de Privacy" is. Opvallend is dat de opstellers van het rapport deze conclusie niet op basis van een analyse van de wetgeving zelf, maar op basis van de perceptie van de geïnterviewden trekken.

In een WODC-onderzoek uit 2000 naar risicofactoren voor de ontwikkeling van delinquent gedrag werd echter geconstateerd dat er wetenschappelijk onvoldoende basis is voor het leggen van een relatie tussen delinquent gedrag en bepaalde risicofactoren: "Eén van de eerste problemen bij de uitvoering van preventieprogramma's is de keuze van een doelgroep, waarop de activiteiten zich moeten richten. Tot nu toe is niet voldoende bekend over het verloop van delinquente carrières en de rol die diverse risicofactoren daarbij spelen, om individuele voorspellingen over het ontstaan van delinquent gedrag mogelijk te maken. Enkel de aanwezigheid van risicovolle omstandigheden in kind of gezin, kan dan ook geen rechtvaardiging voor vroegtijdig preventief ingrijpen vormen. In plaats van preventieprogramma's toe te passen op individuen van wie verwacht wordt dat zij zich in een verkeerde richting ontwikkelen, kan er ook voor gekozen worden om preventieprojecten op te zetten in wijken of op scholen waar zich veel risicovolle omstandigheden onder kinderen voordoen, om zodoende voor zoveel mogelijk potentiële risicojeugdigen de ontwikkeling van risicofactoren op verschillende terreinen tegen te gaan" (Ministerie van Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) 2000: 93). De afwezigheid van een duidelijk verband tussen bepaalde risicofactoren en een bepaald type gedrag geldt ook meer algemeen voor asociaal gedrag. De Britse criminologisch psycholoog Farrington (2005: 186) die al jaren onderzoek naar de relatie tussen risico-indicatoren en

gedrag doet, stelde: "How far any given risk factor generally predicts a variety of different outcomes (as opposed to specifically predicting one or two outcomes) and how far each outcome is generally predicted by a variety of different risk factors (as opposed to being specifically predicted by only one of two risk factors) is unclear."

Een rapport uit 2005 van het Wetenschappelijk Instituut voor het CDA over jeugdbeleid, kenmerkt zich door een nogal relativerende toon wat betreft de waarde van het registreren en analyseren van gegevens en cijfers over kinderen, jeugdigen en de gezinnen waarin ze opgroeien. Allereerst, zo stelt het rapport, is er de vraag naar de werkelijkheid achter de cijfers. Bovendien: het gaat in ons land om tussen de 150.000 en 250.000 kinderen uit 75.000 tot 125.000 gezinnen. Met andere woorden, beleidsmakers moeten oorzaken van problemen vooral in perspectief zetten. Vermeldenswaard is dan de conclusie: "In de publieke beeldvorming – en niet zelden in het politieke debat – worden deze verbanden vervolgens nogal eens verabsoluteerd, en *wordt de risicogroep tot algemene probleemgroep*. Soortgelijke processen hebben zich ook in het verleden voorgedaan met tal van andere maatschappelijke (sub)groepen, zoals lager opgeleiden of kinderen uit eenoudergezinnen. Statistische verbanden gingen in de beeldvorming stap voor stap over in oorzakelijke verbanden, waarbij vrijwel altijd de veel grotere groep *zonder* problemen over het hoofd werd gezien" (Wetenschappelijk Instituut voor het CDA 2005: 29).

Het rapport *Investeren Rondom Kinderen* (RMO & RVZ 2009), ten slotte, concludeert dat door de focus op risicosignalen te leggen, de zogeheten 'beschermende factoren' uit het oog verloren worden. Er wordt weinig gekeken naar elementen die bepaalde risico's als het ware kunnen neutraliseren, zoals een goede ouder-kindrelatie of een breed sociaal netwerk dat het gezin steunt (zie ook Hall et al. 2010). "De sociale omgeving wordt weliswaar regelmatig opgenomen als risicofactor bij de opsporing en diagnostiek, maar op het niveau van de interventie speelt slechts het microniveau van het kind en het gezin" (De Winter in RMO en RVZ 2009: 34). Door te focussen op risicotaxatie, vroegsignalering en preventieve interventies bij individuele kinderen en gezinnen gaat veel relevante kennis en kunde over maatschappelijke en sociale achtergronden verloren, aldus De Winter (RMO & RVZ 2009: 34). Andere problemen die RMO en RVZ signaleren als het gaat om risicotaxatie, is ten eerste de tegenstelling tussen een overheid die steeds vaker op de stoel van de opvoeder gaat zitten versus de wens om ouders vooral zelf verantwoordelijkheid te laten dragen. Ten tweede gaat risicotaxatie gepaard met hoog oplopende kosten. Ten derde komt een aantal risicofactoren zo vaak voor dat het niet mogelijk is voor de overheid om via monitoring en interventie die risico's effectief te bestrijden. Ten vierde leidt de bureaucratie die monitoring en screening met zich meebrengt er niet toe dat er effectief en daadkrachtig ingegrepen kan worden. Ten slotte loopt men ook tegen de grenzen aan van wat wenselijk is aangaande overheidsinmenging in de private sfeer (RMO & RVZ 2009: 36).

Kort samengevat: alhoewel uit het voornoemde en ander onderzoek blijkt dat er verbanden zijn tussen risicofactoren bij 12-minners en later crimineel gedrag (Loeber et al. in RMO & RVZ 2009: 27), tussen een toestand van armoede in het gezin en sociale uitsluiting (SCP in RMO & RVZ 2009: 27) en tussen armoede en gezondheidsproblemen (SCP in RMO & RVZ 2009: 27), wordt tegelijk ook beargumenteerd dat risicotaxatie geen garantie is voor objectieve, toetsbare en betere beslissingen voor kinderen (Ten Berge 2005). Ook is door meerdere auteurs gewezen op de negatieve implicaties van deze benadering van een risicosamenleving (Boutelier 2005; Beck 1997; Buruma 2005, 2006). Desalniettemin zetten politiek en bestuur in op a) het verzamelen van zoveel mogelijk aanwijzingen voor mogelijke risico's die jeugdigen lopen, en b) het uitvoeren van risicotaxaties om specifieke doelgroepen die risico's lopen zo goed mogelijk op het netvlies te krijgen (ministerie van Justitie & het ministerie voor Jeugd en Gezin 2008). Nog afgezien van de wetenschappelijke onderbouwing van de te leggen relaties zijn bij het in kaart brengen van risico's om daar vervolgens beleid op te voeren nog specifieke kanttekeningen te plaatsen. Eerst en vooral zijn dat kanttekeningen bij het maken van en handelen conform zogenaamde 'risicoprofielen'. Zo wijzen Bekkers et al. (2006: 39) op problemen rondom de betrouwbaarheid van de gegevens die het uitgangspunt vormen voor de profielen. Ten tweede, zo stellen zij, hoeven statistische correlaties niet per se een feitelijke weerslag te kennen. Een verband dat op theoretisch niveau wordt gelegd hoeft in de praktijk lang niet altijd realiteit te worden. Ten derde, vervolgen ze, bestaat de kans dat risicoprofielen een eigen leven gaan leiden en de aandacht van professionals en andere betrokkenen primair uitgaat naar de risico's die deel uitmaken van het risicoprofiel. Hierdoor kunnen de bredere context en andere kwesties die spelen naar de achtergrond verdwijnen of zelfs helemaal uit het oog worden verloren. Ten vierde speelt op een fundamenteler niveau het risico, aldus Van Gunsteren (2008: 174), dat de ontwikkeling van het begrip 'burger' verknoopt raakt met die van het begrip 'veiligheid', terwijl die ontwikkelingen tot voor kort betrekkelijk los van elkaar verliepen.

Paternalisme en de verschuiving van strafrechtelijk handhaven achteraf naar bestuurlijk preventief optreden

De overheid heeft zich, mede ook door het oprichten van een programmaministerie voor Jeugd en Gezin, expliciet gecommitteerd aan het welzijn van de jeugdige. Naast het voorzien van kwalitatief hoogstaande zorg is het ook een expliciete ambitie van de rijksoverheid om jeugdigen, zo vroeg mogelijk en waar nodig, bij te sturen, zodat erger voorkomen kan worden. Na toetsing van 153 beleidsmaatregelen uit vijf gemeenten die alle betrekking hadden op sociale veiligheid, concluderen Prins en Boutellier dat de lokale veiligheidszorg wordt gekenmerkt door elementen van het voorzorgdenken (Prins & Boutellier 2010). Daarbij heeft de overheid, zo toont onder meer het recente 'achter-de voordeur-beleid', duidelijke opvattingen over het al dan niet wenselijke gedrag van kinderen en hun ouders. Voorkomen dient te worden dat jeugdigen worden geconfronteerd met allerhande sociale problemen,

criminaliteit en andere als schadelijk ingeschatte invloeden en gedragingen. Deze proactieve en preventieve inzet van de jeugdzorg wordt met name mogelijk gemaakt door de in de vorige paragraaf beschreven focus op het in kaart brengen van risicosignalen bij jeugdigen. In feite gaat het hierbij om taxatie met het oog op de toekomst vanuit observaties en risicocalculaties in het heden, waarbij individuele jeugdigen langs de meetlat van geconstrueerde populaties van risicojongeren worden gelegd en daarop worden afgerekend. Of in de woorden van Schinkel: "subpopulaties worden geproblematiseerd op grond van het *verondersteld toekomstige gedrag* van leden daarvan" (Schinkel 2009).

Maar er zijn meer redenen waarom de politiek de ambities binnen de jeugdzorg verlegt: mede om te voorkomen dat de strafrechtsketen verstopt raakt onder de last van vervolging van grote aantallen strafbare feiten, richt de politiek de aandacht op preventief bestuurlijk optreden onder de algemene noemer van – maatschappelijke, sociale en individuele – veiligheid.[30] Van *post-crime* naar *pre-crime* (Zedner 2007). Ook Garrett (2004) stelt vast dat steeds meer de domeinen van jeugdzorg en van jeugdrecht geïntegreerd geraken. De hang naar preventie vanuit deze ambitie is dan ook duidelijk zichtbaar in een eerder beschreven initiatief als Prokid van de politie Gelderland. Maar ook in het buitenland wordt eenzelfde tendens waargenomen. Zo spreekt Parton (2008) in een analyse van het Britse jeugdzorgprogramma over de opkomst van een "preventive-surveillance state".

En als het om preventie gaat zijn nieuwe technologische mogelijkheden bij uitstek in staat de ambities van controleren, beheersen en proactief optreden binnen de jeugdzorg vorm te geven. Beleid en praktijk gericht op vroegtijdig signaleren en ingrijpen zijn onlosmakelijk verbonden met de opkomst van een waaier aan surveillancesystemen in de jeugdzorg (Parton 2006: 989). Databanken bieden onbeperkte mogelijkheden tot het registreren en langdurig bewaren van grote hoeveelheden gegevens over jeugdigen. Door de koppeling van deze databanken kan een breed scala aan partners langs digitale weg en gelijktijdig met elkaar 'in gesprek' raken. Vroegtijdige signalering en geïnformeerde risico-inschatting is te realiseren met behulp van profileringstechnieken (datamining), waarmee *typen* risicojongeren en probleemgezinnen worden geduid. En in de toekomst valt er nog veel meer te verwachten: Teeuw en Vedder wezen in een studie voor het ministerie van Binnenlandse Zaken op vele ongekende kansen die de ontwikkeling van zogenaamde NBIC-technologie (nano-, bio-, informatie- en cognitietechnologie) biedt voor proactief optreden (Teeuw & Vedder 2008).

Van individu naar type jeugdige

Samenwerken in een keten van partners biedt de mogelijkheid een variëteit aan gegevens over jeugdigen in beeld te brengen. Daarmee kan dan ook de stap worden gezet naar het ontwaren van tendensen in de ontwikkeling van jeugdigen en kan een beeld over jeugdigen en type jeugdigen worden geconstrueerd. Het is

met name deze intensieve manier van gegevensverzameling en -uitwisseling die de tendens tot vroegtijdig ingrijpen faciliteert. Zonder voorbij te gaan aan de kansen die technologie biedt voor de overheid om beleid via technologie vorm te geven, brengt digitalisering, ook binnen de jeugdzorg, andere veranderingen met zich mee dan uitsluitend het steeds verder optimaliseren van 'de informatiepositie' van individuele betrokken zorgverleners (Garrett 2005).

Zo is, vanuit het niveau van beleidsvorming, de relatie tussen de jeugdzorg en de betrokken jeugdigen er ook een geworden van een relatie tussen overheid en *type* jeugdige. Met de nieuwe mogelijkheden van datamining (het met elkaar in verbinding brengen van gegevens om daar patronen uit te destilleren) zoomt het beleid steeds meer in op een bepaald type probleemjeugdige of risicojeugdige. Door het verzamelen van zoveel mogelijk gegevens rond een specifiek persoon tracht men een 'holistisch beeld' van die persoon te vormen (zie ook Prins & De Vries 2003). Welke persoon, met welke (gedrags)kenmerken heeft welke voorkeur in welke situatie en onder welke (sociale en economische) omstandigheden? Deze factoren worden steeds inzichtelijker en spelen daarmee een prominentere rol in het beleid van de overheid. Het zal geen verrassing zijn dat de overheid hierbij ook steeds meer aandacht heeft voor etnische verschillen en etnische effecten.[31] Door deze verregaande, vaak geautomatiseerde, verzameling en uitwisseling ontstaat een opvallende paradox. Enerzijds weet men steeds meer over een jongere, omdat er heel veel gegevens over hem of haar verzameld worden waardoor een *digital persona* (Clarke 1994), een digitaal model van een jeugdige, ontstaat in de systemen van de jeugdzorg. Anderzijds impliceert deze uitgebreide verzameling gegevens niet dat men iemand 'persoonlijk' kent en een duidelijk zicht heeft op hoe een individu zich ontwikkelt en verandert (Van der Hof et al. 2009). Peckover et al. (2008) spreken in deze van *data doubles* en *electronic children*. De wijze waarop jongeren in het systeem worden gerepresenteerd hangt in grote mate af van de manier waarop de database is ingericht (White et al. 2009). In plaats van zich te richten op het weergeven van een beeld van de betrokken jeugdige wordt in het domein van de jeugdzorg steeds meer aandacht besteed aan het opdelen van de jeugdige in verschillende velden en boxen die ingevuld moeten worden om zo te voldoen aan de eisen die in het systeem vastliggen (Parton 2009: 719).

Dat roept de vraag op hoe dynamisch al deze digitale typen en profielen zijn. Bestaat de mogelijkheid om profielen aan te passen, verouderde typen te wissen? Of is eens een straatschoffie altijd een straatschoffie en is er na vallen nooit meer opstaan (Prins 2008)? Het antwoord is cruciaal als we kijken naar de mogelijke effecten van de tendens tot profileren en typeren. Mensen gaan elkaar en zichzelf beoordelen op basis van – door de overheid gecreëerde – typeringen. Achterstelling, stigmatisering en discriminatie liggen op de loer. Juist om dergelijke – veelal sluipende – ontwikkelingen voor te zijn is het van groot belang dat we bij complexe technologische ontwikkelingen de verborgen maatschappelijke implicaties

en de wijze waarop die een blijvend karakter krijgen, vroegtijdig trachten te ontwaren. Vanuit haar beschermende functie is de overheid gehouden ook hier een open en kritisch oog en oor voor te hebben.

Verantwoordelijkheid en toezicht bij verknoopte relaties

Waar digitalisering in de jeugdzorg er langs de ene kant van de relatie voor zorgt dat hulpverleners de jeugdige steeds meer als een *type* jeugdige gaan zien, zo verandert langs de andere kant van de relatie ook de wijze waarop de jeugdige en zijn ouders de jeugdzorg percipiëren. Het faciliteren van een goede samenwerking tussen alle betrokken instanties door middel van indexen, dossiers en risicotaxaties maakt een toegesneden zorg mogelijk. Hulpverleners vinden elkaar gemakkelijker waardoor overleg sneller en beter kan plaatsvinden. Tegelijk wordt de interactie tussen de verschillende instanties, zoals we zowel in deze als in subparagraaf 8.5.1 zullen constateren, aan het oog van de jeugdige onttrokken juist door dezelfde systemen die de samenwerking mogelijk maken.

Vroeger hadden kinderen, jongeren en hun ouders dikwijls te maken met verschillende instanties zoals consultatiebureau, school, arts, Informatie Beheer Groep, enzovoorts. Nu beslissen deze en andere instanties over jeugdigen als *ketenpartners* binnen *informatiestelsels*. Steeds minder eenvoudig valt vast te stellen welke instelling binnen de jeugdzorg voor deze beslissing de verantwoordelijkheid draagt. Daarbij is het van belang voor ogen te houden dat de ketens en stelsels zich niet beperken tot de grenzen van de overheid. De verwijsindex, gecombineerd met nummers (in het bijzonder het Burgerservicenummer) en andere technische applicaties faciliteren, zoals we hiervoor hebben gezien, een complexe digitale wereld van publiek-private samenwerking, waardoor het toezicht op *overheids*handelen steeds minder eenvoudig wordt (Garrett 2005). En in deze wereld van ketens en systemen is het voor jeugdigen steeds minder eenvoudig om met hun klacht de weg te vinden naar de verantwoordelijke instantie (Nationale Ombudsman 2009). Van der Hof et al. (2009: 59) spreken in deze van *system opacity*. Over het algemeen heeft men geen idee op welke manier persoonsgegevens in databases opgeslagen en uitgewisseld worden, tenzij er een 'ongeluk' gebeurt en datalekken, vergeten USB-sticks en verloren cd-roms het nieuws halen. Parton (2009); Tregeagle en Darcy (2007) concluderen over de situatie bij de Britse jeugdzorg dat de introductie van ICT met name gericht is op het verankeren van interne procedures en deze introductie wordt gedreven door het verhogen van controle en surveillance op professionals en jeugdigen. Veel minder is het gericht op de *empowerment* van de jeugdige zelf of het ondersteunen van de creativiteit van de professional. Jeugdigen en hun ouders krijgen te maken met 'onzichtbare zichtbaarheid'. Ze worden steeds zichtbaarder voor instanties op een voor henzelf onzichtbare wijze (Keymolen 2007). In de literatuur over surveillance wordt ook wel gesproken over de "disappearance of disappearance" (Haggerty & Ericson 2000).

Deze ontwikkeling lijkt in ieder geval te verlangen dat bij controle en toezicht de aandacht niet alleen op instanties, maar ook op systemen wordt gericht (Prins 2007). Een instrument dat de positie van jeugdigen en hun ouders mogelijk kan verstevigen is in feite al ontwikkeld door de Gemeentelijke Ombudsman (2006) van Amsterdam. Een inwoner van de gemeente kwam diverse malen in de problemen met gemeentelijke instanties ten gevolge van een foutieve inschrijving (de fout lag bij de gemeente) in de gemeentelijke basisadministratie. De Gemeentelijke Ombudsman oordeelde dat wanneer de gemeente een fout maakt, zij de burger hierover via een zogenaamde toonbrief moet informeren en uitleg moet geven, zodat de burger deze brief kan gebruiken bij andere instanties die gebruikmaken van de foutieve gegevens. De aanbeveling van de Gemeentelijke Ombudsman zou breder getrokken kunnen worden door te stellen dat zorgvuldigheid van overheidsoptreden verlangt dat de instanties binnen de jeugdzorg burgers van informatie voorzien die hen in staat stelt hun belangen te beschermen. Alleen met deze informatie is het voor hen mogelijk een gelijkwaardige (bewijs)positie in te nemen (Prins 2007).

Wetgeving via een achterdeur

Opvallend is ook de wijze waarop de wetgever de initiatieven in de jeugdzorg van een juridisch fundament voorziet. Veel van de ambities lijken momenteel via een achterdeur te worden geregeld. Zo is het EKD bijvoorbeeld afgekaart in één enkele bepaling (artikel 5, derde lid Wet publieke gezondheid) van een wet die zeer veel andere zaken (zoals infectieziekten) omvat. Vele uitvoeringsregelingen worden vervolgens belegd in nadere wetgeving, onttrokken aan een politieke discussie en daarmee democratische controle. Kenmerkend voor veel van de initiatieven is bovendien dat het juridische fundament pas wordt gelegd als de projecten al lang op stoom zijn en daarmee de inrichting (welke gegevens worden opgenomen, wie mag de gegevens aanleveren, wie mag ze inzien, met welke andere initiatieven wordt gekoppeld, enz.) al lang concreet is bepaald. Wetgeving fungeert in feite alleen nog als legitimerend voor een reeds bestaande uitvoeringspraktijk in plaats van piketpalen slaand voor de ontwikkeling van deze praktijk. Overigens is de kritiek dat wetgeving verwordt tot een beleidsinstrument (Raad van State 2006) en sprake is van een "erosie van de wetgevende functie", aldus Hoekstra (2009) van de Raad van State, niet specifiek voor de thematiek van deze bijdrage, maar speelt de zorg meer algemeen.[32]

Kijkend naar de prominente plaats die de initiatieven spelen bij de uitvoering van het jeugdbeleid, het type gegevens waar het hier over gaat (medische gegevens, signalen over criminaliteit, enz.) en de implicaties die de initiatieven hebben voor de positie van de diverse betrokkenen, mag van een zorgvuldige wetgever worden verwacht dat het fundament op een andere wijze en een eerder tijdstip zichtbaar wordt.

Een keten of een netwerk?

Welhaast onlosmakelijk verbonden met de drang om in een zo vroeg mogelijk stadium – preventief – te signaleren en te handelen lijkt de tendens om allerhande digitale initiatieven binnen verschillende maatschappelijke domeinen met elkaar in verband te brengen, te verbinden en heel concreet te koppelen. Illustratief voor de reikwijdte van de ambities is het voornemen van de minister van Jeugd en Gezin om de eerdergenoemde 'landelijke kop' bij het EKD zo in te richten dat deze aansluit bij het Landelijk SchakelPunt (LSP) van de digitale zorginfrastructuur. "Daarmee worden dan tegelijkertijd een aantal stappen gezet die noodzakelijk zijn om te zijner tijd aan te kunnen sluiten bij het Elektronisch Patiëntendossier in de zorg.", aldus de minister in zijn brief aan de Tweede Kamer van juli 2008. De wens tot het leggen van verbanden tussen verschillende initiatieven kan teruggevonden worden bij de verwachtingen die er zijn over te leggen verbanden met het Elektronisch Leer Dossier (ELD), waar scholen in het voortgezet onderwijs gegevens in opnemen over ontwikkeling, leren en begeleiden van kinderen. In april 2008 werd voor het ELD een concept 'Businessplan op hoofdlijnen' gepresenteerd (Van Asselt 2008: 32-34).

De tendens naar betrokkenheid van steeds meer partijen via een keten van met elkaar communicerende systemen verlangt een politieke visie op de coördinatie van de coördinatie. Kenmerkend voor keteninformatisering is dat niet langer de organisatorische eenheid of instantie centraal staat, maar een beleidsprobleem of maatschappelijke behoefte. Afspraken over coördinatie en de verantwoordelijkheid daarbij moeten dan om het probleem, om de behoefte dan wel om het belang heen worden georganiseerd. Voor het politiek-bestuurlijke niveau betekent dit dat helderheid gegeven dient te worden wie men vanuit het probleem of de behoefte verantwoordelijk wil laten zijn voor de informatieketen als geheel. Waar ligt de regie en welke instantie in de zorgketen is als eerste aangewezen om verantwoordelijkheid voor bepaalde handelingen en zaken op zich te nemen? Opvallend was in ieder geval dat in het gesprek met de betrokkenen bij ICTU (verantwoordelijk voor de ontwikkeling en het beheer van de landelijke verwijsindex) het punt van de overkoepelende paraplu-verantwoordelijkheid niet werd herkend of erkend.

Illustratief voor het feit dat het antwoord op de voornoemde vragen niet eenvoudig te geven valt, is ook dat in de keten van de jeugdzorg vele actoren samen moeten werken en alle betrokken instanties niet alleen redelijk autonoom zijn in de nadere inkleuring en invulling van hun taken, bevoegdheden en verantwoordelijkheden, maar dat de toepasselijke wetgeving en de financieringsstructuren ook hun invloed hebben op bevoegdheden en daarmee coördinatiemogelijkheden. Bovendien zijn deze bevoegdheden en verantwoordelijkheden nogal verschillend ingevuld en belegd. Zo zijn de Bureaus Jeugdzorg gefinancierd via de provincie, terwijl weer andere spelers hun middelen vanuit de gemeente krijgen. De jeugdgezondheidszorg acteert op basis van de Wet collectieve preventie volksgezondheid,

terwijl de Bureaus Jeugdzorg dat doen via de Wet op de jeugdzorg. Kortom, uniformiteit en helderheid rondom positie, verantwoordelijkheden en bevoegdheden ontbreekt, wat duidelijke afspraken over coördinatie niet eenvoudig maakt. Een relevante vraag is ook – nu het initiatief voor de digitalisering op lokaal niveau wordt belegd – of alle betrokken lokale actoren wel over voldoende expertise beschikken om er zeker van te zijn dat de systemen en de informatie-uitwisseling die hiermee plaatsvindt, voldoen aan de benodigde juridische en technische vereisten.

In een door technologie gefaciliteerde ketensamenwerking neemt ook de complexiteit van relevante drijfveren toe. Diverse partijen in de jeugdzorg percipieren bijvoorbeeld veiligheid nogal verschillend. Bureau Jeugdzorg kijkt bij de veiligheid voornamelijk naar het individuele kind, terwijl de politie eerder het veiligheidsbelang van de samenleving in ogenschouw neemt. Zelfs het uitwisselen van voornamelijk 'dat'-informatie in plaats van 'wat'-informatie lost dit euvel van de verschillende narratieven en perspectieven van professionals niet op. White et al. (2009: 1213) concluderen dat professionals allemaal hun eigen ontologieën hebben en dat zelfs een simpele lijst met verschillende data in potentie een verhaal is. Met name in een systeemomgeving waar informatie gedigitaliseerd en gecomprimeerd is, kan dit gemakkelijk leiden tot verkeerde interpretaties.

Dit brengt ons ten slotte bij de gebruikers van de systemen zelf. Ook zij spelen een belangrijke verbindende rol als het gaat om de verschillende systemen die in het jeugdzorgdomein gebruikt worden. Zelfs wanneer systemen technologisch niet aan elkaar verbonden worden en er dus geen sprake is van ketensamenwerking, fungeren de verschillende professionals wel als knooppunten tussen deze verschillende systemen. Informatie uit het ene systeem komt via hun persoonlijke dossiervorming rond een jeugdige in het andere terecht. In deze is het ook beter te spreken van netwerken dan van ketens. Bij ketens wordt er nog enige mate van overzicht gesuggereerd, terwijl bij netwerken veel meer het wisselende en interactieve element van de informatiestromen tot zijn recht komt. In netwerken is het veel moeilijker overzicht te bewaren over de wijze waarop informatie tussen knooppunten stroomt, wie wat uitwisselt en wie uiteindelijk verantwoordelijk is. In de praktijk van de verschillende systemen die in de jeugdzorg gebruikt worden, raakt informatie via de hulpverleners op veel meer manieren dan uitsluitend via de band van ketensamenwerking verspreid. Behalve het gevaar op verlies van overzicht maakt deze aan het zicht onttrokken netwerkstructuur dat informatie contextloos wordt overgedragen of andere betekenissen krijgt, omdat het zonder duidelijk te traceren historie van het ene dossier in het andere wordt 'overgepend'.

8.5 MOTIEVEN

8.5.1 TRANSPARANTIE

Het zal niet verrassen: via de inzet van niet alleen de verwijsindex, maar ook de andere hiervoor besproken initiatieven, wordt het wel en wee van jongeren transparanter, kenbaarder en herkenbaarder voor de overheid en de keten van zorgverleners. Tegelijkertijd geldt de toegenomen transparantie in veel mindere mate voor het wel en wee van de verwijsindex, in de zin van kenbaarheid voor jongeren van de meldingen die over hen worden gedaan en door welke instanties.
Dat terwijl technologie juist de mogelijkheid biedt om jongeren zelf het nodige inzicht te verschaffen. Met, meest vergaand, een scenario waarin de jeugdzorg via internet aan jongeren inzicht biedt in hun digitale dossier, bijvoorbeeld in de vorm van een digitale kluis zoals vele jaren geleden gepropageerd door de commissie-Snellen in het advies over de modernisering van de Gemeentelijke Basisadministratie (Tijdelijke Adviescommissie Modernisering GBA 2001).

Dat het bestaan en functioneren van de verwijsindex voor de jongeren een (deels) onzichtbaar fenomeen blijft, heeft in belangrijke mate te maken met de politieke keuze dat jongeren (of hun ouders als de jongere nog geen 16 jaar is) pas uiterlijk op het moment van de match op de hoogte behoeven te worden gesteld van het feit dat zij aan de verwijsindex zijn gemeld. Alhoewel de wetstekst aangeeft dat de professional de jongere op de hoogte brengt van het feit dat hij een melding aan het systeem doet, mag deze mededeling worden uitgesteld tot het moment dat er sprake is van een tweede melding (pas op dat moment is feitelijk sprake van een match). Eerder hoeft niet. Immers, zo merkt de minister op, de match betekent uitsluitend dat professionals met elkaar contact hebben opgenomen om de hulp, zorg of bijsturing af te stemmen. "Niets meer en niets minder. De jeugdige wordt dus niet geconfronteerd met voldongen feiten."[33] Ook de VNG toonde zich een voorstander van uitgestelde transparantie: "Ouders en jeugdigen dienen ons inziens niet geïnformeerd te worden bij een melding zoals genoemd in artikel 2r maar bij een match" (VNG 2008: 4). Soms ook hoeft melding in het geheel niet plaats te vinden: "In uitzonderingsgevallen kan de informatieplicht achterwege blijven. Ook dit is geregeld in de Wet bescherming persoonsgegevens. Dat mag alleen indien dat noodzakelijk is in het belang van de bescherming van de jeugdige, of bijvoorbeeld de professional. Hiervan zal dus alleen bij hoge uitzondering sprake zijn. De professional zal hierbij een belangenafweging moeten maken. Bij deze belangenafweging dient de professional de beginselen van zorgvuldigheid, subsidiariteit en doelmatigheid in acht te nemen", aldus de minister.

In de praktijk van alledag blijkt het zorgvuldig en duidelijk informeren van jongeren en hun ouders heel wat complexer dan de papieren 'werkelijkheid'. Juist ook omdat professionals concreet het dilemma ervaren tussen het melden van een

risicojongere en het hebben van een vertrouwensband met de jongere en diens ouders. Niet verrassend concludeert de evaluatie van de proeftuin dan ook dat er bij professionals nogal wat onzekerheid en soms ook onduidelijkheid bestaat over de mededelingen die aan jongeren en ouders gedaan moeten worden (*Evaluatie proeftuin* 2008: 13). Een van de vragen waar zij mee worstelden is of jongeren alleen bij de eerste melding aan het systeem ingelicht moeten worden of iedere keer dat een signaal wordt afgegeven. Bovendien vinden ze het ingewikkeld om aan jongeren en ouders te vertellen wat precies het gevolg is van een risicomelding aan het systeem. Overigens staat niet alleen het belang van de vertrouwensrelatie op gespannen voet met het melden aan de verwijsindex en de transparantie naar jongeren over die melding. Dat geldt ook voor het beroepsgeheim van artsen. De KNMG adviseerde artsen dan ook om in principe alleen een melding te doen met toestemming van de jeugdige of diens ouders. Daarbij wijst de KNMG erop dat "de jeugdige c.q. diens ouders, voordat toestemming wordt verkregen, voldoende is c.q. zijn geïnformeerd over de VIR en de mogelijke gevolgen van de melding" (KNMG 2009). Al met al blijkt sprake van weinig eenduidige opvattingen over de mate van transparantie en het moment waarop ouders en jongeren worden geïnformeerd. De kamerleden Voordewind en Dijsselbloem verzochten de minister dan ook via een motie niet alleen professionals, maar ook ouders en jongeren van eenduidige informatie te voorzien.[34]

Wanneer we niet alleen kijken naar het moment van transparantie, maar ook het instrument dat daartoe wordt ingezet, zien we dat volgens de minister het informeren van de jongeren in de praktijk vaak zal neerkomen op een gesprek tijdens het ingezette hulpverleningsproces. Maar het mag ook anders, zo valt af te leiden uit zijn antwoord op een vraag van de SP-fractie over administratieve lasten en informatievoorziening. "Ten slotte wordt de manier waarop jeugdigen en hun ouders worden ingelicht over de melding niet voorgeschreven. Er hoeft dus geen brief naar hen te worden gestuurd waarin staat dat de jeugdige is gemeld. En ook in die gevallen waarin daarmee wel gewerkt zou worden – dat is aan de gemeenten – zal met een standaardbrief gewerkt kunnen worden." En tenslotte, wat exact krijgt de jongere te horen? In ieder geval zal – aldus de parlementaire stukken – de jeugdige op grond van de Wbp ten minste moeten worden verteld wat het doel van de verwijsindex is. Ook moet hij op de hoogte worden gesteld van de reden waarom hij zal worden gemeld en via welke instantie hij inzage kan krijgen. Daarnaast moet de jeugdige op de hoogte worden gebracht van de overige rechten die hij heeft. Opvallend is dat de minister feitelijke inzage in het systeem in verband brengt met de al dan niet verwerking van persoonsgegevens: "Ouders hebben geen toegang tot het systeem. De ouders zouden ook weinig hebben aan een dergelijke inzagemogelijkheid, aangezien in de verwijsindex geen inhoudelijke informatie staat." Zeker in verband met de eerdere constatering dat op lokaal niveau wel degelijk ook inhoudelijke informatie wordt verwerkt, is het interessant te bezien hoe transparantie zich de komende jaren op lokaal niveau ontwikkelt en

welke afwegingen professionals daarbij maken. Op welk moment blijken hulpverleners een jongere in kwestie in te lichten: in het vroege stadium van de melding of juist op het uiterste moment van de match?

8.5.2 EFFICIËNTIE EN EFFECTIVITEIT

Op landelijk niveau is de introductie van de verwijsindex expliciet gemotiveerd vanuit het beginsel van effectiviteit: de verwijsindex kan alleen effectief zijn als er sprake is van een landelijk dekkend netwerk. Impliciet ligt effectiviteit ook ten grondslag aan de expliciete wettelijke basis die via de nieuwe regeling is gecreëerd voor het gebruik van het Burgerservicenummer (BSN). Door gebruik te kunnen maken van het BSN kan de identiteit van de betrokken jeugdige snel en eenduidig worden vastgesteld. Op lokaal niveau vormt het begrippenpaar efficiëntie en effectiviteit de motivatie voor nog andere ambities met de verwijsindex. Hier lijkt juist de verlokking van het genereren van managementinformatie en het daarmee kunnen sturen op efficiënt en effectief handelen in een keten van professionals groot. In diverse gesprekken bleek de oorspronkelijke doelstelling – zorg voor jeugdigen – daardoor naar de achtergrond te zijn verschoven. Juist vanuit deze constatering moeten we vaststellen dat het primair het onderdeel efficiëntie uit het begrippenpaar (efficiëntie & effectiviteit) is dat een stuwende werking heeft voor de implementatie en ontwikkeling van de verwijsindex. Alhoewel effectiviteit vaak als motief wordt aangedragen, is de uiteindelijke effectiviteit – het feitelijk helpen van jonge en kwetsbare mensen – veel minder aantoonbaar. Veelal gaan voortgangsrapportages over calculeerbare en objectiveerbare afwegingen en beslissingen rondom aantallen dossiers. Zo wordt in diverse gemeenten de effectiviteit van de verwijsindex afgemeten aan het aantal matches dat ontstaat tussen meldende instanties en hun werkgevers. Het jaarverslag 2008 over het lokale signaleringssysteem SISA in de regio Rotterdam meldt bijvoorbeeld dat 30.018 signalen werden afgegeven, waarvan er 2.277 leidden tot een match. Ook op landelijk niveau spreekt de politiek graag in termen van aantallen aansluitingen, signalen en hits bij het duiden van de voortgang van de verwijsindex (Ministerie voor Jeugd en Gezin 2010b). Minder duidelijk echter is hoeveel jeugdigen daadwerkelijk vooruit zijn geholpen dankzij de totstandkoming van een match. Waar de verwijsindex kan leiden tot een efficiëntere samenwerking in de zin van een technisch gefaciliteerde en gestuurde samenwerking, is het verre van duidelijk wat de betekenis van het systeem is voor de effectiviteit van de jeugdhulpverlening. Volgens in ieder geval het, al in subparagraaf 8.4.2 geciteerde, rapport van de RMO en RVZ is die betekenis gering. De raad signaleerde in het advies *Investeren rondom kinderen* diverse problemen van de risicobenadering, die er in feite op neerkomen dat risicosignalering niet effectief is (RMO & RVZ 2009: 36).

8.5.3 KEUZEVRIJHEID

Wanneer we kijken naar het beginsel van keuzevrijheid, dan stellen we allereerst vast dat keuzevrijheid met name relevant is voor de professionals die met de verwijsindex werken. Uit de aard van de problematiek bestaat er voor jongeren weinig tot geen keuzevrijheid. Een jongere zelf heeft immers nauwelijks tot geen invloed op de vraag: wel of geen melding aan het systeem. Hij heeft hoogstens met de Wbp in de hand een recht op verzet, maar ook dit is geen absoluut recht. Keuzevrijheid raakt kortom primair de positie van professionals, in het bijzonder omdat de wijze waarop de verwijsindex zowel technisch als organisatorisch is ingericht hun professionele handelingsruimte inperkt en daarmee hun autonomie onder druk zet.[35]

Professioneel handelen van hulpverleners wordt in technische zin gestuurd door actoren die de inrichting van het systeem en de keuzes voor het gebruik daarvan kunnen bepalen, waaronder gemeenten maar ook systeemontwikkelaars. Hiernaast is, zo bleek hiervoor al, een belangrijk deel van de professionals in feite verplicht met het systeem te werken. Daarbij komt dat zij de afweging over het al dan niet afgeven van een signaal en opname van gegevens in het dossier ter onderbouwing van het signaal vaak zelf niet meer kunnen of mogen maken. Het systeem en de onderliggende (wettelijke) afspraken dicteren in belangrijke mate dat in bepaalde situaties een signaal wordt afgegeven en daarmee relaties worden gelegd. In feite is het aan de hulpverlener om aan te tonen waarom hij geen actie op een signaal ondernam, wat het risico met zich meebrengt dat 'heeft u gemeld' een toetsingscriterium wordt. De veilige weg is dan natuurlijk te handelen. Op lokaal niveau zal de handelingsruimte van professionals overigens nog verder worden ingeperkt. Zo beogen de betrokkenen bij het signaleringssysteem Zorg voor Jeugd dat een jongere die "bij de intake op basis van bepaalde criteria wordt aangemerkt als een jongere met een hulpvraag 'automatisch' wordt opgenomen" (Holla 2008: 13).

Van belang hier is verder dat het wettelijk vastgelegde meldrecht niet een bevoegdheid is die een professional zomaar naast zich neer kan leggen. De minister: "Het feit dat de wet een expliciete bepaling hierover bevat, is een heel duidelijk signaal aan de professional, maar ook aan de maatschappij: deze bepaling maakt een einde aan de onzekerheid en onbekendheid die er thans bestaat over het doen van meldingen; de wet – de Wjz – maakt klip en klaar dat er geen juridische beletselen zijn om te melden. Deze duidelijkheid is zowel goed voor de professional, als voor de burger, die hierdoor weet wat hij van de instanties kan verwachten en ook weet wat de plichten van die instanties zijn en wat zijn eigen rechten zijn. Het meldrecht is in mijn ogen dus een stevig recht. Ik verwacht dat de professional in de zorg (in ruime zin) met dit recht goed zal kunnen omgaan, het in zal zetten waar nodig, maar er ook niet lichtvaardig mee om zal gaan." Dit 'stevige recht' heeft ook institutioneel handen en voeten gekregen. Als er een match tot stand komt krijgen

beide melders een e-mail met daarin de contactgegevens van de andere melder. Na deze match dienen beide professionals zo snel mogelijk contact met elkaar op te nemen. De gemeentelijke regievoerder moet, zoals in paragraaf 8.3 is aangegeven, erop toezien dat dit ook feitelijk gebeurt.

Afgezien van de factoren die min of meer direct in verband met het initiatief van de verwijsindex staan, komt de eigen professionele opvatting over de omgang met medische en psychosociale gegevens van jongeren (moreel) onder druk te staan door de politieke opvattingen over het beeld dat van jongeren verkregen moet worden. In de ogen van de wethouders van de vier grote gemeenten moet dit beeld met behulp van de verwijsindex en het EKD een *volledig* beeld zijn. Als reden voeren ze in hun brief aan de minister voor Jeugd en Gezin van 10 juli 2007 niet alleen aan dat alleen bij een dergelijk beeld de brede zorgcoördinatie en risicosignalering is waar te maken. Een beperkte variant (dat wil zeggen alleen een beeld op basis van medische gegevens) zou ook leiden tot "*onacceptabele desinvesteringen*" (cursief auteurs) en is "voor onze gemeenten een stap terug" (wethouders Jeugd van Amsterdam, Utrecht, Rotterdam en Den Haag 2007). Daarbij komt ook nog dat voor de politiek het verkrijgen van een beeld van een *individuele* jongere niet langer toereikend lijkt. Vanuit de Tweede Kamer bereikte de minister via de motie Sterk het verzoek om de verwijsindex uit te breiden tot de gezinssituatie, zodat signaleringen over meerdere jeugdigen in één gezin bij elkaar zijn te brengen (Kamerstukken II, 2008/09). Zo ontstaat niet alleen een volledig, maar ook een allesomvattend beeld van jongeren. Alhoewel de minister in eerste instantie liet weten deze stap vooralsnog niet op landelijk niveau te willen zetten, veranderde hij om niet nader uitgewerkte redenen zijn mening en meldde hij in 2010 aan de Kamer dat aan de gezinsfunctionaliteit en de daartoe noodzakelijke wettelijke borging wordt gewerkt (Ministerie voor Jeugd en Gezin 2010b: 21).

Gegeven dit politiek-bestuurlijke klimaat om een zo volledig en omvattend mogelijk beeld van jongeren te verkrijgen, zou een terughoudende opstelling van professionals geïnterpreteerd kunnen worden als een spaak in het wiel van de verwijsindex. Illustratief voor de druk die op professionals wordt uitgeoefend is de observatie van de KNMG dat JGZ-artsen door hun GGD "de opdracht" krijgen om het aantal signaleringen in de verwijsindex te verhogen, "bijvoorbeeld door te eisen dat 'Op 1 december 2009 moet uw team 40 procent meer kinderen signaleren … dan nu'" (KNMG 2009). Alhoewel de minister in een reactie op dit bericht aan de Tweede Kamer liet weten geen aanwijzingen te hebben dat van een beleid als gesuggereerd sprake zou zijn (Ministerie voor Jeugd en Gezin 21 januari 2010), vindt toetsing van de verwijsindex in de praktijk vooralsnog uitsluitend plaats aan de hand van kwantitatieve factoren (percentages en getallen)[36] en is er daarmee een gerede kans dat ook juist op die factoren wordt gestuurd. Zo meldde een rapportage van het SISA-verwijssysteem aan het Rotterdamse college naar aanleiding van een geconstateerde daling van het aantal signalen door het Centrum voor

Jeugd en Gezin dat "wordt bekeken waar die daling vandaan komt" (Rapportage SISA-signaleringssysteem 2010: 3). Illustratief is in dit verband ten slotte dat de Vereniging van Nederlandse Gemeenten in de reactie op de conceptwetgeving naar de minister sterk aandrong de doorzettingsmacht van gemeenten in het wetsvoorstel te regelen: "Mochten er op basis van meldingen in de VIR signalen binnenkomen dat een situatie met een jeugdige uit de hand loopt en de meldingsbevoegden nemen daarop, aangesproken door de regievoerder, hun verantwoordelijkheid niet of onvoldoende, dan moet helder zijn wie uiteindelijk de doorzettingsmacht heeft om zaken te regelen en hulpverleners een aanwijzing te geven" (VNG 2008: 2).

Een laatste inperking van de professionele autonomie houdt verband met het feit dat individuele hulpverleners niet langer zelfstandig kunnen besluiten bepaalde gegevens uit een digitaal dossier te verwijderen. Gedeelde systemen en keteninformatisering maken dit onmogelijk. Weliswaar kunnen professionals een signaal laten vervallen, waarmee er geen actief signaal meer is (en mogelijk dus ook geen match plaatsvindt), de melding blijft op de achtergrond bewaard. Kortom, besluit een hulpverlener een gegeven of een signaal in te voeren, dan geeft hij de jongere als het ware uit handen en staat de ontwikkeling van deze jongere in de meest vergaande situatie nog tientallen jaren in de overheidssystemen als sociaalpsychologisch risicovol te boek.[37] Het voorgaande raakt natuurlijk ook aan de vertrouwenspositie van de individuele hulpverlener en de rol van vertrouwen in de relatie tussen jeugdige en diens ouders en de hulpverlener. Overigens komt deze vertrouwensband ook onder druk te staan doordat anoniem melden in de verwijsindex vrijwel onmogelijk is. Daarbij: een match betekent bijna altijd actie. Het is niet verwonderlijk dat hulpverleners zorgen hebben over de effecten hiervan voor de vertrouwensrelatie die zij met een jongere of een gezin hebben.

8.5.4 ACCOUNTABILITY

Wat de analyse in deze studie in ieder geval duidelijk maakt is dat bij de verwijsindex een wirwar van partijen betrokken is. Partijen die ieder vanuit hun professie gebonden zijn aan eigen voorwaarden voor de verantwoordelijkheid voor hun handelen. Maar ondertussen worden al deze werelden op technisch niveau met elkaar verbonden. En dat betekent dat jongeren en hun ouders potentieel met ieder van die actoren en daarmee het gevarieerde scala aan voorwaarden van doen kunnen krijgen. Het risico is daarmee zeker niet ondenkbaar dat zij in de keten verstrikt raken (Nationale Ombudsman 2009). Dat roept de vraag op of in het wettelijk regime een regeling is getroffen voor de eindverantwoordelijke. Met andere woorden of er een overkoepelende verantwoordelijkheid is gecreëerd over ieder van de individuele meldende instanties heen. Zoals hiervoor in subparagraaf 8.4.2 al werd opgemerkt, is niet alleen het systeem als zodanig complex, maar geldt dat ook voor diverse kwesties rondom verantwoordelijkheid.

In de wet wordt de minister voor Jeugd en Gezin aangemerkt als verantwoordelijke voor de verwijsindex, met één uitzondering. Die uitzondering is dat de colleges van burgemeester en wethouders verantwoordelijk zijn voor de toepassing van de artikelen 34 tot en met 40 en 43 van de Wbp. De gemeenten zijn dus voor de jeugdige en zijn ouders het directe aanspreekpunt als het gaat om vragen over opname in de verwijsindex of het maken van bezwaar daartegen. Gemeend is dat dit voor de jeugdigen en hun ouders van groot belang is, aangezien een aanspreekpunt op afstand letterlijk een drempel voor hen kan zijn. Te meer, daar zij in de regel al veel met gemeentelijke en meldende instanties te maken zullen hebben gehad. Het is dan verwarrend als zij voor de verwijsindex naar een andere instantie – de minister – zouden moeten. Bovendien is de gemeente zelf de spil waar het gaat om de lokale samenwerking, in het algemeen, en waar het de verwijsindex betreft, aldus de minister. De uitzondering kon niet op instemming van het College bescherming persoonsgegevens rekenen (CBP 2008: 6). Het CBP vroeg zich allereerst af of het wel mogelijk is om de verantwoordelijkheid ten aanzien van een deel van de Wbp-verplichtingen bij wet aan een andere instantie op te dragen. Hiernaast maakt de voorgestelde constructie het systeem van verantwoordelijkheid alleen nog maar complexer, aldus het CBP.

Problematisch aan het centraal beleggen van verantwoordelijkheid is overigens wel dat de instantie die een oordeel moet vellen op een verzoek van een jongere, bijvoorbeeld een correctieverzoek, in feite ook inhoudelijke informatie ter beschikking moet staan. Immers, om te kunnen beslissen op een correctieverzoek van een jongere moet deze instantie niet alleen op de hoogte zijn van de gegevens uit de verwijsindex zelf (het signaal), maar ook kennis kunnen nemen van de achterliggende inhoudelijke informatie die voor de professional die de melding deed de concrete aanleiding vormde om een signaal af te geven (zie ook CBP 2008). Het CBP riep de minister op een laagdrempelig centraal loket in te richten, waar de betrokkene terecht kan met vragen en klachten. Dit loket zou desgewenst te benaderen kunnen zijn via de gemeenten. Hier zou de jongere of diens ouders eenvoudig na moeten kunnen gaan of en door wie hij gemeld is in de verwijsindex. "Voor het uitoefenen van het recht op correctie en verzet zou de betrokkene zich dan rechtstreeks kunnen vervoegen bij de meldingsbevoegde door wie hij is aangemeld" (CBP 2008: 6).

8.5.5 PRIVACY

Wie de parlementaire behandeling van de verwijsindex erop naslaat, treft niet alleen een beperkte, maar ook een sterk gepolariseerde opvatting over de privacy-implicaties van het initiatief aan. Een beperkte opvatting, omdat de minister privacy lijkt gelijk te stellen aan beveiliging: "De privacyaspecten zijn in de verwijsindex geborgd door het gebruik van zware beveiligingsprocedures. De toegang tot de verwijsindex wordt geregeld met PKI-overheidscertificaten."[38]

Een gepolariseerde opvatting als de minister stelt: "Bescherming van privacy mag niet gebruikt worden als excuus om jeugdigen die in de problemen zitten niet te helpen."[39] En: "Gesteld mag worden dat ook in de maatschappij anders over privacy wordt gedacht dan zo'n twintig, dertig jaar geleden, omdat duidelijk is geworden dat er door te zwijgen dingen kunnen voortgaan die het daglicht niet kunnen verdragen. De professional is daardoor in zekere zin onzeker geworden over wat wel en niet is toegestaan. Het wetsvoorstel verwijsindex en de publiciteit daaromheen raakt deze discussie in het hart: door een expliciet meldrecht te creëren wordt een duidelijk signaal afgegeven dat melden nodig kan zijn en is toegestaan. De verwijsindex maakt het lastige onderwerp van zwijgen, melden en privacy bespreekbaar tussen professionals, binnen en tussen instellingen en in de maatschappij en trekt de discussie daarover uit de nevel van onduidelijkheid en onzekerheid. (…) Hierdoor zullen aan de ene kant de professionals meer duidelijkheid krijgen omtrent hun speelruimte en de afwegingen die zij daarbij hebben te maken, en zullen aan de andere kant jeugdigen en hun ouders of andere verantwoordelijken meer duidelijkheid krijgen over hun positie en wat zij van de hulpverlening kunnen verwachten. In die zin is de verwachting dat we toegroeien naar een cultuuromslag waarin melden meer de norm wordt, en er tegelijkertijd veel aandacht is voor een zorgvuldige voorbereiding en belangenafweging. Het gaat daarbij niet om het 'melden om te melden', maar om het melden van daadwerkelijk meldenswaardige situaties." Na het lezen van deze passages is het niet verrassend dat zowel de Raad van State als het College bescherming persoonsgegevens op dit punt kritisch over het voorstel adviseerde en meer algemeen vaststelde dat de regering ten onrechte voorbijgaat aan privacybelangen bij de diverse initiatieven in de jeugdzorg (Kamerstukken II 2007/08b: 5).

Soms komt privacy toch in beeld. Dat was op lokaal niveau het geval toen de politiek vanuit de gemeenschap onder druk werd gezet omdat, zoals in Rotterdam, ouders zich keerden tegen de in hun ogen intimiderende vragenlijsten die de gemeente had opgesteld om opvoedingsproblemen vroegtijdig te signaleren. Ook de Tweede Kamer uitte zich zeer kritisch over een soortgelijke vragenlijst.[40] Privacy komt ook in beeld via het populaire beleidsthema Privacy by Design. Zo bevat de wet enkele – zij het nogal eenvoudige – voorzieningen die als voorbeelden van het populaire beleidsthema Privacy by Design vallen te karakteriseren. Misbruik van het systeem (bijvoorbeeld institutionele nieuwsgierigheid) wordt niet alleen organisatorisch maar ook technisch aangepakt. Nogal vanzelfsprekend is de maatregel dat de verwijsindex alleen voor geautoriseerde professionals toegankelijk is en de voorziening hierop periodiek dient te worden getoetst. Het principe van de verwijsindex dat professionals geen inzagerecht hebben en slechts een melding aan de verwijsindex kunnen doen, voorkomt volgens de parlementaire stukken eveneens gebruiksfraude. Ten slotte verlangt de wet dat door middel van logging het meldgedrag van een professional nagegaan moet kunnen worden.

8.6 SLOT

Het moge duidelijk zijn dat de digitalisering in de jeugdzorg vele voordelen en kansen met zich meebrengt. De ambitie om jeugdigen niet uit het oog te verliezen en zij die het nodig hebben zo snel mogelijk hulp te bieden door hen van adequate en efficiënt georganiseerde zorg te voorzien, is noodzakelijk en nastrevenswaardig. Dat in technologie een mogelijkheid wordt gezien om deze ambitie waar te maken, ligt in lijn met een maatschappijbrede ontwikkeling waarbij steeds vaker op verschillende terreinen informatiesystemen worden ontwikkeld en ingezet om doelen te verwezenlijken die anders niet of slechts heel moeizaam bereikt zouden kunnen worden. "Voor beleidsmakers is informatietechnologie de magic bullet voor de misère in de jeugdketen" (Horstman 2010: 13). Wat in het domein van de jeugdzorg opvalt, is dat ambities op centraal en decentraal niveau uiteenlopen. Daarmee ook loopt de verdere uitbouw van de verwijsindex steeds meer uiteen, wat vervolgens weer consequenties heeft voor de vorm en inhoud van de systemen en informatieprocessen. Als we kijken naar de digitaliseringsslag in de jeugdzorg, en meer specifiek naar de case van de Verwijsindex Risicojongeren, dan zien we dat er op centraal niveau voor wordt gekozen een substantieel deel van de verantwoordelijkheid (zowel als het gaat om de ontwikkeling, uitrol als ook om het beheer van het systeem) op decentraal niveau te beleggen. Positief ingezet maakt deze aanpak het mogelijk ruimte te laten voor de noden en bijzonderheden op lokaal niveau. Er kan een systeem ontworpen worden geheel toegespitst op de plaatselijke situatie.

De andere kant van de medaille is echter dat controle en toezicht op de invulling van deze decentrale ruimte beperkt is. Zo richtte het programmaministerie voor Jeugd en Gezin zich voornamelijk op het opleggen van technische eisen en richtlijnen. De feitelijke inhoud van het lokale systeem – de wijze waarop informatiestromen lopen en hoe bepaalde verantwoordelijkheden vorm krijgen (bijvoorbeeld als het gaat om beheer en doorontwikkeling) – wordt niet of nauwelijks in ogenschouw genomen. Hierdoor ontstaan er als het ware twee werkelijkheden: de wereld van de tekentafel op rijksniveau waar een systeem omschreven wordt en de wereld van de werkvloer op lokaal niveau waar niet alleen een technisch systeem, maar ook de achterliggende informatieprocessen inhoudelijk vorm krijgen. Kijkend naar de ontwikkelingen kunnen we stellen dat op rijksniveau de aandacht primair uitgaat naar *technologie*, terwijl juist op lokaal niveau *informatie* en daarmee verbonden processen (en daarmee te realiseren functionaliteiten) de cruciale factor lijkt te zijn.

Wat verder opvalt is dat met de keuze om de ontwikkelingen voor een belangrijk deel ook op lokaal niveau neer te leggen, sturing op en verantwoording van de uitbouw en het gebruik van de verwijsindex problematisch wordt. Zo zien we dat op centraal niveau een organisatie als ICTU, met veel professionele kennis tot zijn

beschikking en ressorterend onder de bestuurlijke verantwoordelijkheid (en daarmee toezicht) van het ministerie van BZK, een landelijk systeem opbouwde, terwijl op lokaal niveau gemeenten of regio's voor hun eigen specifieke variant zelf in zee (moesten) gaan met (semi)commerciële partijen waarbij de publieke controle op het eindresultaat summier te noemen is. Bovendien is het maar de vraag of gemeenten, alhoewel zij meer kennis hebben van de plaatselijke noden en daarop het systeem en de informatieprocessen zouden kunnen inrichten, ook meteen vanuit deze kennis een betere opdrachtgever zijn dan de centrale overheid. Hebben zij juist op andere vlakken dan de jeugdproblematiek gerelateerde zaken genoeg kennis en middelen in huis om ervoor te zorgen dat het systeem daadwerkelijk zo ontwikkeld wordt dat de lokale doelstellingen behaald worden? Of is het in de praktijk zo dat deze commerciële partijen heel veel invloed hebben op de uiteindelijke functionaliteit en werking van het systeem? De risico's daarvoor zijn in ieder geval volop aanwezig. Relevant daarbij is dat – als we althans mogen afgaan op de eigen communicatie van het College bescherming persoonsgegevens (jaarverslagen, website) – van toezicht op de gekozen functionaliteit en gegevensverwerking van de lokale systemen nauwelijks sprake is.

Relevant is ook de dynamiek die we ontwaren rondom de meldcriteria. Op rijksniveau is er op de tekentafel een lijst met meldcriteria ontworpen die verder ingevuld worden door de lokale organisaties die melden aan de VIR. Het voordeel hiervan is dat organisaties rekening kunnen houden met de lokale context waarin risico's zich kunnen voordoen. Een bepaalde situatie kan in de grote stad eerder leiden tot een mogelijk risico dan een soortgelijke situatie op het platteland. Tegelijk leidt dit echter ook tot een enorme diversiteit aan meldingscriteria op de werkvloer waarvan sommige criteria op zijn minst twijfelachtig zijn te noemen. Zo worden kinderen op de peuterspeelzalen in Rotterdam gesignaleerd als de ouders een schuldenproblematiek hebben, of als (een van de) ouders een geestelijke dan wel lichamelijke handicap heeft. Ook kinderen van gescheiden ouders die niet op goede voet met elkaar staan, worden gemeld (Risicoprofiel SISA 2010). Hoewel het zo kan zijn dat het hier gaat om adequate risicoschetsen, is dat gezien het weinige toezicht hierop niet of nauwelijks te toetsen.

Op rijksniveau wordt de Verwijsindex Risicojongeren omschreven als een zeer gewenst maar niet verplicht systeem. Als de individuele hulpverlener geen baten ziet in het gebruik van de VIR is hij niet bij wet verplicht te melden. Op de werkvloer lijkt het voor hulpverleners echter niet zo eenvoudig zich aan het systeem te onttrekken. Niet alleen omdat hulpverleners die in dienst zijn van een instantie zich hebben te houden aan de intern gemaakte afspraken over signaleren, maar ook omdat lokale systemen zoals in Rotterdam en Noord-Brabant voortgangsbewaking en andere beheersfuncties kennen die toezicht op de hulpverlener en het opvolgen van signalen mogelijk maken. Als de hulpverlener zich aan dat laatste niet onderwerpt, kan dat onder meer gevolgen hebben voor de wijze waarop zijn

functioneren beoordeeld wordt (en uiteindelijk ook zijn verantwoordelijkheid en aansprakelijkheid). Wat hij doet is dan immers niet zichtbaar voor het systeem. Dit alles kan er ook toe leiden dat de druk om toch maar te signaleren zeer groot wordt. Hulpverleners willen immers niet de ontbrekende schakel in de jeugdzorg zijn wanneer er onverhoopt iets met een kind fout blijkt te zijn gegaan. Het risico bestaat dat de hulpverlener het als zijn taak ziet te melden en, vanaf dat ogenblik, meent dat het systeem de verantwoordelijkheid overneemt. Dit alles leidt tot de vraag in welke mate de professionele autonomie van de hulpverlener wordt beperkt door de functionaliteit die de VIR lokaal krijgt.

Zonder hier verder in te gaan op de wenselijkheid van deze ruimte voor lokale invulling en de aard van deze invulling, kunnen we wel stellen dat het debat over de digitalisering van de jeugdzorg, met de introductie van de Verwijsindex Risicojongeren als sprekend voorbeeld, armoedig is. De discussie beperkt zich tot de tekentafelontwerpen op rijksniveau, terwijl de echt prangende vragen en dilemma's eigenlijk op lokaal niveau verscholen gaan. De vraag is dan ook of de voordelen van de ruimte die op centraal niveau gegeven wordt aan het decentraal niveau, opwegen tegen het ontstane gebrek aan inzet, overzicht en toezicht op de processen en ontwikkelingen op de lokale werkvloer.

NOTEN

1 Wet van 4 februari 2010 tot wijziging van de Wet op de jeugdzorg in verband met de introductie van de verwijsindex, Staatsblad 2010, 89.
2 http://www.meldcriteria.nl/, geraadpleegd 25 oktober 2010.
3 31 855, nota naar aanleiding van het verslag, blz. 13.
4 31 855, Memorie van Antwoord, blz. 2.
5 Het oorspronkelijke wetsvoorstel kende een halfopen systeem, inhoudende dat er naast artikel 2j nog een vangnetbepaling was opgenomen. De vangnetbepaling maakte het mogelijk dat professionals ook bij andere, niet nader in de wet genoemde risico's tot een melding aan de verwijsindex zouden mogen overgaan. Deze bepaling is geschrapt naar aanleiding van het advies van de raad en omgezet in een limitatieve lijst.
6 31 855, nota naar aanleiding van het verslag, blz. 2.
7 31 855, nr. 33; 31 855, nr. 50.
8 31 855, nota naar aanleiding van het verslag, blz. 25.
9 31 855, nota naar aanleiding van het verslag, blz. 26.
10 31 855, nota naar aanleiding van het verslag, blz. 6.
11 http://www.sisa.rotterdam.nl/index.php?pageID=3686, geraadpleegd op 14 januari 2010. Het betreft de website van het lokale signaleringssysteem SISA van de regio Rotterdam.
12 Staatsblad 2010, 302.
13 Door de overheid gefinancierde organisaties ter ondersteuning van mensen met een handicap, beperking of chronische ziekte – www.mee.nl.
14 http://www.samenwerkenvoordejeugd.nl/smartsite.net?id=842&proj=789, geraadpleegd op 5 oktober 2010.
15 http://noord-brabant.zorgvoorjeugd.nu/userfiles/file/20100630%20VIR%20special.pdf, geraadpleegd op 5 oktober 2010.
16 Algemene Brochure Zorg voor Jeugd, blz. 2. http://noord-brabant.zorgvoorjeugd.nu/images1/zorgvoorjeugd/bestanden/ZVJ2_scherm.pdf, geraadpleegd op 18 januari 2010.
17 Factsheet SISA, Stadsregio november 2009, http://www.sisa.rotterdam.nl/download.php?itemID=15911, geraadpleegd op 18 januari 2010.
18 Rapportage SISA-signaleringssysteem 4e kwartaal 2009, blz. 4. http://www.sisa.rotterdam.nl/download.php?itemID=17110, geraadpleegd op 6 april 2010.
19. http://www.sisa.rotterdam.nl/download.php?itemID=21950, geraadpleegd op 5 oktober 2010.
20 Overigens ervaren de gebruikers van KIDOS het eigenaarschap bij de publieke instelling juist als een voordeel.
21 Staatsblad 2010, 302.
22 31 855, nota naar aanleiding van het verslag, 31 855, blz. 31.
23 Memo betreffende Rapportage SISA-signaleringssysteem 1e kwartaal 2010 aan de

Wethouder Jeugd, Gezin, Onderwijs en Sport van de Gemeente Rotterdam, blz. 2.

24 Staatsblad 2010, 302, blz. 15.

25 Het wetsvoorstel (31 316) werd mei 2008 door de Tweede Kamer goedgekeurd en in juli 2008 vond de eerste behandeling in de Eerste Kamer plaats.

26 Stb. 2008, 406; Stb. 2008, 482.

27 31 855, nota naar aanleiding van het verslag, blz. 6.

28 31 855, nota naar aanleiding van het verslag, blz. 6.

29 31 855, nota naar aanleiding van het verslag, blz. 7.

30 Waarbij we overigens moeten vaststellen dat een omvattende conceptuele analyse van het begrip veiligheid ontbreekt.

31 Zo wordt in de studie van de Radboud Universiteit t.b.v. het Prokid-project opgemerkt: "In het huidige onderzoek kon geen aandacht besteed worden aan mogelijke etnische verschillen in de effecten die bepaalde criteria kunnen hebben op het gedrag van kinderen. Omdat de gezinssituaties kunnen verschillen voor kinderen uit de Nederlandse cultuur en kinderen met een etnische minderheid achtergrond, en ook de betekenis van bepaalde factoren voor recidive kunnen verschillen over culturen is het raadzaam om hier verder onderzoek naar te doen. Op die manier kan het mogelijk worden om adequaat en op maat te reageren wanneer een kind bepaalde signalen uitzendt, rekening houdende met de culturele achtergrond van dat kind", supra noot 25, blz. 78.

32 Hiernaast bestaan er twijfels over de kwaliteit van ministeriële regelingen en de waarborgen voor kwaliteit (Voermans & Eijlander 2002).

33 Overigens krijgen ouders in Rotterdam een (standaard)brief als hun kind gemeld wordt (dus voordat er een match plaatsvindt) en tevens als er een match heeft plaatsgevonden.

34 Motie voorgesteld 1 juli 2009, 31 855, nr. 41.

35 Overigens concludeerde het College bescherming persoonsgegevens in het advies over het Ontwerpbesluit Verwijsindex Risicojongeren dat "de professionaliteit van de meldingsbevoegden in het ontwerpbesluit onvoldoende is gewaarborgd" nu er onvoldoende garanties zijn dat diens opleiding de meldingsbevoegde in staat stelt te beoordelen of het criterium op grond waarvan hij meldt van toepassing is (CBP 2009: 3-4).

36 Zie bijvoorbeeld de uitspraken hierover op de website van Zorg voor Jeugd onder "Verwijsindexmonitor" (http://noord-brabant.zorgvoorjeugd.nu/detailnews.asp?newside=103).

37 In het oorspronkelijke wetsvoorstel EKD zouden de opgenomen gegevens worden bewaard gedurende 15 jaar vanaf het moment dat een kind de meerderjarige leeftijd bereikt. Met andere woorden, tot de leeftijd van 32 jaar.

38 En: "De verwijsindex is ontworpen met toepassing van de meest actuele beveiligingsvoorschriften (NEN7510). Periodiek wordt door officiële instanties het beveiligingsniveau gecontroleerd op mogelijke hack- en kraakbedreigingen. Bij het beheer van de verwijsindex wordt een actief beleid gevoerd op de waarborging van de beveiligingsniveaus."

39 31 855, nota naar aanleiding van het verslag, blz. 25.
40 *Algemeen Dagblad*, 4 juni 2009 "Meer oog voor privacy bij kinddossier".

LITERATUUR

Asselt, R. van (2008) 'Elektronisch leerdossier voor doorlopende leerwegen', *OnderwijsInnovatie*, juni: 32-34.

Aarntzen-Tacken, I.L., R.H.J. Scholte & R.C.M.E. Engels (2008), *Gezinsgebonden risicofactoren voor overlastveroorzakend en crimineel gedrag bij twaalfminners*, Nijmegen.

Beck, U. (1997) *De wereld als risicomaatschappij*, Amsterdam: De Balie.

Berge, I. ten (2005) 'Tovermiddel of nieuwe valkuil? Voordelen en beperkingen van risicotaxatie', *Tijdschrift voor kindermishandeling* 4.

Bekkers, V., A. van Sluis & P. Siep (2006) *De nodale oriëntatie van de Nederlandse politie: over criminaliteitsbestrijding in de netwerksamenleving, Bouwstenen voor een beleidstheorie*, Rotterdam: Centre for Public Innovation.

Boutelier, H. (2005) *De veiligheidsutopie. Hedendaags onbehagen en verlangen rond misdaad en straf*, Den Haag: Boom Juridische uitgevers.

Buruma, Y. (2005) *De dreigingsspiraal. Onbedoelde neveneffecten van misdaadbestrijding*, Den Haag: Boom Juridische uitgevers.

Buruma, Y. (2006) 'Toekomstvoorspelling en repressieve maatregelen', (vooraf) *Nederlands Juristenblad 2006:* 559.

Brouwer, E.R. & D. Houtzager (2009) 'De Verwijsindex Antillianen: Registratie naar etniciteit en een (te) beperkte uitleg van het discriminatieverbod door de Afdeling Bestuursrechtspraak', *Nederlands Juristenblad* 203, 5: 302.

CBP (2008) *Wetgevingsadvies Verwijsindex Risicojongeren*, 9 juni 2008.

CBP (2009) *Advies over het Ontwerpbesluit Verwijsindex Risicojongeren*, Den Haag, 20 oktober 2009.

Clarke, R. (1994) 'The digital person and its application to data surveillance', *The Information Society* 10, 2: 77-92.

Dienst Maatschappelijke Ontwikkeling (2010), http://www.dmo.amsterdam.nl/onderwijs/matchpoint_jeugd_en/matchpoint_jeugd_en geraadpleegd op 8 februari 2010.

Dienst Preventie, Jeugdbescherming en Reclassering (1996), *Signalen voor toekomstig crimineel gedrag. Een onderzoek naar de signaalwaarde van kinderdelinquentie en probleemgedrag op basis van casestudies van ernstig criminele jongeren:* Den Haag.

Evaluatie proeftuin Verwijsindex Risicojongeren (2008), Andersson Elffers Felix, Utrecht, december 2008.

Farrington, D.P. (2005), 'Childhood Origins of Antisocial Behavior', *Clinical Psychology and Psychotherapy*, 12: 177-190.

Garland, D. (2001) *The Culture of Control. Crime and Social Order in Contemporary Society,* Chicago: The University of Chicago Press.

Garrett, P.M. (2004) 'The electronic eye: emerging surveillant practices in social work with children and families', *European Journal of Social Work* 7, 1: 57-71.

Garrett, P.M. (2005) 'Social work's 'electronic turn': notes on the deployment of informa-

tion and communication technologies in social work with children and families', *Critical Social Policy* 25, 4: 529-533.
Gemeentelijke Ombudsman Amsterdam (2006), *Rapport RA0612546*, 18 december 2006: Amsterdam.
Graaf, M. de et al. (2005) *De Nederlandse Jeugdzorg in cijfers*, NIZW.
Gunsteren, H. van (2008) 'Burgerschap en veiligheid in Nederland', blz. 169-183 in G. Alberts et al. (red.) *Burger in uitvoering. Jaarboek Kennissamenleving*, Amsterdam: Aksant.
Haggerty, K. & R. Ericson (2000) 'The surveillant assemblage', *British Journal of Sociology* 51, 4: 605-622.
Hall, C., N. Parton, S. Peckover & S. White (2010) 'Child-Centric Information and Communication Technology (ICT) and the Fragmentation of Child Welfare Practice in England', *Jnl Soc. Pol.*, Cambridge University Press: 1-21.
Hoekstra, R.J. (2009) 'Jaarrede Nederlandse Juristenvereniging 12 juni 2009', *Nederlands Juristenblad,* 2009: 1261.
Hof, S. van der, R. Leenes & S. Fennell (2009) *Framing citizen's identities. The construction of personal identities in new models of government in the Netherlands*, Tilburg.
Holla, Poelman & Van Leeuwen advocaten (2008), *brief*, 28 maart 2008.
Horstman, K. (2010) *Dikke kinderen, uitgebluste werknemers en vreemde virussen. Filosofie van de publieke gezondheidszorg in de 21e eeuw*, rede Maastricht, 25 juni 2010.
Ieder Kind Wint (2010) http://iederkindwint.nl, geraadpleegd op 8 februari 2010.
Janssen, H. (2008) 'Preventie en privacy: behoedzaamheid geboden met gegevens over ras en etniciteit', in P. van Sasse et al. (red.) *Handhaving van de openbare orde: is voorkomen beter dan genezen?*, Den Haag: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
Keymolen, E. (2007) *Helmuth Plessner ontmoet profiling*, scriptie, Rotterdam: EUR.
Keymolen, E. & D. Broeders (2010a) 'Verloren onschuld. Inzicht en toezicht binnen de Verwijsindex Risicojongeren', blz. 73-90 in W. Pieters et al (red.) *Inzicht en toezicht. Controle in de kennissamenleving*, Amsterdam: Aksant.
Keymolen, E. & D. Broeders (2010b) 'Innocence Lost. Care and Control in Dutch Digital Youthcare', paper presented at the *IPA 2010 Conference Discourse and Policy Practices: Politics – Legitimacy – Power*, Grenoble, June 23-25, 2010.
Kamerstukken II (2005/06), 29 284, nr. 18, blz. 5.
Kamerstukken II (2004/05), 30 131, nr. 3.
Kamerstukken II (2007/08a), 28 684, nr. 119.
Kamerstukken II (2007/08b), 31 316, nr. 4.
Kamerstukken II, (2008/09), 31 855, nr. 38.
KNMG, *Brief van 22 december 2009 aan de Eerste Kamer inzake de Verwijsindex Risicojongeren*, Utrecht.
Lahav, G. & V. Guiraudon (2000) 'Comparative perspectives on border control: Away from the border and outside the state', blz. 55-77 in *The wall around the west. State borders and immigration controls in North America and Europe*, Lanham: Rowman and Littlefield publishers.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2008) *Politie gaat kans op criminaliteit bij kinderen signaleren*, http://www.minbzk.nl/114112/politie-gaat-kans-op, geraadpleegd op 8 februari 2010.

Ministerie voor Jeugd en Gezin (2005) Brief aan de Tweede Kamer, 5-12-2005, kenmerk: PG/OGZ-2640352.

Ministerie voor Jeugd en Gezin (2007) *Brief van 6 november 2007,* Kamerstuk, 2007/08, 31 001, nr. 33: Den Haag.

Ministerie voor Jeugd en Gezin (2007), *Alle Kansen voor Alle Kinderen*, http://www.jeugdengezin.nl/rapporten/2007/alle-kansen-voor-alle-kinderen.asp, geraadpleegd op 8 februari 2010.

Ministerie voor Jeugd en Gezin (2008a) *Resultaten haalbaarheidsstudie ketenbrede informatieuitwisseling*, Brief aan de Eerste en Tweede Kamer, Den Haag.

Ministerie voor Jeugd en Gezin (2008) Beleidsagenda 2009, Den Haag.

Ministerie voor Jeugd en Gezin (2009) *Beleidsagenda Jeugd en Gezin 2010*: Den Haag.

Ministerie voor Jeugd en Gezin (2010a) *Brief van 21 januari 2010*, Kamerstuk, 2009/10, 31 855, F.

Ministerie voor Jeugd en Gezin (2010b) *Brief van 19 mei 2010 met de voortgangsrapportage over het programma 'Samenwerken voor de jeugd'*, Kamerstuk 2009/10, 31 001, nr. 91.

Ministerie van Justitie, Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), *Moeilijke jeugd. Risico- en protectieve factoren en de ontwikkeling van delinquent gedrag in een groep risicojongeren*, Den Haag 2000.

Ministerie van Justitie (2009) *Nieuwsbrief programma Aanpak jeugdcriminaliteit*, jaargang 2, editie 2 (april 2009).

Ministerie van Justitie (2010) *Helpdesk Privacy Jeugd en Gezin (HPJG), http://www.justitie.nl/onderwerpen/jeugd/helpdesk-privacy/HPJG/#,* geraadpleegd op 8 februari 2010.

Ministerie van Justitie & Ministerie voor Jeugd en Gezin (2008) *Overlast door 12-minners. Een stevige aanpak*, 12 september: Den Haag.

Ministerie van Volksgezondheid, Welzijn en Sport (2006) *Brief aan de Voorzitter van de Tweede Kamer*, PG/OGZ-2640352; Den Haag.

Multisignaal (2009) *Signaleren en Samenwerken, Protocol van Toestemming*: Oude-Tonge.

Multisignaal (2010) http://www.multisignaal.nl, geraadpleegd op 2 februari 2010.

Nationale Ombudsman (2009) *De burger in de ketens. Jaarverslag 2008*, Den Haag 2009.

Parton, N. (2006) '"Every child matters": The shift to prevention whilst strengthening protection in children's services in England', *Children and youth services review,* 28: 976-992.

Parton, N. (2008) 'The 'Change for Children' Programme in England: Towards the 'Preventive-surveillance state'', *Journal of Law and Society* 35, 1: 166-187.

Parton, N. (2009) 'Challenges to practice and knowledge in child welfare social work: From the 'social' to the 'informational'? *Children and youth services review*, 31: 715-721.

Peckover, S., S. White & C. Hall (2008) Making and managing electronic children: E-assessment in child welfare, *Information, communication and society*, 11, 3: 275-294.

Politie Gelderland-Midden (2008) *persbericht*, 7 februari: Arnhem.
Prins, J.E.J. & M. de Vries (2003) *ID or not to be? Naar een doordacht stelsel voor digitale identificatie*, Den Haag: Rathenau Instituut.
Prins, J.E.J. (2007) 'Technocratie en de toekomstagenda van de Nationale Ombudsman', blz. 111-134 in: *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context* (jubileumbundel 25 jaar Nationale Ombudsman), Den Haag: Boom Juridische uitgevers.
Prins, J.E.J. (2008) Heeft Digitale Jeugdzorg De Toekomst? blz. 23-50 in M. van den Berg et al. (red.) *In De Greep Van De Technologie*, Amsterdam: Van Gennep.
Prins, J.E.J. (2009) 'Discriminatie signalen', *Nederlands Juristenblad* 85, 2: 59, http://njblog.nl/2010/01/11/discriminatiesignalen/#more-799.
Prins, Ruth & Hans Boutellier (2010) 'De lokale voorzorgcultuur. Over de steeds verder naar voren werkende overheid in de aanpak van sociale veiligheid', *Tijdschrift voor Veiligheid* 9, 2: 3-17.
Raad van State (2006) *Jaarverslag*, Den Haag.
Radboud Universiteit (2008) *Prokid: een onderzoek naar de betrouwbaarheid en predictieve validiteit van de methodiek Prokid,* Nijmegen.
Rapportage SISA-signaleringssysteem 3de kwartaal 2009, *memo aan de Wethouder Jeugd, Gezin en Sport*, gedateerd op 27 oktober 2009: http://www.sisa.rotterdam.nl/download.php?itemID=15921, geraadpleegd op 18 januari 2009.
Rapportage SISA-signaleringssysteem 2e kwartaal 2010, *memo aan de Wethouder Jeugd, Gezin en Sport*, gedateerd op 28 juli 2010: http://www.sisa.rotterdam.nl/ download.php?itemID=21950, geraadpleegd op 15 december 2010.
Risicoprofiel SISA voor jeugdwerk en peuterspeelzalen (2010), http://www.sisa.rotterdam.nl/download.php?itemID=15930, geraadpleegd op 14 januari 2010.
RMO & RVZ (2009) *Investeren rondom kinderen*, Den Haag.
Schinkel, W. (2009) 'De nieuwe preventie. Actuariële archiefsystemen en de nieuwe technologie van veiligheid', *Krisis. Tijdschrift voor actuele filosofie* 2: 1-21.
SISA (2009) 'Samenwerking over de ketens heen', *brochure mei*, 5.
Teeuw, W. B. & A. H. Vedder (red.) (2008) *Security Applications for Converging Technologies. Impact on the constitutional state and the legal order*, WODC, reeks Onderzoek en Beleid, nr. 269.
Tijdelijke Adviescommissie Modernisering GBA (2001) *GBA in de toekomst. Gemeentelijke Basisadministratie Persoonsgegevens als spil voor toekomstige identiteits-infrastructuur*, maart.
Torpey, J. (2000) *The invention of the passport; surveillance, citizenship and the state,* Cambridge: Cambridge University Press.
Tregeagle, S. & M. Darcy (2007) 'Child Welfare and Information and Communication Technology: Today's Challenge', *British Journal of Social Work* 38, 8: 1481-1498.
Tweede Kamer (2008/09) 31 855, *Wijziging van de Wet op de jeugdzorg in verband met de introductie van een verwijsindex om vroegtijdige en onderling afgestemde verlening van hulp, zorg of bijsturing ten behoeve van jeugdigen die bepaalde risico's lopen te bevorderen (verwijsindex risico's jeugdigen)*: Den Haag.

Verwijsindex (2010), http://www.verwijsindex.nl/privacy_privacywegwijzer/, geraadpleegd op 2 februari 2010.

VNG (2008) *Brief Vereniging van Nederlandse Gemeenten met een reactie op de conceptwetgeving Verwijsindex*, Den Haag, Nederlandse Vereniging van Gemeenten, 12 maart 2008.

Voermans, W. & P. Eijlander (2002) *Onderzoek kwaliteit van ministeriele regelingen*, Den Haag.

Volkskrant, de (2008) 'Je moet je kop niet gek laten maken', interview met minister Rouvoet, 1 oktober.

Weerd, M. de & P.J. Krooneman (2004) *Opvoed-, opgroei- en gezinsondersteuning in gemeenten. Eindrapport*, Amsterdam: Regioplan.

Wethouders Jeugd van Amsterdam, Utrecht, Rotterdam & Den Haag (2007) *Brief aan de minister van Jeugd en Gezin over het Elektronisch Kinddossier*.

Wetenschappelijk Instituut voor het CDA (2005) *De Gordiaanse jeugdknoop. Jeugdbeleid met meer gezin en meer gezag*, Den Haag.

White, S., C. Hall & S. Peckover (2009) 'The descriptive tyranny of the common assessment framework: Technologies of categorization and professional practice in child welfare', *British Journal of Social Work* 39: 1197-1217.

Zedner, L. (2007) 'Pre-crime and post-criminology', *Theoretical Criminology* 11, 2: 261-281.

9 DE DIGITALE PATIËNT CENTRAAL – MEDISCHE INFORMATIE IN EEN DIGITALE WERELD

Anne-Greet Keizer

"Het uiteindelijke doel is een EPD dat in staat is om alle gegevens van een patiënt van wieg tot graf te bevatten en toegankelijk te maken, zodat 24 uur per dag de juiste gegevens van de patiënt op het juiste moment beschikbaar zijn voor de zorgverleners en voor de patiënt zelf."

(Minister van VWS, Tweede Kamer 2004-2005: 12)

9.1 INLEIDING

De geschiedenis van de gezondheidszorg laat grote stappen voorwaarts zien door de inzet van technologie, zoals de achttiende-eeuwse uitvinding van de thermometer of het hedendaagse in kaart brengen van het menselijke genoom. Gezondheidszorg is een domein waarbij het nut en de noodzaak van technologische vernieuwing met het oog op het belang van goede gezondheid en zorgen over de betaalbaarheid van de zorg, breed gedragen worden. De doelen lijken onomstreden: betere zorg voor minder geld; maar in de praktijk gaat het om lastige politieke en ethische afwegingen, waarvoor veelbelovende technologische vernieuwingen een verlichting kunnen bieden. In de afgelopen decennia wordt deze verlichting veelal gezocht door de inzet van ICT, voortkomend uit de centrale positie die informatie in dit domein inneemt: "The health sector is arguably one of the most information-dependent businesses of all" (HLCH 2003: 2). Deze informatieafhankelijkheid betreft niet alleen patiëntendata als temperatuur en bloeddruk, maar ook informatie voor patiënten, informatie voor wetenschappelijk onderzoek en informatie ter ondersteuning van managementprocessen.

In de laatste decennia zijn er ook belangrijke beleidsmatige veranderingen te signaleren die verbonden zijn met nieuwe mogelijkheden rond informatie en technologie. Allereerst is het beleid gericht op een omwenteling van aanbodgerichte naar vraaggerichte zorg. Het heersende adagium is: de patiënt hoort centraal te staan in het zorgproces. Dit adagium komt in verschillende verschijningsvormen terug in beleid, zoals de introductie van marktwerking, zorg-op-maat, of persoon(s)gebonden budgetten (Vorstenbosch 2009; Rathenau Instituut 2005). Ten tweede groeit het besef dat vergrijzing van de samenleving het karakter van de vraag naar zorg en de kosten zal doen toenemen en tegelijk het arbeidsaanbod van zorgverleners zal doen verkleinen (Vorstenbosch 2009). Technologische innovatie wordt gepresenteerd als een belangrijk instrument om het hoofd te bieden aan de vergrijzing en tegelijk het ideaal te realiseren van zorg waarbij de patiënt centraal staat. Een voorbeeld van een dergelijke innovatie is het Elektronisch Patiëntendos-

sier (EPD). Artsen werken al sinds de jaren zeventig aan de ontwikkeling van EPD's (Knottnerus 1999), maar vanaf midden jaren negentig is de Nederlandse overheid steeds actiever beleid gaan voeren om deze technologische innovatie voor alle burgers te realiseren, in de vorm van een landelijk Elektronisch Patiëntendossier (L-EPD).[1] Het openingscitaat weerspiegelt de ambitie om de patiënt van de wieg tot het graf en te allen tijde centraal te kunnen stellen, en tegelijk zou het L-EPD verbetering brengen ten aanzien van kwaliteit, effectiviteit en efficiëntie van de zorg (vergelijk Pluut 2010: 29).

De keuze van de term 'dossier' is enigszins misleidend, want het L-EPD behelst niet zozeer het invoeren van gegevens uit papieren patiëntendossiers in een computer of centrale database, maar omvat het opzetten van een infrastructuur waarbinnen zorgprofessionals via een schakelpunt digitale informatie kunnen uitwisselen over patiënten.[2] Binnen deze infrastructuur zullen straks ook nieuwe bronnen van informatie worden gecreëerd, zoals een speciaal diabetesdossier, en specifieke waarborgen worden toegevoegd, zoals geautomatiseerde waarschuwingen bij verkeerde combinaties van medicijnen. De invoering van het L-EPD brengt dus verschillende veranderingen mee in het gezondheidszorgdomein. Ten eerste heeft een elektronisch dossier een ander karakter, een andere wijze van gebruik en andere functionaliteiten dan zijn papieren voorloper. Ten tweede werken het andere karakter en de andere functionaliteiten door op de context van dit dossier, zoals de organisatie van de medische sector en de relatie tussen arts en patiënt.

De ontwikkeling en invoering van het L-EPD past in een bredere trend van het inzetten van informatie- en communicatietechnologieën, die mogelijk is dankzij digitalisering van (medische) informatie: electronic Health (eHealth). Medische informatie omvat in dit kader veel meer dan de gegevens over een patiënt in zijn dossier; het gaat ook om medische informatie gericht op preventie, geaggregeerde en geanonimiseerde data voor onderzoek en informatie over zorgprocessen ten behoeve van bedrijfsvoering van ziekenhuizen. Ook voor deze typen informatie brengt digitalisering een nieuwe dynamiek van kansen en risico's met zich mee. Zo kunnen burgers zichzelf sneller en goedkoper informeren via internet over de Mexicaanse griep en daarmee voorkomen dat ze patiënt worden. Maar er ontstaan ook nieuwe risico's, omdat het toezicht op de kwaliteit van deze informatie moeilijker te reguleren en waarborgen is.

Centraal in deze studie staat de vraag wat digitalisering van medische informatie, en de nieuwe mogelijkheden die deze met zich meebrengt, betekent voor de bestaande relaties in dit domein. In hoeverre verandert het gebruik van een computer-gebaseerd systeem zoals het L-EPD daadwerkelijk (delen van) de sociale orde? Computersystemen worden niet alleen geproduceerd of verspreid, maar ook geconsumeerd (Kling 1991). Systemen worden ontwikkeld en gebruikt in een bepaalde sociale context, in een geschiedenis van sociale arrangementen. Hoe

verhouden overheid en burger, maar ook de intermediërende actoren zoals de arts en zorginstelling, zich tot elkaar in dit domein waar in hoog tempo informatie wordt gedigitaliseerd en 'verrijkt' met nieuwe functionaliteiten?

De termen 'overheid' en 'burger' zijn hierbij niet meer dan constructen die het mogelijk maken te redeneren over burgers of overheden in verhouding tot elkaar en andere actoren. De overheid valt uiteen in een scala aan overheidsonderdelen, lopend van minister en parlement tot aan de Inspectie voor de Gezondheidszorg (IGZ) en het College bescherming persoonsgegevens (CBP). Daarnaast maakt het verschil of we spreken over burgers, patiënten, potentiële patiënten, ex-patiënten, zorgconsumenten of verzekerden. Deze verschillende rollen gaan gepaard met hun eigen gedrag, belangen en verwachtingen (vergelijk Dijstelbloem et al. 2004).[3] Verder bestaat het domein gezondheidszorg uit een dicht landschap van organisaties en individuen die met verschillende belangen en doelen en in onderlinge afhankelijkheden zich 'bemoeien' met die gezondheidszorg.[4] In het vervolg zullen de verschillende actoren en instituties waar relevant expliciet benoemd worden, waarbij aangetekend kan worden dat deze groepen in hun onderlinge relaties niet altijd eenduidig zijn te onderscheiden. De burger verwacht goede en betaalbare gezondheidszorg en kijkt hiervoor in algemene zin naar de (rijks)overheid, in haar hoedanigheid als eindverantwoordelijke voor een goed functionerend zorgsysteem. Maar in individuele zin is de patiënt gericht op een goede diagnose en behandeling door zijn eigen arts, binnen een relatie waarin communicatie en vertrouwen tussen beide partijen centraal staat. De arts, de zorginstelling, en meer indirect ook de verzekeraar, kunnen gezien worden als intermediair tussen de overheid en de burger; een 'instrument' om goede gezondheidszorg in algemene zin te bereiken. Tegelijk hebben ook de intermediaire partijen in de relatie overheid-burger hun eigen belangen, ten opzichte van zowel de overheid als de burger.

Voordat we toekomen aan de vraag hoe ontwikkelingen als het L-EPD (paragraaf 9.4) en eHealth (paragraaf 9.5) van invloed zijn op de onderlinge relaties in dit domein, komt eerst het karakter van medische informatie aan de orde in paragraaf 9.2, gevolgd door de ontwikkeling van het medisch dossier in paragraaf 9.3. In paragraaf 9.6 staat centraal welke betekenis deze ontwikkelingen hebben op beginselen die tezamen de relaties in dit domein vormgeven.

9.2 MEDISCHE INFORMATIE[5]

In reactie op de brief van de minister van VWS van november 2008 hebben 425.568 burgers bezwaar gemaakt tegen opname van hun dossier in het L-EPD.[6] Dit relatief grote aantal bezwaren laat zien dat de veelgehoorde redenatie 'als je niets hebt te verbergen, dan hoef je je ook geen zorgen te maken' voor veel burgers niet opgaat bij medische informatie. Uit een enquête die de WRR in samenwerking met ECP-EPN en Centerdata heeft gehouden, blijkt dat burgers in hoge mate (74%) voor-

stander zijn van de idee dat zorgverleners zoveel mogelijk gegevens bijhouden in een EPD. Tegelijk vindt 83 procent het van belang deze gegevens ook zelf te kunnen inzien en wil 75 procent bezwaar kunnen aantekenen tegen de opgenomen gegevens (Attema & De Nood 2010). De grote betrokkenheid van burgers die hieruit blijkt, hangt samen met het karakter van medische informatie.

9.2.1 MEDISCHE INFORMATIE OVER DE PATIËNT

Patiëntgegevens kennen bijzondere karakteristieken. Ten eerste zijn ze veelal niet stabiel, maar dynamisch van aard. Bij waarden zoals bloeddruk, bloedsuiker en temperatuur is het juist de verandering van de waarde (de temporele dimensie) die van belang is voor het zorgproces. Ten tweede maken de gegevens onderdeel uit van een zorgproces met een contingent karakter: er is weliswaar sprake van een behandelingsplan, maar het patiëntentraject is een zaak van constant monitoren en aanpassen. Ten derde zijn medische gegevens verbonden met de context waarin zij ontstaan (Rathenau Instituut 1998):

- De gegevens worden geproduceerd voor een bepaald praktisch doel. De hardheid en specificiteit van de gegevens wordt op dat doel afgestemd.
- Gegevens kunnen in combinatie met andere gegevens betekenis krijgen. Informatie of kennis ontstaat omdat geïsoleerde waarden samengevoegd kunnen duiden op een bepaalde afwijking. De arts werkt met een 'verhaal' waarbinnen bepaalde waarden samen betekenis krijgen.
- De betrouwbaarheid van de gegevens en informatie kan wisselen. Een arts verzamelt informatie vanuit verschillende bronnen zoals de anamnese, labwaarden en eigen waarneming. Gegevens die de patiënt zelf verstrekt zijn van een andere orde dan labwaarden van een bloedonderzoek.

Het dynamische karakter van medische informatie komt ook tot uiting in nieuwe typen van medische informatie die naar verwachting een steeds prominentere rol in de gezondheidszorg gaan innemen, zoals DNA of genetische informatie. In snel tempo wordt met behulp van hoogwaardige technologieën het menselijk DNA in kaart gebracht en, in een nog minder hoog tempo, vervolgens ingezet in het zorgproces. De inzet van deze *high technology* brengt een verschuiving met zich mee van nadruk op ziekte en genezing, naar keuze, verbetering en risico (Sulik 2009).

Dit type informatie biedt niet alleen informatie over het hier en nu, maar ook over de te verwachten toekomst. Het geeft geen feitelijke stand van zaken aan, maar een dispositie: een eigenschap die zich met een bepaalde mate van waarschijnlijkheid in de toekomst *zou kunnen* manifesteren als een stand van zaken (Vorstenbosch 2009). Deze informatie is daarmee niet alleen van belang voor de patiënt en zijn behandeling, maar ook voor de potentiële patiënt en zijn levensstijl. Waar voorheen gezondheidszorg draaide om genezing, richt het zich steeds meer op voorkomen: surveillance van de burger als potentiële patiënt (Sulik 2009).

Een andere karaktereigenschap van medische informatie komt tot uiting in de spelregels die vastgesteld zijn voor de omgang met dit type informatie. Medische gegevens hebben een bijzondere status: het gaat om zeer gevoelige gegevens waarvoor "bij uitstek geldt dat de betrokkene er belang bij heeft dat geen anderen dan bevoegde personen tot de opgeslagen informatie toegang hebben en dat deze niet wordt gebruikt voor andere doeleinden dan waarvoor zij werd verkregen en vastgelegd (…)" (Staatscommissie Koopmans 1976: 85). Naast de algemene bescherming in de Wet bescherming persoonsgegevens (Wbp) is er de Wet op de geneeskundige behandelingsovereenkomst (WGBO), die verplicht dat de zorgaanbieder een dossier inricht waarin de gegevens omtrent de gezondheid van de patiënt en zijn behandeling zijn aangetekend. Het uitgangspunt van beide bepalingen is dat, zonder toestemming van de patiënt, een zorgaanbieder aan anderen geen informatie geeft over zijn patiënt. Daarbij zijn ook de omstandigheden waaronder deze gegevens worden verzameld bepalend: de gegevens komen voort uit de relatie arts-patiënt en worden daarmee beschermd door de regels van het medisch beroepsgeheim. Dit medisch beroepsgeheim begrenst de mogelijkheden om deze gegevens door te geven aan derden.[7]

9.2.2 MEDISCHE INFORMATIE VOOR DE PATIËNT EN DE ZORGCONSUMENT

De digitaliseringstrend betekent veel voor algemene medische informatie voor 'nog gezonde burgers' of patiënten, en wordt zowel met enthousiasme als met scepsis ontvangen (vergelijk Adams et al. 2006 en 2009; Mager 2009). Voorstanders benadrukken dat het kan bijdragen aan versterking van de positie van de patiënt, terwijl sceptici wijzen op het gevaar van het blootstaan aan fraude en kwakzalverij. Medische informatie is dankzij de internettechnologie niet langer gebonden aan medische instituties, maar 'ontsnapt' naar de bredere samenleving via de (sociale) media (Mager 2009: 2). Internet biedt de zorgconsument informatie die toegankelijk, persoonlijk, en laagdrempelig kan zijn en daarmee een bron van kennis en expertise, maar tegelijk ook een vluchtmogelijkheid. Het aanbod is zo groot en veelzijdig dat de gebruiker ook alleen die informatie kan selecteren die past bij zijn 'wensen' en verwachtingen (Kivits 2009).

De overheid gebruikt het aanbieden van informatie via websites volop als beleidsinstrument: informatie over gezonde levensstijl (loketgezondleven.nl gemaakt door RIVM), ziektebeelden (kiesBeter.nl), of over de Mexicaanse griep (grieppandemie.nl). Dit instrumentarium past bij de stelselwijzigingen van de afgelopen jaren die een omschakeling van aanbodgerichte naar vraaggerichte zorg moesten realiseren. Het veelvuldig gebruik van de term 'zorgconsument' laat zien hoe het marktwerkingsdiscours zijn intrede heeft gedaan in de gezondheidszorg (Dijstelbloem et al. 2004). Zorgconsumenten hebben elk jaar de mogelijkheid te wisselen van zorgverzekeraar, en verzekeraars hebben keuze in het afnemen van zorg tussen verschillende zorginstellingen. Voor dit beleid, dat draait om keuzevrijheid

van de zorgconsument, is beschikbaarheid van relevante informatie een voorwaarde. Om aan deze voorwaarde te voldoen heeft de overheid voorzien in verschillende websites, waarbij aangetekend dient te worden dat het sterk de vraag is of de beschikbaarheid van informatie wel resulteert in rationeel keuzegedrag (Tiemeijer et al. 2009; Hurenkamp & Kremer 2005).

Box 9.1 Websites met medische informatie

De zorgportal kiesBeter.nl is een openbaar portal bedoeld voor alle volwassen inwoners van Nederland die vragen hebben op het gebied van zorg, zorgverzekering en gezondheid. De informatie van kiesBeter.nl is betrouwbaar en kan helpen bij het maken van keuzes op dit gebied, (bron: kiesBeter.nl geraadpleegd op 28-11-2009).
Deze website wordt gemaakt door het Centrum voor Volksgezondheid Toekomst Verkenningen van het RIVM; de opdrachtgever en enige financier is het ministerie van VWS.

De website regelhulp.nl geeft een overzicht van zorg, hulp en financiële steun. De zorgconsument kan online voorzieningen aanvragen of contact leggen met de juiste organisatie (bron: regelhulp.nl, geraadpleegd op 28-11-2009).
Deze website is een initiatief van het ministerie van VWS, SZW, UWV, UWV Werkbeding, CIZ.

Via de website Ribiz.nl (Registratie en informatie beroepsbeoefenaren in de zorg) kan iedereen nagaan welke zorgverleners geschorst zijn of uit hun beroep zijn gezet na een uitspraak van de tuchtrechter (bron: kiesBeter.nl, geraadpleegd op 28-11-2009).

Het is voor de burger bovendien lastig te beoordelen welke informatie uit het aanbod te volgen. Zo heeft zorgverzekeraar CZ begin oktober 2010 via de rechter afgedwongen een lijst te mogen publiceren van ziekenhuizen waarvan ze geen specialistische borstkankerzorg willen inkopen. De Samenwerkende Algemene Ziekenhuizen (SAZ) spanden (tevergeefs) een kort geding aan tegen deze publicatie met het argument dat het kwaliteitsoordeel van CZ vooral is gebaseerd op het aantal operaties in een ziekenhuis, terwijl wetenschappelijke onderbouwing voor minimum aantal operaties ontbreekt (*NRC Handelsblad*, 30-09-2010). De vereniging van borstkankerspecialisten heeft in een reactie op de lijst van CZ aangekondigd in 2011 te komen met een eigen lijst, omdat de vele ranglijsten die in omloop zijn telkens weer anders zijn en gebaseerd zijn op indicatoren die niet echt kwaliteit meten (*de Volkskrant*, 08-10-2010). Het aanbieden van gegevens alleen is dus niet genoeg om ook daadwerkelijk de voor het keuzeproces noodzakelijke kennis en transparantie te realiseren.

9.2.3 INFORMATIE VOOR WETENSCHAPPELIJK MEDISCH ONDERZOEK

Medische gegevens zijn niet alleen van belang voor het individuele zorgproces, maar ook voor medisch-wetenschappelijk onderzoek. Dit type onderzoek is in de twintigste eeuw geprofessionaliseerd en op grotere schaal uitgevoerd, mede dankzij de groeiende mogelijkheid om databestanden uit te wisselen, ook internationaal.[8] Toenemende capaciteit voor opslag, uitwisseling en verwerking biedt ruimte voor een groeiende informatiebehoefte die de laatste decennia is verbonden met standaardisatie van werkprocessen en de nadruk op *evidence-based medicine* (EBM) (Timmermans & Berg 2003). De term EBM wordt verschillend gebruikt, maar verwijst meestal naar het gebruik van klinische richtlijnen gebaseerd op eerdere klinische resultaten ten behoeve van het verspreiden van diagnostische en therapeutische kennis, en past in een langere traditie van het zoeken naar uniformiteit en kwaliteitscontrole door het stroomlijnen van processen. EBM is, net als op andere beleidsterreinen, binnen de gezondheidszorg niet onomstreden (Sackett et al. 1996). Voorstanders zien het als een paradigmawisseling en zelfs een nieuwe sociale beweging, terwijl critici nadruk leggen op het fanatisme en het gebrek aan theorie. Waar de voorstanders geloven in de overtuigingskracht van een kosten-batenanalyse en wijzen op de belofte van transparantie, accountability, effectiviteit en efficiëntie, waarschuwen critici dat EBM de geneeskunde reduceert tot een "kookboek-professie" (Timmermans & Berg 2003: 156).

Standaardisatie heeft onder andere betrekking op onderzoeksprotocollen, inzet van medische technologie en behandelingstrajecten. Het wordt vaak neergezet als een 'technische kwestie', maar beïnvloedt de inhoud en structuur van de medische wereld en de verbonden professies (Rathenau Instituut 1998). "Standards are inherently political because their construction and application transform the practices in which they become embedded. They change positions of actors: altering relations of accountability, emphasizing or deemphasizing preexisting hierarchies, changing expectations of patients"(Timmermans & Berg 2003: 22). Standaardisatie is zeker op twee manieren een politieke onderneming. Ten eerste omdat de uitkomst (de standaard) het product is van een voortdurende onderhandeling tussen verschillende actoren waarbij geen van allen beschikt over totaaloverzicht of controle. Ten tweede omdat standaardisatie onvermijdelijk de praktijk herordent, en daarmee de positie van actoren beïnvloedt (Timmermans & Berg 2003).

Ook ten aanzien van het gebruik van medische informatie voor wetenschappelijk onderzoek kent het domein gezondheidszorg een stelsel van regels en waarborgen. De Wbp, de WGBO en de Wet medisch-wetenschappelijk onderzoek met mensen (WMO) bieden een kader van regels dat verschillende aspecten rondom het gebruik van gegevens omvat.[9] Ploem (2004) constateert geen wezenlijke verande-

ring in de uitkomsten van de afweging tussen het onderzoeks- en privacybelang over de afgelopen decennia, hoogstens een kleine versterking van de positie van het wetenschappelijk onderzoek. Het voornemen van het kabinet om een wetsvoorstel in te dienen dat de bewaartermijnen moet verlengen onderstreept deze trend (Medisch Contact 2010). Bij wetenschappelijk onderzoek speelt naast het individuele privacybelang ook het privacybelang van een groep of categorie. Juist bij groepsprivacy zijn de technologische ontwikkelingen met betrekking tot het samenbrengen van data, het koppelen van bestanden en nieuwe privacybeschermende beveiligingstechnieken relevant. Een probleem bij een dergelijke afweging tussen belangen is dat ze niet definitief gemaakt kunnen worden, omdat technieken zich ontwikkelen en databestanden worden veranderd en/of aangevuld.

De belangen van de individuele patiënt worden gewaarborgd met het instrument *informed consent* (Corrigan 2003). Dit instrument omvat nadrukkelijke toestemming van de patiënt gebaseerd op uitleg en begrip van het doel van de handeling, die kan uiteenlopen van behandeling tot het verzamelen van medische informatie, of lichaamsmateriaal. Wbp, WGBO en WMO bevatten verplichtingen om voorafgaand aan het verzamelen van gegevens toestemming van de betrokkene (patiënt) te verkrijgen.[10] Informed consent kan conditioneel, verbonden aan bepaalde voorwaarden, of onconditioneel, onafhankelijk van het verdere gebruik van de informatie, zijn. Conditionele toestemming is in de praktijk niet eenvoudig toe te passen vanwege de omvang van de organisatorische schaal, de veelal lange tijdsspanne, de betrokkenheid van diverse partijen, en het potentieel gebruik van de data voor een grote hoeveelheid van onderzoeksprojecten (Petersen 2005).

Informed consent is te beschouwen als de opbouw en vastlegging van een vertrouwensrelatie tussen arts/onderzoeker en patiënt. De onderliggende redenatie achter dit model is dat de rechten en het belang van het (autonome) individu beschermd zijn door de mogelijkheid een vrije en geïnformeerde keuze te kunnen maken. Hierdoor werkt het als een tegenmacht tegen het medisch paternalisme, en daarmee als instrument in een dichotoom voorgestelde relatie tussen arts en patiënt (Corrigan 2003). In de praktijk blijft het ook binnen het model de vraag hoe ver de plicht van de arts tot informatieverstrekking reikt. En in hoeverre is er sprake van een echte vrije keuze wanneer de patiënt in een onzekere en afhankelijke positie verkeert? De kwetsbaarheid van de regeling is bijvoorbeeld aan de orde bij eenmalige uitdrukkelijke toestemming voor gebruik van gegevens in wetenschappelijk onderzoek, omdat na die toestemming niets verder gebruik van die gegevens in de weg staat (vergelijk WGBO art. 7: 457 BW). Dat legt druk op de procedure van het verkrijgen van toestemming. Ten eerste moet alle relevante informatie van tevoren zijn verstrekt, maar het is niet altijd duidelijk welke informatie dat betreft. Ten tweede moet de informatie voldoende specifiek zijn, maar bij grote algemene onderzoeksregistraties (bijvoorbeeld voor bevolkingsonderzoek) is vooraf nog niet altijd duidelijk voor welke specifieke onderzoeksprojecten

de informatie waardevol kan zijn. Ten derde kan de plicht tot het verstrekken van informatie en vragen van toestemming bijten met het belang van de behandeling (bijvoorbeeld bij psychiatrische patiënten). En tot slot is in de praktijk het recht op intrekking van toestemming lastig, zeker wanneer gegevens voor het onderzoek worden bewerkt tot niet (direct) herleidbare gegevens. Voorwaarden met betrekking tot opslag, gebruik, verwerking, bewaring en publicatie zijn niet altijd zo vanzelfsprekend en eenduidig, zeker nu de mogelijkheden voor koppelen en bewerken tot nieuwe data zo zijn toegenomen en nog steeds toenemen. Projecten als Parelsnoer en Mondriaan laten zien hoe realistisch en actueel deze trend is (zie box 9.2).

Box 9.2 Projecten voor koppeling van databases

Het Parelsnoer-initiatief is een in 2007 opgericht samenwerkingsverband tussen de acht universitaire medische centra's (UMC's). Binnen dit samenwerkingsverband worden gegevens verzameld over het ziektebeloop en lichaamsmaterialen van patiënten, met als doel hier op een later moment wetenschappelijk onderzoek (op) te kunnen doen. In eerste instantie omvat het project acht ziektebeelden (parels): cerebro vasculair accident (beroerte), diabetes mellitus, erfelijke darmkanker, inflammatoire darmziekten, leukemie, neurogeneratieve ziekten (o.a. Alzheimer), nierfalen en reumatoide artritis/artrose. De uitgesproken verwachting is dat later, op het moment dat de infrastructuur (het 'parelsnoer') werkt, andere ziektebeelden toegevoegd zullen worden (bron: factsheet geraadpleegd op 18-01-2010; www.parelsnoer.org).

De ambitie van het Mondriaan-project is om het volgende tot stand te brengen: "A grid to integrate and to enrich existing and new health data platforms in order to fuel pharmaceutical research in The Netherlands and to play an internationally competitive role in drug intelligence and innovation" (www.tipharma.com, geraadpleegd op 18-01-2010). Om deze doelstelling te bereiken, wordt onder andere gewerkt aan het koppelen van bestaande Nederlandse databases in een gezamenlijk framework. Het project wordt gedragen door een samenwerking van publieke en private partners: GlaxoSmithKline, Sanofi Aventis, UMC Utrecht, UMC Groningen, Universiteit Groningen en Universiteit Utrecht. Het Mondriaan-project werkt samen met het Parelsnoer-initiatief.

9.2.4 INFORMATIE VOOR ZORG- EN MANAGEMENTPROCESSEN

Informatie is ook in bestuur en management van de zorg een steeds prominentere rol gaan spelen. Passend in de New Public Management (NPM) trend ligt de nadruk op sturing op output en minder op input en processen, gecombineerd met een toenemende aandacht voor het meten van kwantificeerbare resultaten (Bal 2008). Marktwerking en de daarvoor noodzakelijke transparantie hebben deze trend versterkt. Sturing op kostenbeperking en kwaliteitsverbetering vraagt om gedetailleerde, op individuele zorgverleners herleidbare gegevens. In dit kader zijn Diagnose Behandel Combinaties (DBC's) ingevoerd. De bekostigingssystematiek

op basis van DBC's had tot doel een transparante zorgmarkt te creëren, door meer inzicht te bieden in de zorgproductie, en tevens kwaliteitsbeleid en benchmarking te bevorderen (Evers 2008). Een DBC is een administratieve code die de zorgvraag en totale behandeling van een patiënt weergeeft. De DBC wordt op naam en Burgerservicenummer (BSN), en dus niet geanonimiseerd, aan de zorgverzekeraar verstrekt voor declaratie van de verleende zorg. Extra informatie gaat gepseudonimiseerd naar het DBC-informatiesysteem (DIS), een centrale databank. De database dient tot doel de zorgvraag van consumenten en de effectiviteit van de behandelmethoden in kaart te brengen, maar mag door het ministerie van VWS en het CBS ook ongelimiteerd benut worden voor wetenschappelijk onderzoek (Evers 2008).

In ziekenhuizen wordt al gewerkt aan een volgende stap: het project DOT (DBC's op weg naar transparantie) (Warners 2009). DOT moet een beter gestructureerd, eenvoudiger en geüniformeerd systeem worden door het aantal DBC's van 30.000 naar 3.000 terug te brengen. In het nieuwe systeem zijn het niet de medisch specialisten die de DBC's rechtstreeks registreren, maar medisch zorgadministrateurs die de DBC's achteraf afleiden van de geregistreerde basisgegevens (diagnoses, verrichtingen en zorgactiviteiten). Voor het vak van medisch zorgadministrateur betekent dit niet alleen een uitbreiding van taken, maar ook een verandering, omdat zorginhoudelijke kennis veel meer dan voorheen noodzakelijk is (Warners 2009).

Voor artsen, en daarmee hun patiënten, is er geen keuzevrijheid wat betreft de DBC-systematiek: zelfs als de patiënt de rekening zelf wenst te betalen is er voor de arts een verplichting tot registratie van DBC's (Evers 2008). De invoering van de DBC's heeft daarom met name onder psychiaters verzet teweeggebracht, geïllustreerd door de oprichting van de actiegroep De Vrije Psychiater in 2005. De psychiaters stellen dat zij met de vermelding van DBC's hun medisch beroepsgeheim schenden. Bovendien ontbreekt na het verlopen van de bestaande gedragscode in februari 2008, de garantie dat verzekeraars misbruik maken van deze privacygevoelige gegevens (Evers 2008). Het College voor Beroep voor het Bedrijfsleven (CBB) heeft op 2 augustus 2010 uitgesproken dat de Nederlandse Zorgautoriteit (NZa) vrijgevestigde psychiaters en psychotherapeuten voorlopig niet langer kan verplichten informatie over diagnoses te vermelden op hun declaraties.[11] Volgens het CBB heeft de NZa onvoldoende de privacybelangen van de patiënt mee laten wegen en te weinig rekening gehouden met de gerechtvaardigde eis van behandelaars om hun beroepsgeheim te waarborgen.

9.3 HET MEDISCH DOSSIER IN ONTWIKKELING

Het medisch dossier is geen doel op zich, maar ontstaan als een instrument voor de professional bij het uitvoeren van zijn taak: het verlenen van zorg. Het dossier

structureert het werk in de zorg (communicatie en organisatie) en het verzamelt en aggregeert verschillende data over een bepaalde patiënt. Het Nederlands Huisartsen Genootschap (NHG) geeft een overzicht van 'klassieke' functies van het medisch dossier (NHG 2004): geheugen voor de arts; bron van gegevens om door te geven bij consultatie of doorverwijzing naar derden; bron van gegevens bij meningsverschil met de patiënt of aansprakelijkheids- of claimzaak; invulling van een van de wettelijke verplichtingen (WGBO 1995; Wbp 2001).

Aan het begin van de twintigste eeuw stappen ziekenhuizen in de Verenigde Staten over van losse werkaantekeningen van individuele artsen of zorgverleners naar het bij elkaar brengen van noodzakelijke informatie om te kunnen omgaan met de organisatorische complexiteit (Berg 1996). Deze ontwikkeling past in de scientific management-beweging in de organisatiewetenschap, en het centraal stellen van de patiënt was dus niet zozeer geïnspireerd vanuit ideële, maar meer vanuit organisatorische motieven. De institutionalisering van het dossier creëerde de mogelijkheid subjectieve aantekeningen op te waarderen tot een objectieve weergave van de gebeurtenissen (Rathenau Instituut 1998).

Deze nieuwe methode van vastleggen bracht nogal wat veranderingen met zich mee voor betrokken actoren, uiteenlopend van ziekenhuisbestuurders, (private) patiënten en artsen. Waar een individuele arts zijn eigen notitiesysteem kon hanteren, was het nu noodzakelijk de patiëntengegevens op een vaste wijze te registreren en coderen. Er ontstonden ook een nieuwe infrastructuur en nieuwe professies voor het aanmaken en verwerken van de dossiers, zoals stenografen en administratieve medewerkers (*record clerks*). Een onverwacht bijeffect was de juridische functie die deze verbeterde verslaglegging met zich meebracht (Timmermans & Berg 2003). Het centraal stellen van de patiënt bleef in deze opvatting echter wel beperkt tot een passieve benadering van de patiënt. De patiënt staat centraal bij het verzamelen en vastleggen van informatie, maar dat betekent (nog) niet dat de patiënt zelf actief dit proces kan sturen.

9.3.1 NAAR EEN ELEKTRONISCH MEDISCH DOSSIER

De eerste Elektronische Zorgdossiers (EZD's) ontstonden in Nederland in de jaren zeventig in poliklinieken en huisartspraktijken, en waren gericht op bedrijfsvoeringsaspecten als financiële en patiëntenadministratie. In tegenstelling tot in de Verenigde Staten, zijn het in Nederland vooral de huisartsen die in de jaren tachtig flinke stappen zetten in het elektronisch opslaan van gegevens in Huisarts Informatie Systemen (HIS). In de jaren negentig is er een ware explosie van (commerciële) systemen, waardoor tegelijk de complexiteit van het gebruik van (communicerende) EZD's in de praktijk naar voren komt (Rathenau Instituut 1998). Aan de klassieke functies van een medisch dossier worden door digitalisering andere functies toegevoegd (NHG 2004): a) betere waarborg voor de continuïteit van de

zorg, omdat het toegankelijk is vanaf diverse werkplekken; b) ondersteunend voor taakdelegatie; c) instrument bij uitvoeren van gestructureerde zorg- en preventietaken; d) instrument voor de 'lerende' zorgpraktijk (informatie voor jaarverslagen, visitatie e.d.); e) bron van gegevens in het kader van transparantie van de hulpverlening (externe toetsing, interne kwaliteitsverbetering en prestatievergelijking); f) in geanonimiseerde vorm bron voor onderzoeks- en andere projecten; g) gebruik van een elektronisch medisch dossier maakt elektronische consultondersteuning mogelijk.

Van Dalen en Stegwee (2006) onderscheiden vijf ontwikkelingsfases van Elektronische Patiëntendossiers (EPD's) en Persoonlijke Patientendossiers (PPD's) (zie ook Pluut & Zuurmond 2009).[12] In de eerstegeneratiesystemen draait het alleen om een digitale weergave van de gegevens, maar in volgende generaties is er sprake van een ontwikkeling naar geautomatiseerde systemen, een digitaal georganiseerde infrastructuur, elektronische dossiers die via een netwerk kunnen worden uitgewisseld, tot virtuele, multidimensionale dossiers op een gedeelde infrastructuur. Technisch is de laatste fase inmiddels mogelijk (in ieder geval een theoretische mogelijkheid), maar in de praktijk blijft die beperkt tot kleinschalige bètaversies.[13]

Naast de bovengenoemde toevoeging van functies gaan bepaalde kenmerken van een papieren dossier verloren bij omzetting; kenmerken die op zich een belangrijke bron van informatie kunnen vormen (Rathenau Instituut 1998). Zo geeft het handschrift informatie over welke zorgverlener en hoeveel zorgverleners data hebben ingevoerd, geeft de dikte van het dossier in één oogopslag een beeld van de omvang en complexiteit van het patiëntentraject en heeft papier een zekere mate van flexibiliteit door de mogelijkheid een memo toe te voegen, pijltjes te trekken of kleuren te gebruiken. Papieren dossiers zijn praktisch in de zin dat ze makkelijk mee zijn te nemen van de ene naar de andere locatie en er geen extra hulpmiddelen nodig zijn om ze overal en altijd in te zien.

9.3.2 WAT DOET HET ELEKTRONISCH DOSSIER MET ZIJN CONTEXT?

De vorm van het dossier beïnvloedt de structuur van het contact tussen arts en patiënt, de organisatie en coördinatie van taken, de hiërarchie van de professie en de mate van juridisering van medisch handelen (Rathenau Instituut 1998; Berg 1996). Het openingscitaat van deze bijdrage weerspiegelt de manier waarop het streven naar te allen tijde beschikbaarheid van alle relevante informatie impliceert dat alle momentopnamen uit het heden en verleden tezamen een 'beeld' vormen van de patiënt. De informatie is een representatie van die patiënt. Maar het voor een concrete behandeling adequate, eenduidige of complete beeld rijst niet vanzelf op uit een dossier dat bestaat uit een verzameling gegevens en stukken informatie (Vorstenbosch 2009). Het is op basis van professionele interpretatie dat een arts

van een verzameling gegevens komt tot een diagnose. Medische gegevens zijn echter, zoals besproken in paragraaf 9.2, verbonden met de context waarin ze ontstaan. Hoe komt eenheid van interpretatie tot stand bij uitwisseling van gegevens of informatie en samenvoeging van gegevens uit verschillende contexten?

De vertrouwensrelatie tussen arts en patiënt is belangrijk voor de waarde van de informatie die de patiënt aanlevert. Wanneer informatie wordt verzameld binnen de spreekkamer geeft dit de arts meer mogelijkheden te beoordelen in hoeverre de patiënt 'ware' informatie aanlevert (in tegenstelling tot sociaal wenselijke informatie), of in staat is de juistheid en volledigheid van informatie zelf in te schatten. Uitwisselen van informatie met derden zet de vertrouwensrelatie naar beide kanten toe onder druk: de patiënt heeft minder controle op door wie en hoe zijn informatie wordt gebruikt en weergegeven, terwijl de arts minder zicht heeft op de omstandigheden waaronder deze informatie is verzameld. Vanuit de zorgconsument gezien wordt zijn vertrouwensrelatie verbreed van een een-op-eenrelatie met de zorgverlener naar een relatie met een (bureaucratisch) systeem (Vorstenbosch 2009), waarbinnen hij letterlijk wordt gereduceerd tot een nummer: het Burgerservicenummer (BSN). Het systeem biedt de patiënt aan de ene kant (nieuwe) mogelijkheden om de stromen van informatie-uitwisseling te volgen via de loggegevens van het systeem, maar tegelijk maakt de betrokkenheid van diverse actoren het voor de zorgconsument minder overzichtelijk.

De overgang naar het elektronisch medisch dossier en het frequent uitwisselen zal opnieuw veranderingen met zich meebrengen voor de betrokken actoren.[14] De vaste wijze van registreren en coderen moet nu niet alleen binnen een systeem, maar ook tussen verschillende systemen gelijk zijn, om uitwisseling technisch mogelijk te maken. De ontstane plaatselijke infrastructuren zullen gekoppeld moeten worden, en zal wederom de opkomst van nieuwe professies en andere werkverdelingen met zich meebrengen. Door toegenomen transparantie van het zorgproces en de individuele bijdragen zal ook de juridische betekenis van een dossier verder toenemen (zie ook Dekker & Hendriks 2009). De precieze gedaante waarin deze veranderingen vorm zullen krijgen is afhankelijk van de specifieke context en het specifieke systeem. In de volgende paragraaf staat centraal hoe in Nederland deze overgang naar een landelijk Elektronisch Patiëntendossier in gang is gezet en zich heeft ontwikkeld.

9.4 HET LANDELIJK EPD

De discussie rond de invoering van het L-EPD is niet iets van de laatste jaren, maar speelt (alhoewel onder andere benamingen) al decennia.[15] Nadat in de jaren zeventig en tachtig vanuit het veld Ziekenhuis Informatie Systemen (ZIS-systemen) en Huisartsen Informatie Systemen (HIS-systemen) zijn geïntroduceerd, stagneert de verdere ontwikkeling van ICT in de zorg, waaronder EPD-systemen. Waar tot dan

de nadruk lag op de eigen verantwoordelijkheid van het veld, kondigt de toenmalige minister van VWS in 1997, in reactie op een Advies van de (voorlopige) Raad voor de Volksgezondheid, een actieplan ICT in de Zorg aan om, weliswaar in goed overleg met de sector, een actieve rol te spelen "in het signaleren en wegnemen van belemmeringen die de actieve toepassing van Informatie- en Communicatietechnologie (ICT) tegengaan" (Ministerie van VWS 2000: 3).

9.4.1 ONTWIKKELING EN INVOERING

Vanaf 1997 wil het ministerie van VWS een actieve rol op zich nemen, "(M)aar de overheid ziet voor zichzelf geen taak om hiervoor een blauwdruk op te stellen" (Tweede Kamer 1997-1998: 5). In de loop der jaren neemt de sturing vanuit het ministerie echter toe, al dan niet in gedelegeerde vorm, bijvoorbeeld door het speciaal opgerichte Nationaal ICT Instituut in de Zorg (NICTIZ) (Pluut 2010). Toch resulteerde de actievere rol van de overheid niet in een voorspoedige uitrol van het L-EPD. Tijdens het moeizame ontwikkelings- en invoeringstraject komen verscheidene facetten van het L-EPD geregeld terug op de agenda, zoals de keuze voor een landelijk versus regionaal systeem, aansprakelijkheden en de communicatie over het L-EPD.

Landelijk versus regionaal

De keuze tussen een centraal of een decentraal ontwerp zien we vaker terugkomen bij de introductie van grote informatiesystemen (vergelijk Jacobs 2010). In tegenstelling tot bij het Elektronisch Kinddossier hangt de minister van VWS sterk aan zijn keuze voor een landelijk systeem. Omdat dit een controversiële keuze blijft onderstreept hij zijn keuze in het debat over het wetsvoorstel in de Tweede Kamer met drie argumenten.

> "Mensen hebben recht op 100 procent dekking van informatie. De noodzaak van veilige en betrouwbare gegevensuitwisseling is heel groot met een landelijke infrastructuur. Met UZI-pas en BSN wordt een optimaal en hoog beveiligingsniveau geboden. Tot slot is het niet efficiënt als elke regio opnieuw het wiel moet uitvinden en als er tussen regio's geen uitwisseling van informatie plaatsvindt" (Tweede Kamer 2008-2009c: 3935).

De argumenten overtuigen niet alle betrokkenen, zoals blijkt uit het blijvende verzet van verschillende belangengroepen verwoord tijdens de twee expert-meetings over het EPD georganiseerd door de Eerste Kamer (zie ook Dekker & Hendriks 2009).[16] Patiënten hebben in de redenatie van de minister recht op goede informatie-uitwisseling, maar in veel gevallen blijft de patiënt voor zorg binnen een bepaalde regio en zal een regionaal systeem dus aan deze voorwaarde voldoen. In reactie wijst de minister op onderzoek van het CBP waaruit blijkt dat regionale

systemen niet voldoen aan eisen van beveiliging en privacy van patiënten (Eerste Kamer 2009-2010a). Maar in antwoord op een motie van de Eerste Kamer aangenomen op 1 juli 2010, moet de minister toegeven dat veiligheid en betrouwbaarheid ook voor regionale systemen gewaarborgd moeten zijn (Eerste Kamer 2010-2011).

Aansprakelijkheden

De minister concludeert in de memorie van toelichting dat de aansprakelijkheden niet wezenlijk van de bestaande aansprakelijkheidsrisico's in de gezondheidszorg verschillen (Tweede Kamer 2007-2008). Deze uitspraak is gebaseerd op een rapport van de Universiteit van Tilburg, dat concludeert dat: "Met de invoering van het EPD zullen in het algemeen de aansprakelijkheidsrisico's niet wezenlijk veranderen. De risico's bestaan vooral uit incidentele gezondheidsschade door onjuiste of ontbrekende gegevens. Een risico dat bij verwezenlijking gevolgen kan hebben voor meerdere individuen is de mogelijkheid van privacyschade door een lek in (een onderdeel van) het EPD" (Barendrecht et al. 2008: 3). Verderop volgt een aanvulling: "Bij een zorgvuldige werkwijze zijn de aansprakelijkheidsrisico's niet of slechts minimaal groter" (Barendrecht et al. 2008: 20). Het rapport erkent wel dat het optuigen van een landelijk systeem voor informatie-uitwisseling, niet betekent dat informatie niet nog steeds onjuist kan zijn of kan ontbreken.

Het is vooral interessant om te zien hoe in dit onderzoek aansprakelijkheid alleen betrokken wordt op dezelfde handelingen in een nieuw systeem. Wat niet wordt meegenomen en meegewogen is dat er door de invoering van een nieuwe technologie ook (deels) een nieuwe situatie ontstaat. In de nieuwe zorgpraktijk zal sprake zijn van meer handelingen en van meer betrokken actoren (zie ook Meyst-Michels Tiems 2009). Het L-EPD werkt met een strikt persoonljjke UZI-pas die de toegang reguleert tot de medische gegevens, maar er zullen naar schatting meer dan een half miljoen UZI-passen in Nederland in omloop komen en de praktijk laat bovendien zien dat meerdere mensen voor het gemak van één en dezelfde pas gebruikmaken (Jacobs 2010). De doelstelling van de nieuwe systemen is dat informatie accuraat en actueel voor betrokkenen beschikbaar is en met meer mensen wordt gedeeld. Meer informatie en meer communicatie van informatie betekent meer kans op fouten en vergissingen. Wanneer het aantal handelingen dat moet worden verricht voor een actie toeneemt, zijn er ook meer momenten waarop een fout kan worden gemaakt. Een nieuwe eis is dat de informatie bovendien actueel moet zijn; binnen 24 uur moeten gewijzigde gegevens in het EPD staan. Deze tijdsdruk kan fouten uitlokken. Maar het niet halen van de deadline kan ook betekenen dat een andere zorgverlener bij de behandeling van de patiënt onterecht uitgaat van volledige en actuele informatie.

Communicatie

Over de communicatie rond het EPD is het nodige te doen geweest, resulterende in verschillende Kamervragen en moties (Pluut 2010). De commotie rond de brief[17]

van het ministerie van VWS waarin burgers de mogelijkheid kregen bezwaar te maken tegen opname in het landelijk EPD laat volgens Vorstenbosch (2009) zien dat de acceptatie van wat hij noemt 'achtergrondapparaten' vaak te maken heeft met onbekendheid. Het EPD is een systeem dat op zich niet tastbaar is en als het goed functioneert ook niet tastbaar wordt. Het is bovendien een complex systeem, zelfs voor professionals die ermee werken of die betrokken zijn bij het proces van ontwikkeling en invoering (zie Pluut 2010; Rathenau Instituut 2009a). Zo blijft, mede door de gehanteerde benaming, voor veel burgers onduidelijk dat het systeem draait om een landelijk schakelpunt dat communicatie tussen zorgprofessionals moet faciliteren, en niet om een nieuw dossier bewaard op een centrale verzamelplaats. De brief van 2008 getuigt van een verwachting dat het bieden van technische informatie over het systeem en een geruststellende uitleg een goede strategie zijn om met deze onbekendheid om te gaan. Maar als onder de onbekendheid een vertrouwensprobleem speelt, maakt meer informatie soms juist wantrouwiger en sceptischer, zoals recent de commotie over vaccinatie voor de Mexicaanse griep heeft laten zien (Vorstenbosch 2009; Versteeg & Hajer 2010). Hetzelfde patroon is zichtbaar in het focusgroepenonderzoek dat het Rathenau Instituut heeft laten verrichten in voorbereiding op de expertbijeenkomst van de Eerste Kamer (Rathenau Instituut 2009c). Om de gebrekkige communicatie rondom het L-EPD te repareren, heeft de Eerste Kamer op 5 juli 2010 een motie aangenomen die vraagt om een communicatieplan van de regering waarin de stand van zaken rond het L-EPD wordt toegelicht en duidelijkheid gegeven wordt over het vervolgtraject (Eerste Kamer 2009-2010b).

9.4.2 EXTERNE KRACHTEN

De politieke en beleidsmatige discussie over het L-EPD vindt niet plaats in een vacuüm, zoals blijkt uit verwijzingen naar andere nationale of private systemen (Tweede Kamer 2008-2009b, c en d). Hoewel Nederland zich graag presenteert als koploper op het gebied van ICT, is het niet het enige land dat zich bevindt in een ontwikkelings- en invoeringstraject van een EPD-systeem. In Denemarken, Spanje (Andalusië) en het Verenigd Koninkrijk zijn soortgelijke systemen in ontwikkeling. Deze systemen kunnen onderling verschillen op aspecten als: de mate van functionele verfijning (wat kan het systeem?); de mate van technologische verfijning (hoe goed (en veilig) werkt het systeem?); en de mate van integratieniveau (hoe veelomvattend is het systeem) (Protti et al. 2009). De systemen die nu in sommige landen al zijn ingevoerd scoren op alle drie de niveaus nog bescheiden (Pluut & Zuurmond 2009), maar de verschillende plannen en programma's kondigen vele ontwikkelingen aan die de scores op de drie niveaus zullen vergroten. De ambities voor de mate van functionele verfijning en integratie zijn hoog. Veelal zijn de mate van technologische verfijning en de organisatorische complexiteit remmende factoren voor realisatie van deze ambities (Brennan 2005; House of Commons 2009).

In het debat met de Tweede Kamer over het wetsvoorstel verwees de minister nadrukkelijk naar koploper Denemarken, maar zette het Nederlandse beleid en de gemaakte keuzes ook positief af tegen het 'top-down' model van het Verenigd Koninkrijk (Tweede Kamer 2008-2009b en c). Het National Programme for IT (NPfIT) is een omvattend programma (reputed to be the largest non-military IT investment in the World (Brennan 2005)), bestaand uit acht verschillende subprogramma's. De doelstelling van het programma omvat allereerst de digitalisering van medische dossiers, maar geplande vervolgstappen zijn het invoeren van een systeem voor klinische en administratieve ondersteuning (Brennan 2005). Het programma ging van start met diverse ICT-leveranciers, maar in de loop der jaren heeft de ene na de andere aanbieder zich teruggetrokken. De Public Accounts Committee van de House of Commons maakt zich zorgen: "The Programme's high dependence on just two major suppliers has implications for the Programme's capacity and capability, and for the Department's leverage" (House of Commons 2009: 3). Een evaluatie in het voorjaar 2009 van databeveiliging binnen de National Health Service (NHS) levert een lijst van 140 beveiligingslekken op in een periode van vier maanden. Na deze evaluatie is besloten toch toe te staan dat NHS-patiënten het recht hebben elektronische samenvattingen van hun behandelingsdossiers te laten verwijderen uit de nationale medische database.[18] De nieuwe coalitieregering van conservatieven en liberalen concludeerde slechts enkele maanden na aantreden in mei 2010 op basis van een review van het NPfIT dat "a centralised, national approach is no longer required, and that a more locally-led plural system of procurement should operate, whilst continuing with national applications already procured"(Department of Health 2010).

Ook commerciële partijen bieden al enige tijd alternatieve EPD-systemen aan. Het gaat dan met name om systemen die geschikt zijn voor gebruik binnen één zorginstelling, zoals het systeem Medlook. Meer recent ontstaat er een nieuw aanbod van Personal Patiënt Dossiersystemen van bedrijven als Google en Microsoft. Deze systemen bieden direct veel meer functionaliteiten dan het Nederlandse L-EPD, namelijk een zorgplatform met web 2.0 functionaliteiten en uitgewerkte regiemogelijkheden voor de zorgconsument. Hoewel GoogleHealth en de mogelijkheden die het de patiënt zou bieden om zelf de regie over zijn zorgproces te voeren aan de orde zijn gekomen in debatten in het Nederlandse parlement, is GoogleHealth alleen nog beschikbaar in een bètaversie in de VS. Introductie van deze dienst in Europa lijkt voorlopig nog niet aan de orde.[19]

9.4.3 HET EPD EN DE ROL VAN DE PATIËNT

Vanaf de eerste discussie over een elektronisch patiëntendossier wijzen voorstanders op de voordelen voor de patiënt. Het Rathenau Instituut constateert echter in 1998 dat de patiënt nauwelijks een stem heeft in de vormgeving van elektronische zorgdossiers in Nederland. Ook patiëntenverenigingen voeren weinig gericht

beleid op deze kwesties. In de loop der jaren, als het ontwerp van EPD en elektronisch medicatie dossier (EMD) steeds meer vorm begint te krijgen, brengt de politiek de positie van de patiënt expliciet naar voren in het debat. Tijdens een debat in maart 2005 spreken Kamerleden van VVD, CDA, GroenLinks, en LPF in verschillende bewoordingen uit dat de patiënt eigenaar/regisseur/sleutelbewaarder moet zijn van zijn dossier/gegevens (Tweede Kamer 2004-2005). De minister antwoordt dat, hoewel er geen juridisch eigendom bestaat van een patiëntdossier voor de patiënt, "de gegevens eigendom zijn van de patiënt. Hij is ook de enige die kan bepalen wie er inzage krijgt in zijn dossiers. Hij moet toestemming geven aan artsen om bijvoorbeeld zijn centrale medicatiedossier van de apotheker in te zien. De patiënt zal op een gegeven moment duidelijk moeten maken binnen welke kring zijn elektronisch dossier gebruikt mag worden"(Ibid.: 10). In de memorie van toelichting staat dat zeggenschap van de patiënt een belangrijke randvoorwaarde is en de minister gaat expliciet in op de rechten van de patiënt: "de patiënt zelf gaat [uiteindelijk] over zijn deelname aan het EPD. Indien de patiënt dat wenst, wordt er geen EPD gemaakt of worden bepaalde gegevens niet in het EPD opgenomen. Het onvermeld laten van bepaalde gegevens kan de betrouwbaarheid van het EPD verlagen" (Tweede Kamer 2007-2008: 7). Verderop: "Als de patiënt dat wenst, kan hij bepaalde patiëntgegevens uit het EPD laten houden en bepaalde zorgaanbieders of categorieën van zorgaanbieders de toegang blokkeren voor het opvragen van het EPD of het opnemen van indexgegevens in de landelijke verwijsindex" (Ibid.: 10).

De patiënt heeft ook recht op verwijdering of wijziging. "De patiënt kan verzoeken bepaalde wijzigingen aan te brengen ten aanzien van gegevens die feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het kan gaan om het verbeteren, aanvullen, verwijderen of afschermen van die gegevens (artikel 36 Wbp). De beheerder en de zorgaanbieder kunnen alleen om goede redenen een dergelijk verzoek weigeren" (Ibid.: 14). Maar hierbij moet aangetekend worden dat de patiënt zich bevindt in een afhankelijke positie: "De beheerder zal noodgedwongen veelal de zorgaanbieder moeten betrekken bij de beoordeling van zo'n verzoek. Het is immers de zorgaanbieder die de indexgegevens bijhoudt en daarbij de vermeende fouten heeft gemaakt" (Ibid.: 14). Voor de contacten met de beheerder om deze rechten uit te kunnen oefenen wordt een landelijk klantenloket ingericht.

In het debat over de wijziging van de wet in 2009 gaan de verschillende actoren nog weer een stapje verder (Tweede Kamer 2008-2009b).[20] Het CDA komt, samen met de PvdA, met een amendement waarmee elektronische inzage en downloaden naar een USB-stick mogelijk gemaakt moet worden (Ibid.: 3774). "De patiënt staat centraal in de zorg. Dat is alleen het geval als hij kan zien welke gegevens van hem zijn opgeslagen en wie de gegevens heeft ingezien. Daarnaast moet hij zijn gegevens zelf kunnen downloaden en opslaan" (Ibid.: 3776). GroenLinks: "Wij zijn

van mening dat een patiënt niet alleen inzage moet hebben in zijn dossier maar dat hij het op deze punten dient te kunnen beheren" (Ibid.: 3781). D66 waarschuwt in dit verband voor een te snelle invoering: "Voer het EPD pas echt in als uit tests is gebleken dat de medische gegevens van patiënten veilig zijn en zij zelf het gebruik van gegevens kunnen controleren. (…) Het gaat erom dat de patiënt zijn dossier kan inzien wanneer hij wil, in zijn huiskamer, vanachter zijn pc, (…) "(Ibid.: 3783). De minister reageert: "Wanneer de verplichting komt dat alle artsen die faciliteit moeten aanbieden, moet het voor patiënten mogelijk zijn om te zien wie er ingelogd heeft in de patiëntengegevens. Dat vind ik inderdaad ook. Het kan nu ook al, maar dan moet het in elk geval ook elektronisch kunnen" (Ibid.: 3925). "Het realiseren van elektronische toegang voor de patiënt is geen voorwaarde voor de inwerkingtreding van het wetsvoorstel. Wel zal de toegang van de patiënt gereed moeten zijn als de verplichting om aan te sluiten voor zorgaanbieders gaat gelden (…)"(Ibid.: 3930). "Het wetsvoorstel geeft de patiënt de mogelijkheid om zijn EPD en de centrale gebruiksregistratie elektronisch op te vragen en raadplegen. Daarnaast kan hij zijn gegevens ook elektronisch afschermen tegen opvragen en raadplegen door een zorgaanbieder of een categorie van zorgaanbieders" (Ibid.: 3948).

In de loop der jaren heeft de minister de invoering van het L-EPD verbonden aan de mogelijkheid voor patiënten tot digitale inzage in uitgewisselde patiëntgegevens en loggegevens over deze uitwisseling via een klantloket. In de voortgangsrapportage van 9 september 2010 schrijft de minister pas op de plaats te moeten maken met de ontwikkeling van dit loket. Een risicoanalyse heeft laten zien dat GSM-kwestbaarheid hoge tot zeer hoge risico's met zich meebrengt voor de huidige ontwikkeling en toekomstige landelijke uitrol van EPD-DigiD[21], de beoogde communicatiewijze tussen patiënt en klantloket. De minister zet daarom invoering van onderdelen van het klantloket die van SMS afhankelijk zijn stil (Tweede Kamer 2010-2011). De minister geeft in deze voortgangsrapportage niet aan welke consequenties het stilzetten van bepaalde onderdelen heeft voor de verdere uitrol van het L-EPD.

9.4.4 VERSCHUIVING IN DE DOELSTELLING VAN HET EPD

De hierboven beschreven aandacht voor de rol van de patiënt markeert een verschuiving in de doelstelling van het EPD. In 1997, aan het begin van het ontwikkelingstraject, spreekt de minister zich in nog zeer algemene bewoordingen uit over het belang van een EPD: "Ik acht de ontwikkeling van een EPD van groot belang vanwege de potentiële bijdrage aan de gezondheidszorg op micro-, meso- en macro-niveau"(Tweede Kamer 1997-1998: 5). In het actieplan dat volgt in 2000 wordt het waarom van het EPD niet systematisch beargumenteerd, maar door de tekst heen vinden we verschillende rechtvaardigingen en doelstellingen, zoals een verwijzing naar de IPZorg-intentieverklaring van september 2000: … omdat het [Elektronisch Patiëntendossier – AGK] een instrument is dat de efficiency en effec-

tiviteit van het zorgproces kan/zal vergroten" (Ministerie van VWS 2000: 11).[22] In de parlementaire debatten komen we in de loop der jaren een scala aan argumenten voor invoering tegen: betere kwaliteit van zorg; voorkomen van ongelukken (medicatiefouten); het zorgproces transparanter, sneller en dus beter maken; een EPD vergroot de toegankelijkheid voor de patiënt en kan daarmee bijdragen aan de versterking van zijn positie; instrument voor verdere protocollering.[23] In de memorie van toelichting wordt het belang van het EPD als volgt weergegeven.

"De voortschrijdende automatisering vergroot de mogelijkheden van de zorgaanbieder om zichzelf en andere zorgaanbieders van de informatie over de patiënt te voorzien die nodig is voor een goede hulpverlening. (…) Uit diverse onderzoeken blijkt dat de kwaliteit van de zorg verhoogd kan worden door de informatievoorziening te verbeteren. Het blijkt dat er in de zorg vermijdbare fouten worden gemaakt als gevolg van gebrekkige gegevensuitwisseling. (…) Verder blijkt uit onderzoek dat de helft van de patiënten klaagt over gebrekkige gegevensuitwisseling tussen zorgaanbieders" (Tweede Kamer 2007-2008: 4, 5).

Bij de behandeling van het wetsvoorstel licht de minister dit verder toe: "Door gebruik te maken van een landelijk EPD verbetert de gegevensuitwisseling in de zorg op een veilige en betrouwbare manier ten opzichte van de huidige situatie" (Tweede Kamer 2008-2009a). De minister verwijst hierbij expliciet naar het HARM-rapport (Van den Bemt 2006), een wetenschappelijk onderzoek dat concludeert dat van de gemiddeld 41.000 geneesmiddel-gerelateerde ziekenhuisopnames per jaar er 19.000 potentieel vermijdbaar zijn. Maar in de debatten, zowel in de Tweede als in de Eerste Kamer, wordt de relevantie van de onderbouwing van deze stelling in twijfel getrokken. De belangrijkste aanbeveling van het rapport is om patiënten die (aanleg voor) een of meerdere risicofactoren vertonen, proactief te benaderen voor extra medicatiebegeleiding. Betere informatie-uitwisseling is volgens de onderzoekers een van de instrumenten om betere begeleiding te realiseren, zonder dat daarbij het Elektronisch Patiëntendossier expliciet aan de orde komt. Kritische ondervraging hierover van Kamerleden van de SP en PVV brengt de minister tot de volgende reactie.

"Ik vind percentages helemaal niet zo relevant. Al kunnen er maar een paar gevallen per dag op de spoedeisende hulp beter worden geholpen, dan is het al goed" (Tweede Kamer 2008-2009c: 3938).

Voor een succesvolle ontwikkeling, invoering en toepassing van het L-EPD is het van belang dat zorgverleners, patiënten en burgers overtuigd zijn van het nut van het L-EPD. Maar de verwarring over het doel van het L-EPD vormt de rode draad door de behandeling van het wetsvoorstel door de Eerste Kamer. Na twee expertbijeenkomsten lijkt de pluriformiteit van verwachtingen en oordelen zowel onder experts als politici alleen maar te zijn gegroeid (Eerste Kamer 2009-2010 c en d).

Ook Pluut (2010) laat zien dat het doel van de toepassing niet altijd helder is voor alle betrokkenen. Bovendien is de doelstelling niet constant gebleken, met als gevolg dat nu functionaliteiten aan het L-EPD worden gehangen (elektronische inzage van de patiënt en zelfs een regisseursfunctie) die niet passen op de oorspronkelijk uitgedachte architectuur. De architectuur is immers nog gebaseerd op de gedachte dat een dossier een instrument is voor de arts om zijn belangrijkste taak (het verlenen van primaire zorg) uit te voeren. Deze verschuiving van een systeem waar de patiënt centraal staat, maar in een passieve rol, naar een systeem waar de patiënt zelf de regie moet kunnen voeren over het zorgproces, op een plaats en tijd die hij zelf kan bepalen, past in het opkomende eHealth-discours.

9.5 eHEALTH

Het domein gezondheidszorg wordt al een aantal decennia gekenmerkt door automatiseringprocessen en programma's als *ICT en zorg*, maar sinds 1999 is er een nieuw 'buzzwoord' in opkomst: eHealth. De term werd in eerste instantie gebruikt door de industrie en marketing, maar is vervolgens ook de academische literatuur binnengedrongen (Eysenbach 2001) en het beleidsdiscours. Zo opent de Europese Commissie haar actieplan uit 2004 met de vaststelling: "eHealth matters" (COM 2004 356 final: 4). Ook het ministerie van VWS denkt na over de betekenis van eHealth voor het beleid, zoals blijkt uit de adviesaanvraag aan de Raad voor de Volksgezondheid uit 2002 (RVZ 2002).

9.5.1 WAT WORDT ER ONDER VERSTAAN?

De invoering van het L-EPD maakt deel uit van de eHealth-trend, maar eHealth omvat veel meer. "eHealth describes the application of information and communications technologies across the whole range of functions that affect the health sector" (COM 2004 356 final: 4). De RVZ hanteert de volgende definitie: "eHealth is het gebruik van nieuwe informatie- en communicatietechnologieën, en met name internettechnologie, om gezondheid en gezondheidszorg te ondersteunen of te verbeteren" (RVZ 2002: 10). Deze brede definitie omvat allerlei ICT-toepassingen in de zorg waarbij verbindingen tussen verschillende actoren worden gelegd, zowel dokter-dokter (D2D), dokter-patiënt (D2P), als patiënt-patiënt (P2P). eHealth is dus een verzamelnaam voor een scala aan toepassingen als telemedicine (toepassingen gericht op het loskoppelen van zorg en tijd en plaats), het aanbieden van medische informatie via internet, en web 2.0-toepassingen.

Naast eHealth wordt ook steeds vaker gesproken over Health 2.0, gebaseerd op de aanduiding Web 2.0, gebruikt voor een nieuwe fase of generatie van internet. De term web 2.0 is afkomstig van Tim O'Reilly, die als belangrijkste aspecten noemt: software als dienst, *mashups* en meerwaarde gecreëerd door gebruikers in interactie met elkaar (Frissen et al. 2008). Centraal bij Health 2.0 staat *empowerment* van

de patiënt: de patiënt staat niet alleen in passieve zin centraal, maar wordt zelf een actieve partij in het vormgeven van het zorgproces.[24] Voorwaarde is dat patiënten beschikken over alle relevante informatie om zelf (rationele) beslissingen te nemen over hun zorg. Het verschil met de traditionele zorg ligt in de toegevoegde waarde voor de patiënt.

Box 9.3 Enkele voorbeelden van eHealth toepassingen

• Genetische (zelf)testen via internet.
Via de website www.23andme.com kan ieder individu een testkit bestellen waarmee genetisch materiaal ingeleverd en uiteindelijk in kaart gebracht kan worden. Naast de testmogelijkheid biedt de website ook platformfuncties aan waarop 'leden' kunnen ontdekken waar genetische verschillen en overeenkomsten liggen met het DNA van andere leden.

• Teleradiologie
Teleradiologie maakt het mogelijk radiologische scans op afstand te lezen en interpreteren. Deze toepassing is met name populair in landen en gebieden met een lage bevolkingsdichtheid zoals Noorwegen. Het maakt het mogelijk gespecialiseerde kennis en technologie voor een bredere doelgroep beschikbaar te stellen.

• Online therapie
Deze vorm van therapie heeft ten opzichte van conventionele therapie voordelen ten aanzien van toegankelijkheid, kostenbesparing en therapieresultaten. Therapeut-patiëntcontacten verplaatsen van de spreekkamer naar e-mail of chatrooms. Maar ook in Second Life, een virtuele wereld op internet, vinden sessies plaats. Ze blijven daar niet beperkt tot het virtuele kantoor, maar kunnen de vorm van rollenspellen aannemen, waarin de nieuw geleerde vaardigheden kunnen worden toegepast, terwijl de therapeut real time feedback kan geven (*New Scientist*, 23 september 2010: 44-45). Naar aanleiding van deze ontwikkelingen pleitte het Trimbos Instituut al in 2007 voor een keurmerk (*de Volkskrant*, 17 oktober 2009).

• Patiëntencommunities op internet: PatientsLikeMe
Deze website is opgericht door drie ingenieurs van MIT die vanuit persoonlijke motivatie een gemeenschap (community) wilden creëren voor patiënten, artsen en organisaties gericht op het inspireren, informeren en empoweren van individuen: www.patientslikeme.com, geraadpleegd op 18 december 2010). De website kent verschillende functionaliteiten: zoeken van medepatiënten, persoonlijke pagina, forum, statistieken over behandelingen en symptomen, onderzoekspagina, privémailbox. Een belangrijk verschil met andere communities is het vergaren en uitwisselen van informatie (zowel kwalitatief als kwantitatief) door patiënten zelf, met als doel meer kennis en inzicht te krijgen in zeldzame aandoeningen. De uitgewisselde data worden niet 'weggegeven' aan onderzoekers, maar direct en zichtbaar met iedereen gedeeld via de website. In een casestudie onderzoek voor het JRC concludeert TNO dat PatientsLikeMe zowel organisatorisch, juridisch als sociaal een substantiële impact heeft (TNO 2009).

De beloftes van eHealth worden door verschillende actoren benadrukt. Zo noemt de Nederlandse Patiënten Consumenten Federatie (NPCF) in 2008 de volgende kansen: betere informatievoorziening (resulterend in verbetering van de kwaliteit van de zorg); doelmatigere zorg (verhoging van de efficiency); focus op de patiënt (vergroting van het zorgaanbod, patiënt empowerment, verbetering arts-patiëntenrelatie, realiseren van vraaggestuurde zorg, vergroting van de mate van zelfregie). Tegenover deze kansen worden enkele kanttekeningen geplaatst (NPCF 2008): eHealth roept vraagstukken (en weerstanden) op ten aanzien van de relatie arts-patiënt, en daarnaast zijn er vragen te stellen ten aanzien van de betrouwbaarheid van de informatie en de voorwaarden voor toegankelijkheid. Het gebruik van eHealth vergt immers bepaalde vaardigheden en middelen.

De eHealth-ontwikkeling wordt niet alleen gepresenteerd als wenselijk, maar ook als noodzakelijk. Het Rathenau Instituut constateerde in 1998 al dat ouderwetse papieren dossiers niet zijn opgewassen tegen de nieuwe taken van de zorgverlening. De noodzaak van de eHealth ontwikkeling wordt onderschreven met verschillende argumenten (NPCF 2008): a) bestuurlijk (bedrijfsvoering): de hoeveelheid en complexiteit van zorginformatie is zo ver toegenomen dat het beheren van het informatieproces een belangrijke taak is geworden van elke zorgorganisatie; b) economisch: het is noodzakelijk betere instrumenten te vinden vanwege (de/een) groeiende vraag naar zorg (vergrijzing) en hoge verwachtingen; c) ethisch: het is een instrument voor de empowerment van de patiënt en het voorkomen van medische fouten.

In een domein waar de beweging is ingezet om de patiënt centraal te stellen in het zorgproces, is empowerment van de patiënt een logische volgende stap. De NCPF omschrijft deze stap als volgt: "(E)en proces om mensen te helpen controle te krijgen over de factoren die invloed hebben op hun leven. Dit omvat zowel de individuele verantwoordelijkheid in de gezondheidszorg en de bredere institutionele, organisatorische of maatschappelijke verantwoordelijkheden waarmee mensen in staat worden gesteld om de verantwoordelijkheid voor hun eigen gezondheid op zich te nemen" (NPCF 2008: 6).

9.5.2 DE OPKOMST VAN eHEALTH IN BELEID

eHealth is weliswaar nog een na te streven ideaal, of volgens sommigen een hype, maar er zijn aanwijzingen dat de idee van eHealth daadwerkelijk verder vorm zal gaan krijgen in beleid en praktijk van de gezondheidszorg, zowel op nationaal als Europees niveau. Hoewel er een trend is in de richting van verdergaand Europees beleid, valt het gezondheidszorgbeleid (nog) binnen de competentie van de nationale overheden.[25] Toch voert de EU beleid ten aanzien van eHealth, met name door actieprogramma's die gericht zijn op het propageren van op Europees niveau geformuleerde beleidsdoelen door middel van rechtstreeks gefinancierde projec-

ten. Het EU-onderzoeksprogramma ondersteunt eHealth al vijftien jaar, en er is al te spreken van een eHealth-industrie (omzet 11 miljard) met de potentie de derde grootste industrie in de zorgsector te worden (na farmacie en medische apparatuur) (COM 2004, 356 final). "eHealth is today's tool for substantial productivity gains, while providing tomorrow's instrument for restructured, citizen-centred health systems and, at the same time, respecting the diversity of Europe's multicultural, multi-lingual health care traditions" (COM 2004, 356 final: 4). Het Europese eHealth-programma wordt verbonden met de eEurope strategie van de EU, gericht op groei en versterking van de kenniseconomie (Lissabon).

Zowel nationaal als internationaal wordt het belang onderkend van internationale overeenstemming over de wijze van communicatie. Nu vindt vastlegging van medische gegevens voor een groot deel nog plaats in normale spreek- of schrijftaal. Er loopt een internationale pilot (waarin NICTIZ en VWS participeren) met een onderzoek naar interoperabiliteit van transnationale eHealth services (Smart Open Services, Open eHealth). Daarnaast zijn er verschillende standaardisatieorganisaties en -initiatieven (ISO, HL7, CEN, IHE). Nederland is lid geworden van International Health Terminology Standards Development Organisation en daardoor mede-eigenaar van SNOMED CT, een terminologiestandaard voor berichtenuitwisseling. Gebruik van SNOMED moet resulteren in meer uniforme interpretatie en is ontworpen om ook grensoverschrijdend te kunnen gebruiken.[26]

9.5.3 MEDISCHE INFORMATIE OP INTERNET

In paragraaf 2 is beschreven hoe overheidsbeleid zich steeds meer richt op het aanbieden van (medische) informatie aan de burger, zorgconsument en/of patiënt. Er is in de afgelopen jaren veel onderzoek gedaan naar het aanbod van online informatie, uiteenvallend in bijdragen die ingaan op de kansen die het biedt voor empowerment, en aan de andere kant bijdragen die de nadruk leggen op de gevaren voor patiënten. Volgens voorstanders zou internet een pluralistische benadering van gezondheidsinformatie bevorderen. De informatie is niet langer beperkt tot de gevestigde medische context, maar informatie op internet stelt de traditionele hiërarchie van kennis ter discussie (Nettleton 2004). Ander onderzoek (Mager 2009; Adams et al. 2006) laat zien hoe in de praktijk dit pluralistische ideaal niet altijd wordt bereikt, onder meer door strategisch gebruik van zoekmachines waarbij sommige aanbieders er in slagen hun webpagina hoog in de ranking van resultaten te krijgen. Sommige stemmen zijn dus luider dan andere. In een poging hun eigen boodschap optimaal te positioneren hanteren websiteproviders een strategie waarin impliciet een specifiek concept van online gezondheid zichtbaar wordt. "They framed their site as coherent information packages with an inner logic to make it attractive for users"(Mager 2009: 11). Ze bieden links aan met websites die ze ondersteunend voor hun eigen aanbod vinden. Maar uit experimenten en interviews met gebruikers, blijkt dat ze aangeboden links veelal als chaotisch, mislei-

dend of tijdrovend beschouwen. Gebruikers kiezen liever voor zoekmachines om structuur te vinden in het enorme aanbod van gezondheidsinformatie (Adams et al. 2006).

Ander onderzoek richt zich op kwaliteit van de aangeboden informatie. Bij veel aangeboden medische informatie ontbreekt het aan accuratesse en compleetheid (Adams et al. 2009). Medische professionals en beleidsmakers pleiten daarom voor ondersteunende instrumenten, zodat de zorgconsument wordt geholpen bij het beoordelen en selecteren van de juiste informatie. Voorgestelde oplossingsrichtingen zijn het toevoegen van een expertoordeel waarop de zorgconsument kan vertrouwen, bijvoorbeeld door gecontroleerde webportals als kiesBeter.nl, of kwaliteitslabels zoals HON (Health on the Net) (Adams et al. 2009). In de praktijk blijken deze kwaliteitscriteria echter niet het gewenste effect teweeg te brengen. Verschillende studies hebben laten zien dat gebruikers (consumenten) deze labels niet waarderen, opmerken of toepassen (Eysenbach & Köhler 2002). De kwaliteitskeurmerken zijn niet effectief. Een belangrijke reden hiervoor is dat deze kwaliteitskeurmerken niet aansluiten bij de praktijk van het gebruiken van internet (Adams et al. 2006). "This indicates that the focus of research should be shifted away from predefined concepts of 'good' and 'bad' quality towards actual information-gathering practices" (Mager 2009: 2).

De informatie-epistemologie van gebruikers verschilt van die van de aanbieders. De gebruikers hebben een scherpe focus: in het algemeen beginnen ze hun zoektocht met brede overzichtsinformatie en focussen dan verder op specifieke informatie zoals voeding, bepaalde behandeling of oefeningen. Gebruikers zijn veelal niet gericht op de bron (adres website), maar hanteren andere evaluatietechnieken. Ze gebruiken meerdere websites tegelijk en beoordelen hoe de verschillende informatie zich tot elkaar verhoudt. "Recurring information becomes increasingly trustworthy in the course of the search process, as a couple of participants articulated" (Mager 2009: 14). Daarnaast relateren ze het nut van de informatie aan de eigen behoeftes en belangen. "Hence users tended to conceptualize online health information as an information flood made up of disconnected bits and pieces of information. Along their interests and Google's transformation of these issues in keyword indexes, they created their own stories, dissolving the boundaries between websites and their providers. The quality and validity of the information was seen primarily as solidifying the process of assembling a coherent story through reception and non-contradiction" (Mager 2009: 14).

Gebruikers hanteren een issue-centered informatie-epistemologie, providers daarentegen hanteren een actor-centered informatie-epistemologie. Waar aanbieders dus wel onderlinge relaties leggen maar websites en de geconstrueerde verhalen gescheiden houden, maken gebruikers een nieuw (en eigen) verhaal uit het aanbod van verschillende websites. Dit verschil in gehanteerde informatie-episte-

mologie heeft consequenties voor de sturingsmogelijkheden van aanbieders van informatie. De Nederlandse overheid heeft dat ondervonden bij twee recente vaccinatieprogramma's van het RIVM (Versteeg & Hajer 2010). Bij het vaccinatieprogramma tegen baarmoederhalskanker heeft het RIVM zich vooraf onvoldoende gerealiseerd wat de invloed is van het zeer kritische informatieaanbod over vaccinaties op internet. Bij het recentere vaccinatieprogramma tegen de Mexicaanse griep heeft de overheid bewust sterk ingezet op het aanbieden van informatie via internet. Maar opnieuw bleek de invloed van tegengeluiden groot, bijvoorbeeld via de website verontrustemoeders.nl. De traditionele monopoliepositie van de overheid als leverancier van medische informatie staat hiermee onder druk, zoals verwoord door Anneke Bleeker, de drijvende kracht achter de site verontrustemoeders.nl: "Anneke Bleeker vindt dat iedereen vooral zelf onderzoek moet doen. 'Wij zeggen: je moet ons niet geloven, je moet het zelf onderzoeken', zegt ze"(*de Volkskrant,* 14 november 2009: 35).

9.5.4 KANSEN EN RISICO'S VAN eHEALTH VOOR VERSCHILLENDE ACTOREN

De eHealth-beweging belooft een verdere stap naar 'patiënt centred care' en empowerment van de patiënt. De populariteit van participatoire benaderingen als een persoonlijk patiëntendossier (PPD) past bij demografische ontwikkelingen en ontwikkelingen binnen de informatiesamenleving. Het wordt bovendien als ethisch beschouwd en patiënten hebben de neiging meer tevreden te zijn wanneer ze een actieve rol hebben in het overwegen van en beslissen over de behandeling (Pluut & Zuurmond 2009). Maar Pluut en Zuurmond benadrukken ook een andere kant. Niet elke patiënt is verstandelijk en emotioneel in staat om zelf te beslissen over de behandeling. De mate waarin de patiënt een egalitaire relatie met de behandelaar op prijs stelt, verschilt van context tot context (Pluut & Zuurmond 2009). Bij de beoordeling van wat eHealth kan betekenen voor 'de burger', is van belang een onderscheid te maken naar wie die burger is en welke rol hij vervult. Voor de (nog) gezonde burger draait het om het vertrouwen dat hij in geval van ziekte kan rekenen op goede zorg, die ook, zowel op individueel als collectief niveau, betaalbaar is. Of deze zorg past in een eHealth-beweging doet daarbij niet zo veel ter zake. Maar vanuit het perspectief van een chronische patiënt zijn er aanvullende wensen te formuleren. Het is juist de chronische patiënt die veel te winnen heeft bij betere communicatie (niet elke keer hetzelfde verhaal opnieuw te hoeven vertellen) en meer invloed op het eigen zorgproces (zelf regisseren wie gevoelige persoonlijke informatie mag inzien).

Al een aantal decennia zien we dat chronische patiënten die lijden aan dezelfde aandoening elkaar opzoeken en zich verenigen in belangenorganisaties en patiëntenverenigingen (Trappenburg 2008). Met de inzet van ICT groeien de mogelijkheden hiervoor en zien we naast de meer institutioneel georganiseerde belangenorganisaties ook lossere verbanden van groepen patiënten (Allsop et al. 2004). Het is

niet verassend dat de NPCF zeer positief staat tegenover de eHealth-trend, omdat de achterban van deze organisatie bestaat uit de burgers wiens (deel)identiteit samenvalt met het ziek zijn (NPCF 2009). Oudshoorn en Somers constateren wel dat traditionele patiëntenorganisaties vaak nog behoudend zijn in het toepassen van nieuwe web 2.0-functionaliteiten op hun websites (Oudshoorn & Somers 2006). Andersom zijn het die functionaliteiten die nieuwe organisatievormen met zich meebrengen. De website PatientsLikeMe is in de eerste plaats een platform waarop patiënten informatie over hun eigen ziektebeeld met andere patiënten, artsen en farmaceutische industrie delen (zie box 9.3). Pas in de tweede plaats is de website gericht op meer 'traditionele' functies, als het vergaren van (wetenschappelijke) informatie en in contact komen met lotgenoten.

Artsen en zorgverleners staan niet onverdeeld positief tegenover alle verschillende nieuwe ICT-ontwikkelingen. *Medisch Contact* publiceerde in 2009 de resultaten van een onderzoek over de deelname van artsen aan het L-EPD (Katzenbauer 2009). Van de ondervraagden had 31 procent bezwaar gemaakt tegen de opname van de eigen medische gegevens in het L-EPD, 25 procent overwoog dat alsnog te doen, en nog eens 7 procent zou het hebben gedaan als bezwaar maken eenvoudiger was. Vanuit de beroepsgroep wordt ook gewaarschuwd voor het verloren gaan van bestaande waardevolle praktijken, zoals de vaardigheid van het schrijven van de klassieke specialistenbrief die verschillende aspecten van het vak samenbrengt bij het afronden van een opname of zorgtraject (Biesma et al. 2010).

Traditioneel had de relatie arts-patiënt de vorm van een professional-leekrelatie. De professional bezit de relevante kennis en vaardigheden. De patiënt kan niet anders dan antwoord geven op de door de professional gestelde vragen en wachten op het oordeel dat de professional op basis van die aangeleverde informatie geeft. We zien een verschuiving in deze relatie naar een meer gelijkwaardige vorm: de patiënt als de partner van de dokter. Dit heeft onder andere te maken met een afname van het informatiemonopolie: medische informatie is veel breder beschikbaar. Het heeft ook te maken met de opkomst van de patiënt als consument: als consument van informatie over ziektes en behandelingen, maar ook van informatie over artsen, ziekenhuizen en verzekeraars. Een stap verder dan een meer gelijkwaardigere relatie tussen arts en patiënt, is de beweging naar een empowered patiënt, een patiënt die zelf de regie kan voeren. De patiënt als 'expert' kan de arts uitdagen, door zijn medische autoriteit ter discussie te stellen. Bovendien veranderen verwachtingspatronen binnen de relatie arts-patiënt met de invoering van een nieuw systeem als het L-EPD (Henwood et al. 2003). Met een L-EPD mag de patiënt verwachten dat de arts te allen tijde over alle informatie beschikt. Daaraan gekoppeld is de verwachting dat de arts ook altijd in staat is deze informatie te interpreteren en er de juiste conclusies uit te trekken.

Ook verzekeraars en de industrie zien kansen voor eHealth, zoals blijkt in de oproep tot opschaling eHealth van zes marktpartijen in 2009.[27] Menzis, Achmea, TNO, Philips, KPN en Rabobank pleiten voor de instelling van een open platform samen met het Zorginnovatieplatform en het ministerie van VWS. Dit nieuwe platform zou barrières van de praktijk moeten slechten, zoals gebrek aan draagvlak bij patiënten en medische professionals, dominantie van de aanbodkant bij het ontwerpen van diensten, onvoldoende uniformering en standaardisatie en gebrek aan financiering. De zorgverzekeraars mengden zich niet actief in de discussie over het L-EPD (vergelijk Pluut 2010). In een positiepaper voor de eerste expertmeeting in de Eerste Kamer geeft Zorgverzekeraars Nederland (ZN) aan voorstander te zijn van een L-EPD, maar zelf geen ambitie te hebben om toegang te verkrijgen tot de EPD's (ZN 2009). Tijdens de expertmeetings in de Eerste Kamer bleek dat burgers en leden van de Eerste Kamer zich toch zorgen maken over mogelijke toegang van zorgverzekeraars tot medische dossiers in de toekomst (Rathenau 2009c; Eerste Kamer 2009-2010c).

Voor de overheid passen de kansen die eHealth biedt bij het bestaande beleid gericht op een verschuiving van een focus op behandeling en genezing naar een focus op het promoten van gezondheid en preventie. De overdracht van informatie of beïnvloeding door informatie verschuift van de spreekkamer naar de huiskamer (via internet). En als de voorspellingen over eHealth-ontwikkelingen realiteit worden, kan het verder opschuiven van het aanbieden van informatie naar het (op afstand) vergaren van informatie.[28] Maar eHealth brengt ook een verlies van de (relatieve) monopoliepositie als leverancier van medische informatie met zich mee. Een overheid die het aanbieden van informatie als een belangrijk sturingsinstrument ziet, zal nieuwe vormen moeten verzinnen om te zorgen dat de aangeboden informatie de burger/patiënt ook daadwerkelijk bereikt (vgl. Tiemeijer et al. 2009).

9.6 BEGINSELEN

In de discussie over de inzet van ICT, zoals bij de introductie van het L-EPD of andere eHealth-toepassingen, brengen actoren verschillende overwegingen in. In het publieke en politieke debat komen we verschillende beginselen tegen die voor- en tegenstanders aandragen, en die bij besluitvorming tegen elkaar moeten worden afgewogen. Aan de hand van een aantal beginselen analyseert deze paragraaf hoe de inzet van ICT van invloed is op relaties binnen dit domein.

9.6.1 EFFICIËNTIE EN EFFECTIVITEIT

Effectiviteit en efficiëntie worden tezamen vaak gepresenteerd als *the best of both worlds*: de zorg kan met behulp van inzet van innoverende technologieën kwalitatief beter (effectief) en goedkoper (efficiënt). Maar de relatie tussen deze twee

beginselen is in dit domein veelal ingewikkeld, omdat betere zorg die voortkomt uit de inzet van nieuwe technologieën vaak (in ieder geval bij initieel gebruik) erg kostbaar is, en dan ook nog niet altijd breed inzetbaar. Het L-EPD is zo'n technologische innovatie die gepresenteerd wordt als efficiënt en effectief voor alle betrokkenen. Hoewel deze onderliggende vooronderstellingen door verschillende actoren in het proces van ontwikkeling en implementatie volop worden gebruikt, ontbreekt de feitelijke onderbouwing, zoals aangegeven in paragraaf 9.4.

9.6.2 PRIVACY

Privacy is een veelgebruikt concept in het domein gezondheidszorg, wat tot uiting komt in de uitgebreide regelgeving die het privacybelang van de patiënt moet waarborgen. In het kader van technologische vernieuwing blijft dit beginsel zeker niet onbesproken, en meer specifiek wordt het belang van het waarborgen van privacy voortdurend bevestigd zowel door voor- als tegenstanders van het invoeren van EPD-systemen. Opvallend is dat waar burgers op andere terreinen een laconieke houding laten zien ten aanzien van hun privacybelang, dit binnen het domein gezondheidszorg anders uitpakt. In dit domein bevindt de burger (de patiënt) zich in een afhankelijke en kwetsbare positie: medische handelingen maken per definitie een inbreuk op de persoonlijke ruimte en tasten de integriteit van het lichaam aan. Absolute privacy is ook niet aan de orde gezien de noodzakelijke communicatie tussen zorgverlener en zorgconsument. Bij medische informatie draait informationele privacy om de bescherming van informatie en gegevens ten opzichte van onbevoegden: het neerzetten van schotten (ondoorlatend) en weerstanden in de informatiestroom. Dit is echter moeilijk te verenigen met de centrale gedachte achter een landelijk systeem voor uitwisseling van medische dossiers: altijd alle (relevante) informatie beschikbaar hebben.

Zoals gezegd komt privacy uitvoerig aan bod en lijkt meegenomen te worden bij ontwerp en implementatie van een nieuw systeem als het landelijk EPD. Maar de vraag wat privacy betekent wordt wel vaak ingevuld vanuit de 'oude' praktijk: de relatie tussen de arts en de patiënt die gekenmerkt wordt door het medisch beroepsgeheim. Wanneer deze oude praktijk verandert door de inzet van ICT, is het de vraag of de invulling van privacy onder druk komt te staan.

9.6.3 TRANSPARANTIE

Met de komst van nieuwe technologieën lijkt er sprake te zijn van een transparantieparadox. Aan de ene kant bieden de nieuwe technieken de kans om meer inzicht en overzicht te verkrijgen in bepaalde ziektes en zorgprocessen. Aan de andere kant maken de technieken het mogelijk onderdelen op te nemen in een groter geheel (zoals zorgketens of geïntegreerde databases) waarbij de relatie tussen dit geheel en de verschillende onderdelen moeilijker wordt om te overzien.

Voor een zorgstelsel gebaseerd op marktwerking, maar ook voor eHealth, en meer specifiek Health 2.0, is transparantie een noodzakelijke voorwaarde. Transparantie, in de betekenis van (volledige) beschikbaarheid van informatie, zou actoren in staat stellen weloverwogen keuzes te nemen. Het accent ligt op de keuzevrijheid van de patiënt ten opzichte van zorgverlener of behandeling. Maar ook andere actoren zouden zijn gebaat bij transparantie. Zo biedt alle informatie van het EPD de arts de mogelijkheid om de 'transparante' patiënt beter te behandelen. Op een hoger aggregatieniveau kan transparante medische informatie resulteren in betere zorg door middel van *evidence based* protocollen, maakt het verzamelen en bewerken van medische data (o.a. van DNA) nieuwe medische doorbraken mogelijk, en maakt transparantie van zorgprocessen het voor verzekeraar en overheid mogelijk gedegen beleids- en financieringskeuzes te maken. Maar om te kunnen beoordelen in hoeverre de introductie van een systeem of technologie daadwerkelijk transparantieverhogend werkt, is het van belang te zien wie of wat transparant wordt voor wie, en in hoeverre er sprake is van een uitruil van transparantiebelangen.

eHealth en de meer gelijke relatie tussen arts en patiënt die het mogelijk maakt, lijken voor beide partijen van deze relatie meer transparantie op te leveren. De patiënt kan zelf zijn informatie beheren en overzien, terwijl de arts door uitwisseling van dossiers zich een 'compleet' beeld van de patiënt kan vormen. Het is wel de vraag hoe deze twee varianten van transparantie zich tot elkaar verhouden. Wanneer de patiënt, zoals is aangekondigd voor de nabije toekomst, daadwerkelijk in staat is meer eigen regie te voeren, is het voor de arts niet meer zo zeker dat hij kan beschikken over alle relevante informatie. Waar de arts eerder communiceerde en informatie uitwisselde met medeprofessionals, gebonden aan dezelfde beroepsethiek, wordt hij nu afhankelijk van de keuzes van de patiënt.

De professional kan transparanter worden voor collega's, management, inspectie en patiënten, wat de kwaliteit van de zorg ten goede kan komen.[29] Transparantie van zorgprocessen en over het functioneren van zorginstellingen is ook noodzakelijk binnen het systeem van marktwerking dat in de zorg is geïntroduceerd. Naast transparantie van medische data (inhoudstransparantie) is ook transparantie van de regels en procedures (procestransparantie) van belang in het domein gezondheidszorg. De patiënt krijgt in het L-EPD inzicht zowel in zijn dossier als in de loggegevens van het systeem, al is nog niet duidelijk op welke manier dit vorm gaat krijgen. Maar in hoeverre zijn deze gegevens transparant voor de patiënt? Uitgaande van een achterstand in kennis is het de vraag wat voor een transparantie dit eigenlijk oplevert.

Er lijkt sprake te zijn van *schijn*transparantie. Zo zal de patiënt straks zelf de loggegevens van het L-EPD kunnen inzien, om te controleren dat daadwerkelijk alleen bevoegde zorgverleners toegang hebben gezocht en verkregen tot zijn EPD. Maar in hoeverre is een situatie, waarin een zorgconsument niet weet wanneer en

hoe vaak hij de loggegevens zal moeten inzien om een actueel beeld te houden van toegang tot zijn EPD, echt transparant te noemen? En in hoeverre bieden deze loggegevens inzicht in de omgang van zorgprofessionals of anderen (de secretaresse die gebruikmaakt van de UZI-pas van de arts) met zijn medische gegevens?

Het belang van transparantie wordt door de belangrijke actoren in het (gezondheids)domein ondubbelzinnig onderschreven, maar het is de vraag of er ook *te veel* transparantie kan zijn in dit domein. Een EPD betekent dat de arts alle beschikbare informatie over de patiënt te zien krijgt, en daarmee een 'totaalbeeld' krijgt van die patiënt. Maar dergelijke transparantie is niet voor elke medische behandeling noodzakelijk, het gaat soms slechts om een momentopname onder specifieke omstandigheden. Naast te veel transparantie voor anderen, is er ten aanzien van gezondheid ook te bedenken dat er sprake kan zijn van te veel transparantie voor zichzelf. Het is de vraag of de patiënt of de potentiële patiënt in alle gevallen wil beschikken over alle mogelijke informatie over zijn gezondheid. Met DNA-onderzoek betreft deze informatie bovendien niet alleen je huidige gezondheid, maar ook je toekomstige gezondheid.

9.6.4 KEUZEVRIJHEID

In het domein gezondheidszorg is de laatste jaren door de overheid sterk ingezet op keuzevrijheid voor de zorgconsument. Met de herziening van het zorgstelsel, waarbij invoering van verdere marktwerking in de zorg centraal stond, is keuzevrijheid zelfs een keuzeplicht te noemen. De overheid heeft verschillende voorzieningen opgezet waar de burger de noodzakelijke informatie kan vinden die hem in staat moet stellen een keuze te kunnen maken, zoals www.kiesBeter.nl. Tegelijk moet de overheid accepteren dat het geen monopolieposities (meer) kan bezetten ten aanzien van deze informatievoorziening. Het aanbod van aan gezondheid gerelateerde informatie op internet is overweldigend, maar niet altijd van gelijke kwaliteit, onpartijdig of in gelijke mate betrouwbaar. Keuzevrijheid voor de burger, in de betekenis van zelf kiezen welke informatiebron je vertrouwt, kan dus ook het beleid van de overheid tegenwerken. Bovendien is het aanbod van informatie over gezondheid zo groot dat het de vraag is of deze hoeveelheid het maken van een keuze juist niet in de weg kan staan.

Centraal in het eHealth-discours is de verwachting dat de positie van de zorgconsument ten opzichte van de medische professional versterkt zal worden. Achter het ideaal van de patiënt als regisseur ligt een mensbeeld van de burger als een rationeel kiezend wezen. De vraag in hoeverre dit mensbeeld terug te vinden is in de empirie speelt extra in het domein gezondheidszorg waar sprake is van kwetsbare posities en sterke afhankelijkheidsrelaties. De idee dat de burger in staat is uit een grote hoeveelheid informatie de 'juiste' keuze te maken staat onder druk (Tiemeijer et al. 2009). Omdat gezondheidszorg iets is wat alle burgers (in hun rol

als potentiële patiënt) raakt, betekent dit dat de overheid (ook een verantwoordelijkheid) heeft zorg te dragen dat alle burgers de technische capaciteit bezitten hun keuzevrijheid in te vullen. De digitale kloof is dus niet te negeren.

Wat betreft de burger is het tot slot opmerkelijk hoe een overheid die sterk wil inzetten op keuzevrijheid van de consument, de keuzevrijheid voor deelname aan het EPD zo heeft geprobeerd in te perken met de brief over de mogelijkheid bezwaar te maken die in het najaar van 2008 is verzonden. De brief gaf een gekleurde presentatie van de keuzevrijheid van de patiënt, door de inspanning te vragen van de burger om af te wijken van de default-optie (deelnemen), en bovendien de suggestie te wekken dat er een deadline aan deze mogelijkheid verbonden was. De keuze voor een opt-out- in plaats van een opt-in-systeem voor het landelijk EPD lijkt ook op gespannen voet te staan met het idee van empowerment van de patiënt. Het is ook de vorm van keuze die bepalend is in hoeverre er sprake is van vrijheid.

De zorgprofessional heeft, anders dan de zorgconsument, geen keuzevrijheid ten aanzien van deelname aan het L-EPD, hij is verplicht deel te nemen. Met de invoering van een gekoppeld systeem als het L-EPD wordt de professional nog meer dan voorheen onderdeel van een keten van zorg. Voorwaarden voor een goed functionerende keten zijn onder andere communicatie, operabiliteit en afstemming van taal. Deze systeemvoorwaarden beperken de keuzevrijheid van de professional, hij moet zijn handelingen aanpassen aan de systeemvoorwaarden. Omdat zorgverleners naast het officiële dossier eigen werkaantekeningen mogen maken die niet hoeven te worden uitgewisseld bestaat de kans dat door de inperking van de professionele keuzevrijheid artsen 'schaduwdossiers' gaan hanteren, waarmee de ambitie van te allen tijde beschikbaarheid van alle informatie weer onder druk komt te staan.

9.6.5 ACCOUNTABILITY

In vorige paragrafen is aangegeven dat het domein gezondheidszorg een scala aan juridische regelingen, van wetten tot professionele gedragscodes, kent die de onderlinge relatie tussen betrokken actoren juridisch vormgeven. Tegelijk is aangestipt hoe deze regelingen nog niet altijd de veranderingen binnen dit domein die te maken hebben met informatie en technologie geïncorporeerd hebben, zoals blijkt ten aanzien van de aansprakelijkheid en het EPD (zie subparagraaf 9.4.1). Het domein en zijn spelregels lijken nog niet goed te zijn afgestemd op de nieuwe situatie. De toegenomen transparantie van het zorgproces door de inzet van ICT maakt de verantwoordelijkheid voor handelingen binnen dit proces zichtbaar. Maar de transparantie kan ook situaties zichtbaar maken, waarvan we vooraf de verantwoordelijkheden niet hebben kunnen afspreken. De medische wetenschap kan helaas niet van tevoren de uitkomsten van de behandeling garanderen. In de prak-

tijk wordt deze onzekerheid gereguleerd door het informed consent, waarmee de verantwoordelijkheidskwestie deels 'buiten spel wordt gezet'.

eHealth stelt de patiënt centraal. Maar deze nieuwe positie brengt naast rechten ook plichten met zich mee, de patiënt wordt de 'collega' van de arts en daarmee samen verantwoordelijk voor zijn gezondheid. De op zich uitgebreide regelgeving in de zorgsector is echter (nog) gericht op het waarborgen van de belangen van de patiënt die zich in een afhankelijke positie bevindt. De introductie van eHealth neemt de afhankelijkheid van de patiënt natuurlijk ook niet weg, maar voegt wel andere afhankelijkheden toe. Hoe accountabel is een arts die een verkeerde diagnose stelt, omdat hij zich, zonder dat te kunnen weten, baseert op een dossier waar de patiënt als regisseur bewust bepaalde onderdelen uit heeft verwijderd? Transparantie en keuzevrijheid brengen ook verantwoordelijkheid voor de keuze met zich mee. Waar vroeger de arts vanuit zijn kennisvoorsprong sturend was in keuze voor een bepaalde behandeling, wordt die keuze en daarmee ook de verantwoording steeds meer bij de zorgconsument gelegd. Het is niet alleen de vraag of de zorgconsument wel in staat is op basis van (goede) informatie een verantwoorde keuze te maken, maar ook of alle patiënten er wel prijs op stellen zelf manager te zijn van hun zorgproces en daarmee ook (mede)verantwoordelijkheid te dragen. Vergelijkbaar brengt de toegenomen transparantie over de relatie tussen gedrag, levensstijl en (genetische) aanleg tot gezondheid de vraag naar voren wie verantwoordelijkheid draagt of kan dragen.

9.7 CONCLUSIES

In deze domeinstudie is een beeld geschetst van actuele ontwikkelingen rond informatie en technologie in het domein gezondheidszorg en de betekenis van deze ontwikkelingen voor de relatie tussen belangrijke actoren. Hierbij is een onderscheid te maken tussen twee typen bevindingen. Ten eerste conclusies over de vormgeving en uitvoering van nieuwe ICT-toepassingen. Ten tweede conclusies die te maken hebben met de idee van een EPD of eHealth: wat betekent dit voor de verschillende actoren, de onderlinge relaties en de beginselen.

9.7.1 VORMGEVING EN UITVOERING

Veranderingen en innovaties roepen weerstand op en dat is in het domein gezondheidszorg niet anders. De grote stappen voorwaarts die dankzij medische innovaties in de geschiedenis zijn gezet laten zien dat dit op zich geen afdoende reden is de status-quo te handhaven. Maar het is wel interessant te zien hoe met deze weerstand wordt omgegaan, en hoe ze wordt meegenomen in het proces van ontwikkeling en implementatie. In de reacties op de invoering van het L-EPD kunnen we twee strategieën herkennen (Vorstenbosch 2009). Een eerste reactie is het relativeren van de opgeworpen problemen: een elektronisch dossier verschilt niet wezen-

lijk van een papieren dossier; dus zijn de bestaande waarborgen ten aanzien van privacy en dergelijke toereikend. Deze redenatie zien we terug in het onderzoek naar aansprakelijkheid van de Universiteit Tilburg (Barendrecht et al. 2008). Een andere strategie is het 'bezweren' van de zorgen met behulp van technologie, zoals de discussie over beveiligde infrastructuur en UZI-passen laat zien. Paradoxaal wordt hier de 'veroorzaker' van de weerstand ingezet om deze te overkomen.

Vanaf het begin van de politieke en beleidsdiscussie over het EPD wordt uitgegaan van een landelijke infrastructuur en een landelijk EPD. Maar in de loop der jaren komt de afstemming tussen bestaande regionale systemen en de landelijke infrastructuur herhaaldelijk terug op de agenda, vooral door interventies van de zorgverleners. Tot nu toe heeft de weerstand van verschillende actoren niet geleid tot een fundamentele heroverweging van het ontwerp van het systeem in relatie tot de doelen. Bij ontwerp en ontwikkeling van het L-EPD vindt uitruil van belangen plaats, zelfs binnen eenzelfde beginsel. Hierboven is beschreven hoe de toename van transparantie bij de ene actor ten koste kan gaan van transparantie voor de andere actor. Ook bij de andere beginselen speelt een dergelijke uitruil. Bij het ontwerp en de ontwikkeling van systemen als het L-EPD zou er constante afweging plaats moeten vinden tussen de baten aan de ene kant en de kosten en risico's aan de andere kant. De afweging is niet alleen relevant bij de initiële keuze voor wel of niet invoeren van een dergelijk systeem, maar ook voor de keuzemomenten in de ontwikkeling. Het L-EPD wordt ingevoerd om medische fouten door gebrek aan informatie en communicatie te voorkomen. Het verhoogde risico voor het privacybelang van de burger wordt hieraan ondergeschikt geacht. Maar dezelfde afweging tussen effectiviteit en efficiency en privacy zou opnieuw en expliciet gemaakt moeten worden bij de ontwerpkeuze van de architectuur van het systeem: een landelijk of een regionaal EPD.

In een sterk gereguleerd domein als de gezondheidszorg is het verleidelijk de nieuwe technologische voorzieningen in te passen in het bestaande systeem van regelgeving. Ten aanzien van de bescherming van privacy van de patiënt en van de aansprakelijkheid voor medisch handelen wordt in het EPD-debat dan ook verwezen naar de huidige bescherming (in de vorm van Wbp, WGBO en WMO) eventueel aangevuld met technische middelen, zoals een UZI-pas voor zorgverleners met BIG-registratie. Maar de invoering van een systeem als het EPD brengt kwalitatieve veranderingen met zich mee die noodzaken dat het bestaande systeem van regelgeving principiëler ter discussie komt te staan.

9.7.2 VAN PASSIEVE PATIËNT TOT REGISSEUR

Het L-EPD en de bredere eHealth-beweging worden gepresenteerd als een enorme kans voor de gezondheidszorg en daarbinnen voor alle verschillende actoren. Hierbij moeten twee kanttekeningen gemaakt worden: (1) zeker bij het begin van

de ontwikkeling van het L-EPD, tonen verschillende actoren eenzijdige aandacht voor nieuwe mogelijkheden en positieve effecten, maar geen of weinig aandacht voor wat er verloren gaat of voor hoe realistisch verwachtingen zijn; (2) de voorwaarden die nodig zijn om die positieve effecten ook daadwerkelijk te bereiken zijn nog niet altijd gerealiseerd of realiseerbaar (zoals toegang van de patiënt tot het L-EPD-systeem). In de loop van het proces is bij sommige actoren, zoals de Eerste Kamer, meer aandacht gekomen voor kritische geluiden.

Het optimistische beeld van de technologie blijft niet academisch, het beïnvloedt daadwerkelijk de praktijk rond een technologische applicatie, zoals het debat over de invoering van het L-EPD laat zien. Het EPD is al lang onderwerp van discussie, al gebeurde dit in een eerder stadium onder een andere benaming, maar de discussie over het EPD en zijn voordelen pasten toen binnen een ander discours: niet zozeer empowerment van de patiënt maar efficiëntie en effectiviteit. In een eerder stadium was er wel (beperkt) oog voor de voordelen van een dergelijk systeem voor de patiënt, maar het beeld hierbij was dat van een passieve patiënt, en niet van een actieve patiënt die niet alleen centraal staat, maar zelf de regie in handen heeft. De structuur van een landelijk EPD waarbij het uitgangspunt van communicatie en uitwisseling de informatie gedeeltelijk 'loskoppelt' van degene die de informatie registreert, heeft de vraag van eigenaarschap op de agenda geplaatst. Waar voorheen het dossier diende ter ondersteuning van de werkzaamheden van de arts, moet het dossier nu primair ten dienste staan van het zorgproces van de patiënt. Maar omdat het huidige ontwerp van de architectuur van het systeem voortbouwt op de oude situatie waarin het dossier een instrument is van de zorgverlener, is het zeer de vraag of de nieuwe functionaliteiten die nu van het systeem worden geëist wel met deze architectuur kunnen worden gerealiseerd.

Er is sprake van een paradox: aan de ene kant draait de invoering van een systeem als het L-EPD om de gedachte dat alle informatie te allen tijde beschikbaar moet zijn, om een goede kwalitatieve zorg te kunnen leveren. Maar tegelijk draait eHealth om versterking van de positie van de patiënt, meer mogelijkheden voor de patiënt om zelf de regie over zijn gezondheid te voeren. Er zit een duidelijke spanning tussen beide idealen: volledige beschikbaarheid van informatie en eigen regie van de patiënt. Deze spanning wordt duidelijk bij het recht dat de patiënt heeft om bepaalde gegevens uit zijn EPD te laten verwijderen. In het voorstel voor wetswijziging van de Kaderwet elektronische zorginformatie-uitwisseling stelt de minister voor dat de onvolledigheid van het dossier zichtbaar moet zijn voor de zorgverlener aan wie dit dossier wordt verstrekt. Maar het CBP concludeert dat de 'melding onvolledig EPD' op gespannen voet staat met de Wbp.[30]

eHealth brengt een verschuiving met zich mee van de spreekkamer naar de huiskamer, of een andere plek met internettoegang. Waar informatie en communicatie over gezondheid en ziekte eerst waren afgebakend in plaats en tijd, 'dringen' ze nu

door tot andere domeinen. De overheid maakt zelf gebruik van deze trend door via verschillende media de burger te wijzen op het belang van een gezonde levensstijl, en door de patiënt op basis van informatie actief te laten kiezen voor een verzekeraar, een voorwaarde om een systeem van marktwerking binnen de zorg te kunnen realiseren. De overheid heeft een instrument om zich ook buiten de directe spreekkamer meer proactief op te stellen door middel van beleid gericht op preventie. Opnieuw kunnen we hier een spanning zien tussen een proactieve overheid en een overheid die beleid voert gericht op een patiënt die zorgconsument moet zijn en eigen regisseur.

Waar de overheid een nieuw sturingsinstrument verwerft, verliest ze tegelijk controle over het aanbod van informatie en communicatie door de enorme groei aan concurrerende informatie. Bovendien blijkt onder invloed van de technologie de zorgconsument deze informatie op een andere manier te gebruiken en toe te passen. In de praktijk blijkt dat burgers of patiënten bij het vormen van een mening of het maken van een keuze zich niet primair laten leiden door de autoriteit van de bron, maar door de manier waarop informatie van verschillende bronnen zich tot elkaar verhoudt en in elkaar past. Met de opkomst van medische informatie op internet is die informatie dus niet langer meer gebonden aan de medische instituties, maar 'ontsnapt' naar de bredere samenleving.

De kansen die eHealth biedt aan de patiënt om zijn positie te versterken zijn helder, maar de rol van regisseur brengt niet alleen rechten maar ook verantwoordelijkheden met zich mee. Een nieuwe verantwoordelijkheidsverdeling zou tot uiting kunnen komen in een nieuwe invulling van het begrip *informed consent* (vergelijk Bergkamp 1996). Het is niet meer de arts die de verantwoordelijkheid draagt voor het verstrekken van relevante informatie, maar de patiënt die de verantwoordelijkheid draagt voor (1) het zelf vergaren van relevante informatie, (2) het delen van die informatie met betrokkenen. Voor de overheid of voor de intermediërende arts of zorginstelling is dit in sommige opzichten wellicht een aantrekkelijk mensbeeld. Maar het is de vraag of alle burgers of (potentiële) patiënten in gelijke mate in staat en gemotiveerd zullen zijn deze nieuwe verantwoordelijkheden op zich te nemen.

AFKORTINGEN

BIG	Beroepen in de Individuele Gezondheidszorg
BSN	Burgerservicenummer
CBB	College voor Beroep voor het Bedrijfsleven
CBP	College bescherming persoonsgegevens
CIZ	Centrum Indicatiestelling Zorg
COM	Commission of the European Communities
DBC	Diagnose Behandel Combinaties
DIS	DBC informatiesysteem
EBM	evidence-based medicine
eHealth	electronic health
EPD	Elektronisch Patiëntendossier
EHR	Electronic Health Record
EZ	Economische Zaken
EZD	Elektronisch Zorgdossier
HARM	Hospital Admissions Related to Medicine
HIS	Huisartsen Informatie Systeem
HLCH	High Level Committee on Health
HON	Health on the Net
ICT	Informatie- en communicatietechnologie
IGZ	Inspectie voor de Gezondheidszorg
IPZorg	ICT Platform in de Zorg
JRC	Joint Research Centre
L-EPD	landelijk Elektronisch PatiëntenDossier
MC	Medisch Contact
NHG	Nederlands Huisartsen Genootschap
NICTIZ	Nationaal ICT Instituut in de Zorg
NPCF	Nederlandse Patiënten Consumenten Federatie
NPfIT	National Program for IT
NPM	New Public Management
NVMA	Vereniging voor Zorgadministratie en Informatie
PHR	Personal Health Record
PCHR	Personal Controlled Health Record
PI	Parelsnoer Initiatief
PPD	Persoonlijk Patiëntendossier
RIBIZ	Registratie en Informatie Beroepsbeoefenaren in de Zorg
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
RVZ	Raad voor Volksgezondheid en Zorg
SAZ	Samenwerkende Algemene Ziekenhuizen
SZW	Sociale Zaken en Werkgelegenheid
UMC	Universitair Medisch Centrum

UWV	Uitvoeringsinstituut Werknemersverzekeringen
UZI	Unieke Zorgverlener Identificatie
VWS	Volksgezondheid, Welzijn en Sport
WGBO	Wet op de geneeskundige behandelingsovereenkomst
Wbp	Wet bescherming persoonsgegevens
WMO	Wet Medisch wetenschappelijk Onderzoek met mensen
ZIS	Ziekenhuis Informatie Systeem
ZN	Zorgverzekeraars Nederland

NOTEN

1 De dominantie van dit thema in het debat wordt zichtbaar in de notitie *ICT en Zorg* van mei 2008 (NICTIZ 2008). Deze notitie behandelt vrijwel uitsluitend de voortgang van (de) invoering van het EPD.

2 De reconstructie van Pluut (2010) laat zien hoe de benaming van dit systeem een rol heeft gespeeld in het ingewikkelde proces van ontwikkeling en invoering.

3 Juist om deze diversiteit aan rollen tot uitdrukking te laten komen maakt deze bijdrage geen keuze voor één term, maar wordt in het vervolg de term gebruikt die het beste aansluit op de rol die aan de orde is.

4 Opvallend is de hoge gelaagdheid van vertegenwoordiging: vrijwel alle actoren zijn verenigd in belangengroepen met vertegenwoordiging, en die vertegenwoordigers maken op hun beurt deel uit van samenwerkings- en overlegstructuren (Dijstelbloem et al. 2004).

5 In lijn met het rapport *iOverheid* maak ik een onderscheid tussen gegevens, informatie (gefilterde gegevens, omdat alleen die gegevens worden beschouwd die relevant zijn binnen een bepaalde context) en kennis (die ontstaat wanneer verschillende informatiecomponenten met elkaar in verband worden gebracht) (WRR 2011)

6 In de voortgangsrapportage van 9 september 2010 wordt gemeld dat 425.568 bezwaren zijn verwerkt. 12.364 verzoeken zijn dubbel ingediend en 29.334 bezwaren zijn niet compleet. 5.892 bezwaren konden niet in behandeling worden genomen en zijn afgewezen (Tweede Kamer 2010-2011). De voortgangsrapportage vermeldt niet waarom de afgewezen bezwaren niet in behandeling kunnen worden genomen.

7 Het medisch beroepsgeheim behoort toe aan de patiënt en omvat twee onderdelen, de plicht tot geheimhouding en het verschoningsrecht voor de arts. Voor personen die de arts ondersteunen bij zijn hulpverlening, zoals secretaresses of dataverwerkers, geldt een afgeleide zwijgplicht.

8 Voor medisch-wetenschappelijk onderzoek worden verschillende bronnen gebruikt, naast gegevens ook lichaamsmateriaal of proefpersonen, maar in deze studie ligt de nadruk op medische gegevens. Dit type persoonsgegevens wordt verzameld en verwerkt in verschillende vormen: anoniem, gecodeerd of betrekking hebbend op een geïdentificeerde of identificeerbare persoon. Gecodeerde gegevens kunnen direct of indirect herleidbaar zijn.

9 Het gaat om regels betreffende: verantwoordelijke, expliciete en gerechtvaardigde doelstelling; verwerkingsgrond; opheffing van het verwerkingsverbod bij verwerking van gevoelige gegevens; doelbinding bij verdere verwerking en bewaring; proportionele, juiste en nauwkeurige gegevensverwerking; adequate gegevensbeveiliging; informatieplicht; meldingsplicht; recht op inzage en correctie (Ploem 2004).

10 Bij de verzameling van primaire gegevens, direct bij de betrokkene, vraagt de Wpb om uitdrukkelijke toestemming; als ook de WGBO van toepassing is, dient de

hulpverlener de betrokkene (patiënt) over het verzamelen van extra gegevens te informeren en hiervoor toestemming te vragen. Onder de WMO mag deelname aan onderzoek pas plaatsvinden nadat schriftelijk *informed consent* is verkregen.

11 LJN: BN3056, College van Beroep voor het Bedrijfsleven, AWB 08/695, 08/696, 08/701, 08/705, 08/709, 08/713, 08/715 en 08/724, te raadplegen op www.rechtspraak.nl.

12 In de literatuur komen we veelal de Engelse afkortingen tegen: Electronic Health Record (EHR), Personal Health Record (PHR) en Personal Controlled Health Record (PCHR). PCHR is een subcategorie van PHR.

13 Halamka, Mandl en Tang (2008) beschrijven verschillende initiatieven met Personal Health Records in de VS in drie ziekenhuizen: Beth Israel Deaconess Medical Center, Boston; Children's Hospital Boston, Boston; Palo Alto Medical Foundation, Palo Alto.

14 Het betreft hier ook een aanpassingsproces dat niet ineens, maar geleidelijk zal plaatsvinden. Dit zien we terug in de recente (2009) bijstelling van De Richtlijn Adequate Dossiervorming met het Elektronisch Patiëntendossier (2004) van het Nederlands Huisartsen Genootschap.

15 Voor het overzicht in deze paragraaf is gebruikgemaakt van de voor dit project geschreven Black Box-studie van Bettine Pluut. In deze studie is een volledig overzicht te vinden van de besluitvorming en opinies rond het landelijk EPD. (Zie Pluut 2010, als webpublicatie beschikbaar op www.wrr.nl). In deze paragraaf wordt een aantal aspecten van het L-EPD uitgelicht.

16 De Eerste Kamer organiseerde, ondersteund door het Rathenau Instituut, expertmeetings in december 2009 en maart 2010 (Eerste Kamer 2009-2010 c en d). Voorafgaand aan de eerste bijeenkomst zijn op verzoek van de Eerste Kamer door verschillende experts en belangengroepen issuepapers ingediend (zie Rathenau Instituut 2009a en 2009b).

17 Brief november 2008, Tweede Kamer 2008-2009a.

18 Guardian 25 mei 2009: "NHS Patients given right to delete electronic record."

19 Interview met M. Bolhuis, Google Nederland.

20 Geldt niet voor alle partijen. De SP wijst op het gevaar van instabiliteit en onveiligheid van het systeem wanneer de patiënt meer macht krijgt of het eigen dossier op afstand in kan zien. De VVD en SGP gaan in dit debat niet specifiek in op dit onderwerp.

21 Price Waterhouse Coopers, de Radboud Universiteit Nijmegen en de Universiteit Tilburg concluderen in december 2008 in een onderzoek aangevraagd door de minister van VWS dat DigiD+ een te lage bescherming biedt voor medische patiëntengegevens. Daarom laat de minister een variant (EPD-DigiD) ontwikkelen met een verbeterd uitgifteproces op basis van face-to-face uitgifte aan een balie voordat de burger toegang krijgt tot het EPD (Tweede Kamer 2009-2010).

22 Het ICT Platform in de Zorg is in 1999 opgericht en bestaat uit vertegenwoordigers van koepels van patiënten, zorgaanbieders, zorgverleners en zorgverzekeraars en de ministeries van EZ en VWS.

23 Zie bijvoorbeeld: Tweede Kamer 2005-2005; Tweede Kamer 2007-2009b en c.

24 Net als bij Web 2.0 bestaat ook over de definitie van Health 2.0 geen overeenstemming, maar het uitgangspunt van empowerment van de patiënt wordt breed onderschreven.

25 Gezondheidszorg valt onder het nationale beleid van de lidstaten, maar "de Gemeenschap vult het optreden van de lidstaten aan gericht op verbetering van de volksgezondheid, preventie van ziekten en aandoeningen bij de mens en het wegnemen van bronnen van gevaar voor de menselijke gezondheid" (Verdrag tot oprichting van de Europese Gemeenschap, Art 152, lid 1). Het Nederlandse beleid ondervindt dus wel invloed van Europese initiatieven en onderzoeken, en oefent op zijn beurt ook invloed uit op Europees niveau.

26 SNOMED CT staat voor Systematized Nomenclature of Medicine Clinical Term en is een medisch terminologiestelsel bedoeld voor het eenduidig vastleggen van medische begrippen in elektronische informatiesystemen (www.NICTIZ.nl).

27 Marktpartijen roepen op tot opschaling e-health, nieuwsbericht 6 juli 2009, www.zorginnovatieplatform.nl, geraadpleegd op 5 november 2009.

28 Een voorbeeld is een vloertegel in de keuken die functioneert als een weegschaal.

29 Het recente incident rond een neuroloog in Twente die verkeerde diagnoses stelde, laat zien hoe nuttig en noodzakelijk meer transparantie in deze relatie is (*NRC Handelsblad* 2009).

30 CBP 2009: z2009-00581. Beschikbaar op www.cbpweb.nl.

LITERATUUR

Adams, S., A. de Bont & M. Berg (2006) Looking for answers, constructing reliability: An exploration into how Dutch patients check web-based medical information, *International Journal of Medical Informatics* 75: 66-72.

Adams, S. & Roland Bal (2009) Practicing Reliability, reconstructing traditional boundaries in the gray areas of health information review on the web, *Science, Technology & Human Values*, volume 34, no.1:34-54.

Allsop, J., K. Jones & R. Baggott (2004) Health consumer groups in the UK: a new social movement?, *Sociology of Health & Illnes*, vol.26:6, 2004: 737-756.

Attema, J. & D. de Nood (2010) *Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit,* rapportage van ECP-EPN in samenwerking met de WRR, WRR-webpublicatie nr.47, www.wrr.nl.

Bal, Roland (2008) *De nieuwe zichtbaarheid. Sturing in tijden van marktwerking*, oratie, Erasmus Universiteit Rotterdam, 29 februari 2008.

Barendrecht, J.M., M.F.M. van den Berg, T.F.E. Tjong Tjin Tai & C.B.M.C. Zegveld (red.) (2008) *Aansprakelijkheden rond het EPD*, rapport in opdracht van het ministerie van Volksgezondheid, Welzijn en Sport, Tilburg: Universiteit van Tilburg, Tilburg Institute for Interdisciplinary Studies of Civil Law and Conflict Resolution Systems.

Bemt, P. van den (2006) *HARM (Hospital Admissions Related to Medication)*, Utrecht: Universiteit van Utrecht.

Berg, Marc (1996) Practices of reading and writing: the constitutive role of the patient record in medical work, *Sociology of Health & Illness*, vol.18 no.4: 499-524.

Bergkamp, L. (1996) De informatiesnelweg en informed consent. De verantwoordelijkheid van de patiënt en informed consent in de 21ste eeuw, *Medisch Contact*, jaargang 51/ 17 mei 1996: 674-678.

Biesma, D., H. Bijlsma & A. Hoepelman (2010) Specialistenbrieven in een digitaal tijdperk, *Medisch Contact*, 27 mei 2010, 65: 21: 949-951.

Brennan, S. (2005) *The NHS IT Project – The biggest computer programme in the World... ever!*, Oxford: Radcliffe Publishing.

College Bescherming Persoonsgegevens (2009) *Wijziging Kaderwet elektronische zorginformatieuitwisseling*, z2009-00581.

Commission of the European Communities (COM) (2004) e-Health – making healthcare better for European citizens: An action plan for a European eHealth Area, Brussel, 30.4.2004, COM (2004) 356 final.

Corrigan, O. (2003) Empty ethics: the problem with informed consent, *Sociology of Health & Illnes*, vol. 25:3, 2005:768-792.

Dalen, J. van & R. Stegwee (2006) 'Generatiekloof dreigt bij invoering EPD', ZM 11:23.

Dekker, B.P. & A. Hendriks (2009) De juridische gevolgen van het EPD voor u en uw dokter, *Nederlands Juristenblad*, 04-12-2009, afl. 42:2759-2763.

Department of Health (2010) press release Department of Health United Kingdom 09-09-

2010, www.dh.gov.uk/en/MediaCentre/Pressreleases/DH_119293 , geraadpleegd op 08-10-2010.

Dijstelbloem, H., P.L. Meurs & E.K. Schrijvers (red.) (2004) *Maatschappelijke dienstverlening. Een onderzoek naar vijf sectoren*, WRR-verkenningen 6, Amsterdam: Amsterdam University Press.

Eerste Kamer, 2009-2010a, 31466 C, memorie van antwoord, 7 september 2009.

Eerste Kamer, 2009-2010b, 31 466 L, motie Slagter-Roukema c.s.

Eerste Kamer, 2009-2010c, 31466 E, verslag ronde tafel gesprek 9 december 2009.

Eerste Kamer, 2009-2010d, 31 466 F, verslag ronde tafel gesprek 22 maart 2010.

Eerste Kamer, 2010-2011, 31466 P, brief minister van VWS, 5 oktober 2010.

Evers, C. (2008) *Privacyschending in de geestelijke gezondheidszorg?!*, Utrecht: Kennispunt Recht, Economie, Bestuur en Organisatie, Universiteit Utrecht.

Eysenbach, G. (2001) What is e-health?, *Journal of Medical Internet Research*, Vol 3(2), April/June 2001.

Eysenbach, G. & C. Köhler (2002) How do consumers search for and appraise health information on the World wide web? Qualitative study using focus groups, usability tests and in-depth interviews, *BJM*, vol. 324 (7337): 573-577.

Frissen, V., M. van Staden, N. Huijboom, B. Kotterink, S. Huveneers, M. Kuipersen, G. Bodea (2008) *Naar een "User Generated State"? De impact van nieuwe media voor overheid en openbaar bestuur,* in opdracht van het Ministerie van BZK, Den Haag: TNO.

Halamka, J.D., K.D. Mandl & P.C. Tang (2008) Early experiences with Personal Health Records, *Journal of the American Medical Informatics Association*, vol 13(2): 121-126.

Henwood, F., S. Wyatt, A. Hart & J. Smith (2003) 'Ignorance is bliss sometimes': constraints on the emergence of the 'informed patient' in the changing landscapes of health information, *Sociology of Health & Illnes*, Vol.25:6, 2003: 589-607.

High Level Committee on Health (2003) Health Telematics Working Group of the High Level Committee on Health: Final Report, HLCH/2003/1/7.

House of Commons Public Accounts Committee (2009), The National Programme for IT in the NHS: Progress since 2006, Second Report of Session 2008-2009, HC 153, London: The Stationary Office Limited.

Hurenkamp, M. & M. Kremer (red.) (2005) *Vrijheid verplicht. Over tevredenheid en de grenzen van keuzevrijheid*, Amsterdam: Van Gennip.

Jacobs, B. (2010) 'Het elektronisch patiëntendossier vanuit informatiebeveiligingsperspectief', G. Munnichs, M. Schuijff en M. Besters (red), *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.

Katzenbauer, M. (2009) Te vroeg voor landelijk EPD, *Medisch Contact*, nr. 20, 14 mei 2009: 880-883.

Kivits, J. (2009) Everyday health and the internet: a mediated health perspective on health information seeking, *Sociology of Health & Illnes*, vol. 31:5, 2009: 673-678.

Kling, R. (1991) Computerization and Social Transformation, *Science, Technology & Human Values*, vol.16, no.3 (Summer, 1991): 342-367, Sage.

Knottnerus, J. A. (1999) 'Role of the electronic patient record in the development of general

practice in the Netherlands', *Methods of information in Medicine*, 38: 350-354.
Mager, A. (2009) Mediated health: sociotechnical practices of providing and using online health information, *New Media & Society*, Sage Publication, vol 11(7): 1-20.
Medisch Contact (2010) Bewaartermijn patiëntendossier moet langer, *Medisch Contact* 65, nr. 14: 650.
Meyst-Michels, J. & S. Tiems (2009) Meer schadeclaims door EPD, *Medisch Contact*, 64 nr. 22, 28 mei 2009: 991-995.
Ministerie van VWS (2000) *Beleidsbrief en Actieplan ICT in de Zorg* (kenmerk: BIO&ICT 2133997), Den Haag: Ministerie VWS.
Munnichs, G., M. Schuijff & M. Besters (red.) (2010) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie*, Den Haag: Rathenau Instituut.
Nettleton, S. (2004), The Emergence of E-Scaped Medicine?, *Sociology*, vol. 38:4: 661-679.
New Scientist, *Avatar therapy: From couch to cyberspace*, 23 september 2010: 44-45.
NHG (2004) *Richtlijn Adequate Dossiervorming met het Elektronisch Medisch Dossier*.
NHG (2009) *Richtlijn Adequate Dossiervorming met het Elektronisch Medisch Dossier*. Aanvulling over Episodegericht registreren.
Nictiz (2008) *ICT in de zorg. Resultaten, ontwikkelingen en agenda*, mei 2008.
NPCF (2008) *Gezondheid 2.0 Toekomst en betekenis van e-health voor de zorgconsument, Visiedocument*, mei 2008, Utrecht.
NPCF (2009) *Notitie ten behoeve van expertmeeting Eerste Kamer*, Utrecht: NCPF.
NRC Handelsblad (2009) *OM opent onderzoek naar Neuroloog*, 17 januari 2009.
NRC Handelsblad (2010) *CZ mag lijst prestaties ziekenhuizen nog niet publiceren*, 30 september 2010.
Oudshoorn, N. & A. Somers (2006) Constructing the digital patient. Patient organizations and the development of health websites, *Information, Communication & Society*, vol.9, no.5: 657-675.
Petersen, A. (2005) Securing our genetic health: engendering trust in UK Biobank, *Sociology of Health & Illnes*, vol. 27:2, 2005: 271-292.
Ploem, M.C. (2004) *Tussen privacy en wetenschapsvrijheid. Regulering van gegevensverwerking voor medisch-wetenschappelijk onderzoek*, Sdu Uitgevers, reeks gezondheidrecht 24.
Pluut, B. (2010), *Het landelijk EPD als black box. Besluitvorming en opinies in kaart*, Den Haag: WRR.
Pluut, B. & A. Zuurmond (2009) *Changing perspectives in informatics? A comparison of three national electronic health records*, paper for International Conference on Health Informatics.
Protti, D., I. Johansen, F. Perrez-Torres (2009) Comparing the application of Health Information Technology in primary care in Denmark, *International Journal of Medical Informatics*, 78 (2209): 270-283.
Raad voor Volksgezondheid en Zorg (2002) *Inzicht in e-health*, Zoetermeer 2002.
Rathenau Instituut (1998), *De nacht schreef rood. Informatisering van zorgpraktijken*, Rathenau studie 27, Den Haag: Rathenau Instituut.
Rathenau Instituut (2005) *Bericht aan het parlement. De politiek en zorg van alledag*,

november 2005, Den Haag: Rathenau Instituut.
Rathenau Instituut (2009a) *Startnotitie expertmeeting elektronisch patiëntendossier*, 9 december 2009, Den Haag: Rathenau Instituut.
Rathenau Instituut (2009b) *Inleiding op de thema's, notitie t.b.v. expertmeeting elektronisch Patiëntendossier,* Eerste Kamer, 9 december 2009, Den Haag: Rathenau Instituut.
Rathenau Instituut (2009c) *Presentatie focusgroepen EPD door Rathenau Instituut, expertmeeting EPD,* Eerste Kamer, 9 december 2009, Den Haag: Rathenau Instituut.
Sackett, D.L., W.M.C. Rosenberg, J.A. Muir Gray, R.B. Haynes & W. Scott Richardson (1996) 'Evidence based medicine: what it is and what it isn't, *British Medical Journal*, 312: 71-72.
Staatscommissie Koopmans (1976) *Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistraties*, Den Haag: Staatsuitgeverij.
Sulik, G.A. (2009) Managing biomedical uncertainty: the technoscientific illness identity, *Sociology of Health & Illness*, vol. 30: 7, 2009: 1059-1076.
Tiemeijer, W.L., C.A. Thomas & H.M. Prast (red.) (2009), *De menselijke beslisser. Over de psychologie van keuze en gedrag*, WRR-verkenningen 22, Amsterdam: Amsterdam University Press.
Timmermans, S. & M. Berg (2003) *The Gold Standard – The Challenge of Evidence-Based Medicine and Standardization in Health Care*, Philadelphia: Temple University Press.
TNO (2009) *Public Services 2.0: The impact of social computing on public services*, EUR 24080 – 2009, serie: JRC scientific and technical reports.
Trappenburg, M. (2008) *Genoeg is genoeg. Over gezondheidszorg en democratie*, Amsterdam: Amsterdam University Press.
Tweede Kamer, vergaderjaar 1997-1998, 25 669, nr. 2.
Tweede Kamer, vergaderjaar 2004-2005, 27529, nr. 14.
Tweede Kamer, vergaderjaar 2007-2008, *Memorie van Toelichting*, 31 466, nr. 3
Tweede Kamer, vergaderjaar 2008-2009a, *Brief van de minister van VWS over het elektronisch patiëntendossier*, 31 466, nr. 10.
Tweede Kamer, vergaderjaar 2008-2009b, *Handelingen nr. 43*, 3769-3794.
Tweede Kamer, vergaderjaar 2008-2009c, *Handelingen nr. 45*, 3920-3959.
Tweede Kamer, vergaderjaar 2008-2009d, *Handelingen nr. 56*, 4485-4504.
Tweede Kamer, vergaderjaar 2008-2009e, *Handelingen nr. 57*, 4670-4672.
Tweede Kamer, vergaderjaar 2009-2010, *Vragen van het lid Zijlstra (VVD) over de beveiliging van het EPD*, Aanhangsel van de Handelingen 1173, 2485-2486.
Tweede Kamer, vergaderjaar 2010-2011, *Voortgangsrapportage*, 27527, nr. 61
Versteeg, W. & M. Hajer (2010) Van ondergraving naar ondervraging. Over de vormgeving van gezag in een gemediatiseerde wereld, in: H. Dijstelbloem, P. den Hoed, J.W. Holtslag & S. Schouten (red.), *Het gezicht van de publieke zaak*, Amsterdam, Amsterdam University Press, p. 333-362.
Volkskrant, de (2009) 'Je depressie mailen naar de psycholoog', 17 oktober 2009.
Volkskrant, de (2009) *Naar wie moeten we luisteren?*, 14 november 2009.

Volkskrant, de (2010) *Specialisten publiceren zelf cijfers borstkanker*, 08 oktober 2010.
Vorstenbosch, J. (2009) *Hoe maakt u het? Technologie in een veranderde gezondheidszorg. Over dossiers, robots en test in de zorg*, Den Haag: ZonMw.
Warners, J. (2009) De nieuwe wereld van DOT, het volledige profiel als incentive, *Tijdschrift voor Zorgadministratie en Informatie* 35, no. 137: 6-9.
Wetenschappelijke Raad voor het Regeringsbeleid (2011) *iOverheid*, Rapporten aan de Regering nr. 86, Amsterdam: Amsterdam University Press.
Zorgverzekeraars Nederland (2009) positiepaper ten behoeve van expertmeeting Eerste Kamer, 2 november 2009, www.eerstekamer.nl.

10 CHIEF INFORMATION OFFICERS BIJ DE RIJKSOVERHEID

Tamara Snijders

10.1 INLEIDING

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft in december 2008 aangekondigd dat in het tweede kwartaal van 2009 binnen alle ministeries een Chief Information Officer (CIO) moet zijn aangesteld ter verbetering van de positionering en kwaliteit van het informatiemanagement bij de rijksoverheid. Het instellen van deze rol op hoog ambtelijk niveau moet bijdragen aan betere sturing en beheersing van grote ICT-projecten[1], betere organisatie en inrichting van het opdrachtgeverschap binnen de ministeries en verbetering van de ambtelijke advisering aan bewindspersonen. De wijze waarop de ministeries deze rol beleggen is vormvrij, de taken, verantwoordelijkheden en bevoegdheden die de rol met zich meebrengt heeft de minister echter wel voor een groot deel bepaald. De directe aanleiding voor aanstelling van de CIO's zijn de vele problemen met ICT-projecten bij de overheid.

Het doel van deze studie is het werkveld van de CIO's bij de rijksoverheid in kaart te brengen. Hiervoor wordt in paragraaf 10.2 nader ingegaan op de vraag naar de aanleiding voor het aanstellen van de CIO's. Het probleem dat geleid heeft tot deze aanstelling en de taken en bevoegdheden die de CIO heeft gekregen om dit probleem bij de staart te vatten worden daar ook besproken. Tevens wordt de literatuur geraadpleegd en getracht inzicht te geven in de heersende opvattingen over de aanstelling van een CIO, zijn of haar mogelijke bijdrage aan een verbetering van het informatiemanagement van een organisatie en de taken en bevoegdheden die daarbij horen.

Paragraaf 10.3 geeft de huidige praktijk van de CIO's bij de verschillende departementen weer. Deze is geschreven op basis van interviews met twaalf CIO's op rijksniveau. De verschillende aspecten in het werkveld van de CIO komen aan de orde. Tevens wordt een beeld geschetst van de ervaringen in de rol van CIO en de invulling die zij in de praktijk aan hun rol geven.

In de vierde paragraaf volgen de conclusies die getrokken kunnen worden op basis van de theorie en de praktijk bij de Nederlandse overheid. Daarnaast wordt een en ander kort vergeleken met de ervaringen met de rol van CIO bij de Amerikaanse federale overheid.

10.2 EEN THEORETISCHE KIJK OP DE ROL VAN DE CIO

Na uitlatingen van een aantal ICT-deskundigen over de verspilling van de Nederlandse overheid aan ICT-projecten (Verhoef 2009) en de hierop volgende motie van Tweede Kamerlid Gerkens (Kamerstukken 2006/07) stelt de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties op 29 juni 2007 voor de Algemene Rekenkamer een onderzoek te laten instellen "naar de omvang van de verspilling door de rijksoverheid van ICT-projecten en de achterliggende oorzaken hiervan" (Kamerstukken 2006/07a: 1). De vaste commissie wil te weten komen wat de belangrijkste achterliggende oorzaken zijn van problemen met ICT-projecten bij de rijksoverheid en hoe het gesteld is met de kwaliteit van de informatievoorziening over deze projecten aan de Tweede Kamer. Men vraagt de Rekenkamer over beide elementen aanbevelingen te doen (Kamerstukken 2006/07a). Tot slot gaat de interesse van de commissie uit naar de wijze waarop doelmatigheid en doeltreffendheid van de uitgaven voor ICT-projecten wordt bijgehouden in de administraties, naar een indicatie van vermijdbare kosten en vertragingen en vraagt men de Algemene Rekenkamer uitspraak te doen over de mogelijkheden en beperkingen van een breed onderzoek hiernaar (Kamerstukken 2006/07a).

In het onderzoek naar de oorzaken van problemen met ICT-projecten vraagt de commissie de Rekenkamer specifiek in te gaan op de mate van "professioneel opdrachtgeverschap", waarbij de commissie aangeeft te denken aan "contracten, aanbestedingsregels en -procedures, leveranciersmanagement enzovoorts" (Kamerstukken 2006/07a: 2). Verder wordt gevraagd in hoeverre samenwerkingsaspecten, de gekozen projectaansturing en -beheersing en de bestuurlijke besluitvorming (zoals wijzigingen in wet- en regelgeving) leiden tot problemen met ICT-projecten. Ook vraagt de vaste commissie de Rekenkamer te kijken naar de mate waarin sprake is van *"*voldoende risicomanagement (inventarisatie, analyse en beheersing van risico's)*"* (Kamerstukken 2006/07a: 2). Tot slot verzoekt de commissie de Algemene Rekenkamer een verdiepingsonderzoek uit te voeren om inzicht te verschaffen in kosten, doorlooptijden en resultaten van een aantal grote ICT-projecten. De bedoeling is dat de commissie een volledig beeld krijgt van de vermijdbare overschrijdingen van kosten en planning bij deze projecten (Kamerstukken 2006/07a).

10.2.1 ONDERZOEK ALGEMENE REKENKAMER

Op 7 augustus 2007 zegt de Algemene Rekenkamer toe het onderzoek uit te voeren en hierover in twee delen te rapporteren. Het eerste deel van het rapport presenteert zij op 29 november 2007 aan de Tweede Kamer, de verdieping volgt op 25 juni 2008 (Kamerstukken 2006/07c-d).

Oorzaken verspilling ICT-projecten

De Algemene Rekenkamer stelt in deel A van het rapport *Lessen uit ICT-projecten bij de overheid* dat de rijksoverheid de neiging heeft ICT-projecten te complex te maken. De hoge politieke ambities en politieke besluitvorming spelen een rol bij de problemen met ICT-projecten. Kosten en doorlooptijden van deze projecten lopen nogal eens uit de hand en de opgeleverde resultaten voldoen niet altijd aan de verwachtingen. De Rekenkamer wijst hiervoor twee oorzaken aan.

Een eerste oorzaak is de gebrekkige informatievoorziening van de betrokken ministers naar de Tweede Kamer. Hierdoor bestaat onvoldoende mogelijkheid de projecten voor aanvang te toetsen, de voortgang ervan te monitoren en de projecten te evalueren (Algemene Rekenkamer 2007).

Een tweede oorzaak die de Rekenkamer noemt is dat ICT-projecten bij de rijksoverheid te ambitieus en complex zijn door een continue spanning tussen de politieke, organisatorische en technische factoren van een project. Aan politieke zijde is volgens de Rekenkamer sprake van een zogenoemd 'ICT-enthousiasme' van bestuurders, onrealistische politieke deadlines en onvoldoende gelegenheid tot heroverwegingen gedurende de projecten. De organisatie van deze projecten brengt met zich mee dat verschillende (autonome) organisaties betrokken zijn en dat men onvoldoende oog heeft voor de impact van een ICT-project op de organisatie. Ook de doelen en eisen van projecten blijken onvoldoende gespecificeerd, de benodigde aansluiting op andere systemen brengt niet zelden problemen met zich mee en de overheid is nauwelijks in staat de razendsnelle ontwikkelingen op ICT-gebied bij te benen. Deze spanning tussen politieke, organisatorische en technische factoren leidt ertoe dat er geen balans is tussen de gestelde ambitie en de beschikbare mensen, middelen en tijd (Algemene Rekenkamer 2007).

Besturing projecten professionaliseren

In deel B van het rapport *Lessen uit ICT-projecten bij de overheid* geeft de Algemene Rekenkamer aan dat *"*een minimale set aan informatie nodig is om zicht te kunnen hebben op de voortgang van een ICT-project en om hierop te kunnen sturen. Maar om daadwerkelijk te komen tot realistische ambities en grip op ICT-projecten is meer nodig, vooral op het terrein van de besturing*"* (Algemene Rekenkamer 2008: 53). Om de besturing van projecten te professionaliseren heeft de Algemene Rekenkamer een aantal aandachtspunten geformuleerd.

Een eerste aandachtspunt heeft betrekking op de inhoud van projecten. De Rekenkamer geeft aan dat het van belang is te zorgen voor samenhang tussen een organisatievraagstuk en de informatievoorziening: *"*de strategie en architectuurontwikkeling*"* (Algemene Rekenkamer 2008: 53). Het primaire proces van een organisatie – bij ministeries zijn dit veelal beleidsafdelingen – moet richtinggevend zijn bij de besluitvorming over informatievoorziening en ICT.

Een tweede aandachtspunt betreft de besturing van projecten (Algemene Rekenkamer 2008). Professionele besturing van een projectenportfolio houdt volgens de Rekenkamer in dat organisaties de wijze van besluitvorming over de informatievoorziening en ICT dienen te organiseren. Er moet nagedacht worden over op welk niveau bepaalde beslissingen worden genomen en welke informatie hiervoor vereist is. Onderdeel van portfoliomanagement is ook dat men realistische prioriteiten stelt op basis van de beschikbare mensen, middelen en tijd. En dat projectvoorstellen beoordeeld dienen te worden op basis van fasering, onderbouwing, ondersteuning door een businesscase, inschatting van de impact per project en in samenhang met andere projecten. Tot slot behoort ook een regelmatige review van projecten tot de professionele besturing van de projectenportfolio (Algemene Rekenkamer 2008).

Een volgend aandachtspunt dat de Rekenkamer noemt, is het vormgeven van leveranciersmanagement. "Leveranciersmanagement betekent dat de organisatie bepaalt hoe en op welke plek of plekken in de organisatie het contact met leveranciers en de selectie plaatsvindt. Ook gaat leveranciersmanagement over expertise en afspraken over aanbestedingen, *sourcing*[2] en andere inkooponderwerpen" (Algemene Rekenkamer 2008).

Het laatste aandachtspunt om de besturing van ICT-projecten te professionaliseren heeft betrekking op de CIO-functie. Bij het organiseren van de besluitvorming rondom ICT-projecten geeft de Rekenkamer aan een persoon te benoemen die de besluiten moet nemen en richt zich hierbij op de Chief Information Officer (CIO). "Door het aanstellen van een CIO plaatst de organisatie het onderwerp informatiemanagement op de agenda van het bestuurlijke niveau van de organisatie" (Algemene Rekenkamer 2008: 59). Een CIO vormt als het ware een schakel tussen organisatievraagstukken en informatievoorziening. "ICT is nu vaak iets van de 'ICT'ers' alleen, terwijl de informatievoorziening en de daarbij behorende ICT veelal grotere impact heeft op de processen in een organisatie en daarom juist de business aangaat" (Algemene Rekenkamer 2008: 59-60). De Algemene Rekenkamer geeft aan dat het voor de CIO van groot belang is dat hij het vertrouwen krijgt van bestuurders en op hetzelfde niveau acteert, maar daarnaast ook inzicht heeft in organisatieprocessen en de mogelijke problematiek rondom de informatievoorziening van de organisatie. Naast het aanstellen van de CIO is het van belang ook op andere niveaus in de organisatie een dergelijke schakelfunctie te creëren. De voornaamste taak van de CIO is het organiseren van een professionele besturing van projecten. Hierbij valt te denken aan strategie- en architectuurontwikkeling, portfoliomanagement, positie en taken afhankelijk van strategisch belang van informatievoorziening voor processen van een organisatie en van de organisatiestructuur (Algemene Rekenkamer 2008).

10.2.2 MAATREGELEN VAN HET KABINET

De rapporten van de Algemene Rekenkamer leiden voor de minister van Binnenlandse Zaken en Koninkrijksrelaties tot de conclusie dat de rijksdienst onvoldoende professioneel ingericht is om grote projecten met een ICT-component tot een goed einde te brengen en binnen de geraamde tijd en budgetten af te ronden. Deze constatering en het besef dat informatie- en communicatietechnologie een steeds belangrijkere rol gaan spelen in de primaire en secundaire werkprocessen van de ministeries waren voor het kabinet de aanleiding om toe te werken naar "een aan professionele standaarden voldoend informatiemanagement, waaronder het opdrachtgeverschap voor (grote) projecten" (Kamerstukken 2007/08a: 2).

Om dit te kunnen realiseren acht het kabinet het noodzakelijk om bij alle ministeries centraal en op hoog ambtelijk niveau een CIO-rol belegd te zien. "Grote ICT-projecten worden veelal ontwikkeld en aangestuurd vanuit beleidsdirecties, niet altijd met centraal toezicht of advisering" (Kamerstukken 2007/08a: 2). De wijze waarop de departementen de rol van CIO in de organisatie beleggen is vormvrij. De integrale managementverantwoordelijkheid van beleidsdirecties voor ICT-projecten blijft gehandhaafd, maar zij kunnen geen nieuwe, grote ICT-projecten starten zonder het oordeel van de CIO (Kamerstukken 2007/08a).

Op basis van het advies van de Algemene Rekenkamer deelt het kabinet een aantal taken en bevoegdheden toe aan iedere departementale CIO (Kamerstukken 2007/08a). Het is de bedoeling dat een CIO de ambtelijke en politieke leiding gevraagd en ongevraagd adviseert over de doelstelling, uitvoering, kosten en risico's van grote ICT-projecten. Daarnaast geeft de CIO een oordeel over de start van ICT-projecten en op kritieke momenten tijdens de uitvoering daarvan. De CIO functioneert als opdrachtgever namens de bestuursraad voor generieke departementale ICT-voorzieningen. Verder is de CIO verantwoordelijk voor het opstellen en actueel houden van de departementale strategie en visie op geautomatiseerde informatievoorziening en ICT. De CIO ontwikkelt en onderhoudt, vanuit de rijksbreed afgesproken kaders, de departementale architectuur en standaarden en is verantwoordelijk voor het toezicht op de naleving van de rijksbrede kaders binnen het ministerie. Ook bewaakt de CIO de samenhang in informatievoorziening en ICT-projecten binnen een ministerie door applicatie- en projectenportfoliomanagement. Hij of zij stelt, op basis van de rijksbrede kaders, eisen aan methodieken voor projectbeheersing en ondersteunt *audits*, *reviews* en *second opinions*. Tot slot is de CIO bevoegd voorstellen aan de bestuursraad te doen over de start van grote ICT-projecten of eventuele opschorting of bijsturing tijdens de uitvoering daarvan (Kamerstukken 2007/08a).

Het kabinet legt de verantwoordelijkheid voor realisatie, borging, onderhoud, ontwikkeling en toepassing van rijksbrede architectuur en instrumenten bij het

directoraat-generaal Organisatie en Bedrijfsvoering Rijk (DGOBR) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), meer specifiek in handen van het CIO-beraad. "Dit beraad coördineert de informatievoorziening en het ICT-beleid van de rijksdienst, borgt het rijksbrede beleid, en doet voorstellen voor de ontwikkeling van nieuwe kaders en standaarden" (Kamerstukken 2007/08a: 3). De directeur Informatiseringbeleid Rijk is voorzitter van het beraad, met de departementale CIO's als leden. Daarnaast vervult hij de rol van centrale CIO voor het rijk en is hij opdrachtgever voor rijksbrede projecten (Kamerstukken 2007/08a).

Het kabinet geeft aan er bewust niet voor te kiezen om één minister verantwoordelijk te maken voor alle ICT-projecten. ICT-projecten van een ministerie vallen onder verantwoordelijkheid van de betreffende minister. De minister van Binnenlandse Zaken en Koninkrijksrelaties neemt de zorg voor verbetering van de kwaliteit van het opdrachtgeverschap op zich. "De rol van de minister van BZK betreft een systeemverantwoordelijkheid, met als speerpunten de kwaliteit van de aansturing van grote ICT-projecten en de kwaliteit van de zogenaamde I-kolom[3] binnen de ministeries" (Kamerstukken 2007/08: 2).

Het aanstellen van CIO's is een van de maatregelen, maar in de ogen van het kabinet niet voldoende om de positie en de kwaliteit van het informatiemanagement bij de rijksoverheid te verbeteren. Om te komen tot een professionalisering van het informatiemanagement acht het kabinet het tevens noodzakelijk om de kwaliteit van het opdrachtgeverschap en de informatievoorziening bij de beleidsdirecties te vergroten. "Professionalisering van het informatiemanagement, waaronder opdrachtgeverschap, vanuit de beleidsdirecties is minstens zo belangrijk als een goede inrichting van de CIO-functie" (Kamerstukken 2007/08a: 3).

Het kabinet stelt een aantal kaderstellende maatregelen voor die moeten bijdragen aan een betere borging van de kwaliteit van grote ICT-projecten bij de beleidsdirecties van ministeries. Het gaat hierbij om eisen aan een projectplan dat ten grondslag moet liggen aan de start van een project, tussentijdse reviews op de voortgang van een project, het werken met eenduidige standaarden, architectuur en interoperabiliteit (Kamerstukken 2007/08). Al deze maatregelen zijn erop gericht de kwaliteit en positionering van het informatiemanagement bij de rijksoverheid te verbeteren (Kamerstukken 2007/08).

Ter verbetering van het opdrachtgeverschap binnen ministeries en aansturing van externen geeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aan dat het kabinet voornemens is op korte termijn een curriculum te ontwikkelen. Hierin komen zaken aan de orde als "opdrachtgeverschap, verander- en innovatiemanagement, inhoudelijke kennis van I-beleid[4] en ICT-toepassingen, en programma- en projectmanagement" (Kamerstukken 2007/08a: 4).

Tot slot geeft de minister van Binnenlandse Zaken enKoninkrijksrelaties aan dat het tijdig betrekken van marktpartijen van belang is voor het slagen van ICT-projecten. Middels een ICT-haalbaarheidstoets en een concurrentiegerichte dialoog kunnen project- en programmaorganisaties wederzijdse verwachtingen tijdig verkennen en ervoor zorgen dat "bij de overheidsorganisatie én bij het ICT-bedrijfsleven een gedeeld beeld aanwezig is over het doel, de aanpak en de uitvoering" (Kamerstukken 2007/08: 6). Dit vergoot de slagingskans van ICT-projecten (Kamerstukken 2007/08). Ook reikt de minister een standaardmodel aan voor rapportages over de projecten en de administratie van kosten (Kamerstukken 2007/08).

10.2.3 INFORMATIEMANAGEMENT EN DE ROL VAN DE CIO

Informatie wordt steeds belangrijker in het primaire proces van overheidsorganisaties. In het bijzonder uitvoerende diensten zijn veelal erg informatie-intensief (Te Velde et al. 2005). Steeds vaker wordt technologie (dikwijls ICT) ingezet om deze informatie te kunnen benutten of managen. Onder invloed van ontwikkelingen op het gebied van technologie treden veranderingen op in de inrichting van overheidsorganisaties. Bureaucratieën ontwikkelen zich richting een 'infocratie', doordat overheidstaken complexer worden en met elkaar verweven raken. Evenals hun werkende systemen, standaarden en sturing. 'Oude' organisatiestructuren volstaan niet meer (Zuurmond & Meesters 2005).

Fasen van informatisering

Een klassiek model om de veranderende rol van informatie en technologie in een organisatie te omschrijven is het model van Nolan (Te Velde et al. 2005; Zuurmond 1998; Zuurmond 2003). Dit beschrijft een aantal fasen in de ontwikkeling van de rol van informatie en technologie voor organisaties. De eerste fase is die van automatisering van informatie-intensieve processen, waarbij kostenbesparing de belangrijkste doelstelling is. De automatisering is nog vooral iets 'mysterieus' en iets van 'ICT-deskundigen' dat zich afspeelt in de bedrijfsvoeringskolom van de organisatie. Er kan gesproken worden van een flinke afstand tussen het primaire proces van de organisatie en het domein van de informatie(technologie). In de literatuur wordt veelal gesproken van het domein van de organisatie (Te Velde et al. 2005) of de (core) business (Henderson & Venkatraman 1999; Maes 2003). In het geval van de rijksoverheid kan hier gesproken worden van het primaire proces van een (beleids)departement of uitvoeringsorganisatie.

In de volgende fase van het model van Nolan raakt informatietechnologie langzaam geïntegreerd in de primaire processen van de organisatie en raken verschillende functies van de organisatie met elkaar vervlochten. De beide domeinen (primair proces en informatie(technologie)) komen dichter bij elkaar te staan. De nadruk ligt op een procesgerichte in plaats van functionele inrichting van orga-

nisaties (*business process redesign*). Het belang van een verbinding tussen het domein van de organisatie en het domein van de informatie en technologie wordt ingezien en informatietechnologie gaat een rol spelen in het bepalen van de organisatiestrategie, inrichting en processen. De Chief Information Officer wordt in deze fase geïntroduceerd als bruggenbouwer (Te Velde et al. 2005; Zuurmond 1998; Zuurmond 2003).

In het oorspronkelijke model van Nolan is de derde en laatste fase de netwerkfase. Informatie wordt in deze fase van steeds duidelijker strategisch belang en gaat over de grenzen van de organisatie heen. Er is in deze fase sprake van een volledige integratie van informatietechnologie met het primaire proces van de organisatie. De CIO is niet langer nodig om het onder de aandacht van de leiding van een organisatie te brengen en het gat tussen de organisatie en technologie te dichten. Zuurmond (1998, 2003) brengt een nader onderscheid aan door de laatste fase in drieën te splitsen. Ten eerste (fase 3a) breidt informatisering zich uit buiten de organisatie in de sector en vindt in toenemende mate informatie-uitwisseling plaats via sectorale infrastructuren. Vervolgens (fase 3b) is sprake van intersectorale of nationale standaardisatie en informatie-uitwisseling en in de laatste fase (3c) is sprake van informatie-uitwisseling op internationaal niveau (Te Velde et al. 2005; Zuurmond 1998; Zuurmond 2003).

Informatisering bij de overheid

Kijkend naar de rijksoverheid kan gesteld worden dat zij zich reeds in een fase bevindt waarbij uitwisseling van informatie op grote schaal over de grenzen van sectoren heen gaat. Ook landsgrenzen worden door de inzet van technologie steeds vaker overschreden voor de uitwisseling van informatie. Kortom, de rijksoverheid bevindt zich in een verregaand stadium van informatisering. Hierbij speelt de inzet van technologie vanzelfsprekend een toonaangevende rol. Daar staat echter tegenover dat de CIO bij de rijksoverheid in veel gevallen pas een jaar geleden is aangesteld. Voorzichtig kan dus gesteld worden dat de maatregelen in termen van sturing en inrichting van de organisatie hier enigszins achter lijken te lopen op de realiteit van verregaande informatisering.

De inzet van informatietechnologie door de overheid is in twee delen te splitsen. Enerzijds zet de overheid informatietechnologie in om haar interne processen te stroomlijnen. Anderzijds wordt informatietechnologie ingezet in de uitvoering van overheidsbeleid. In dit laatste geval kan de inzet van ICT direct van invloed zijn op haar relatie met burgers, bedrijven en andere stakeholders. In dergelijke gevallen zijn het primaire proces van een organisatie en de ICT zichtbaar geïntegreerd. Deze inzet van ICT ten gunste van de service van overheidsdiensten wordt in de literatuur veelal aangeduid als 'eGovernment' of 'eOverheid': "the use of modern information and communication technologies – currently especially internet and web technology – by a public organization to support or redefine the

existing and/or future information, communication and transaction relations with 'stakeholders' in the internal and external environment in order to create added value" (Bekkers & Homburg 2009: 217).

Uit deze definitie van eGovernment blijkt dat de kern van dit concept elektronische dienstverlening richting burgers, bedrijven en andere stakeholders behelst, onder de voorwaarde van toegevoegde waarde te zijn. Deze toegevoegde waarde kan bestaan uit: "increasing government accessibility, increasing the quality of service delivery, stimulating internal efficiency, supporting public and political accountability, and increasing the political participation of citizens" (Bekkers & Homburg 2009).

Veelgehoorde kritiek op de eGovernement-beweging is het uitgangsidee: "a new and better government [...] that is responsive as a whole" (Bekkers & Homburg 2009: 221). De doelen en uitdagingen waar de politiek zich voor stelt en het vermogen van de overheid om aan de gestelde doelen en uitdagingen te voldoen, lijken echter niet zelden behoorlijk uit elkaar te staan. eGovernment is geen zaak van implementatie van een blauwdruk voor een betere en responsievere overheid, maar eerder een ontwikkeling van de overheid die stukje bij beetje zal moeten plaatsvinden en vorm zal moeten krijgen (Bekkers & Homburg 2009).

Naast deze mythe van een nieuwe en betere overheid waarschuwen Bekkers & Homburg (2009: 225) voor het overmatige vertrouwen in "the power of ICT to realize effects that can lead to a revolution in government". Zij spreken van een "realm of evangelism about the good life ICT will bring" in beleidsdocumenten van de Nederlandse overheid (Bekkers & Homburg 2009: 226) en wijzen op het feit dat de effecten van de inzet van IT vaak slechts in een zeer specifieke context geplaatst kunnen worden.

Verder lijkt de nadruk in de Nederlandse beleidsstukken voornamelijk te liggen op het creëren van een virtueel serviceloket en wordt nauwelijks aandacht besteed aan de implementatie van een elektronische dienst en consequenties voor de organisatie (Bekkers & Homburg 2009). Dit roept de vraag op of we de overheid wel kunnen zien als een service georiënteerde organisatie en de burger als consument van deze overheidsservices (Zouridis & Thaens 2005). De burger als consument sluit niet aan op de uitgangspunten van een open en responsieve overheid. De rol van burger gaat immers verder dan de consument van overheidsdiensten, zij heeft ook een participerende rol in de democratie (Bekkers & Homburg 2009).

Tot slot kan opgemerkt worden dat zowel in beleidsstukken als literatuur over de eOverheid, de focus in sterke mate lijkt te liggen op het middel en de uitkomst. Namelijk de inzet van IT met het oog op verbeterde dienstverlening richting stake-

holders. Er bestaat slechts beperkte aandacht voor de beschouwing van het proces en de inrichting en sturing van dit proces. Genoemd wordt de voorwaarde van interoperabiliteit en de integratie van backoffices als kritische succesfactor voor eOverheid. Bij dit proces van herontwerpen en integreren van front- en backoffices wordt in de literatuur een aantal barrières opgemerkt. Vaak is sprake van coördinatieproblemen tussen de samenwerkende organisaties en krijgt men te maken met de verscheidenheid aan backoffices, de keerzijde van ICT die naast het faciliteren van verandering ook veel weerstand op kan roepen en de (wettelijke) grenzen aan het verzamelen, koppelen en bewerken van informatie (Van Venrooij 2002; OECD 2003; Bekkers & Homburg 2005). De vraag hoe deze problemen te overwinnen en het proces in te richten wordt in de literatuur slechts beperkt beantwoord. Aangehaald wordt dat de vaak gehanteerde klassieke benadering van projectmanagement niet langer houdbaar is. De oplossing wordt gevonden in het benaderen van initiatieven van eOverheid vanuit het procesmanagement in plaats van projectmanagement, zodat meer aandacht en ruimte is voor het bereiken van consensus en samenwerking (De Bruijn et al. 2002; Bekkers & Homburg 2005).

Informatiemanagement en het strategisch verbinden van eilanden

Uit en door de toenemende inzet van informatietechnologie is volgens Henderson en Venkatraman (1999) het begrip informatiemanagement ontstaan. Informatietechnologie en de ontwikkeling en toename van gebruik van deze technologie heeft ertoe bijgedragen dat men het belang is gaan inzien van het op de juiste manier omgaan met deze technologie. En de kansen en mogelijkheden die de inzet van informatietechnologie voor een organisatie met zich mee kan brengen. De praktijk van de informatietechnologie heeft zich als het ware omhooggewerkt en verplaatst van het niveau van de backoffice van een organisatie naar een strategischer niveau in de organisatie. Dit wordt ook wel *strategic management of information technology* genoemd (Henderson & Venkatraman 1999).

De verbinding tussen het informatie- en organisatiedomein voert duidelijk de boventoon in de literatuur over informatiemanagement. Henderson en Venkatraman (1999) stellen dat de kern van informatiemanagement is dat organisaties de 'business', oftewel het primaire proces, en informatietechnologie op één lijn moeten brengen om investeringen in informatietechnologie van waarde te kunnen laten zijn voor de organisatie.[5] Naast afstemming tussen de twee organisatiekolommen (*functional integration*) geven zij aan dat afstemming ook dient plaats te vinden tussen de verschillende organisatieniveaus. Het strategische en operationele domein van beide kolommen moeten hun werkzaamheden en plannen op elkaar afstemmen (*strategic fit*). Deze afstemming tussen kolommen en niveaus noemen Henderson en Venkatraman (1999) *strategic alignment*. Informatiemanagement wordt in deze discussie geduid als het managen van de relatie tussen het primaire proces van een organisatie en de informatietechnologie die hierin een rol speelt. Deze afstemming vindt plaats op twee niveaus, te weten een

strategisch niveau en een operationeel niveau, zowel in het primaire proces als in de ICT-kolom van een organisatie (Henderson & Venkatraman 1999).

Het definiëren van informatiemanagement als het managen van de afstemming tussen het primaire proces van de organisatie en het domein van de technologie, lijkt echter wat vaag en mist praktische handvatten (Maes 2003; Te Velde 2005). Het veronderstelt volledige maakbaarheid van beide domeinen en de mogelijkheid tot afstemming in de praktijk. Hoe de verbinding moet worden gelegd en de afstemming moet verlopen wordt uit het model niet duidelijk. Maes (2003) vult het strategic alignment-model aan door aan te geven dat de belangrijkste problemen van informatiemanagement zich afspelen in de verbinding tussen het primaire proces en technologie. Dit is waar informatiemanagement in een organisatie zich afspeelt. Hij stelt dat directe afstemming niet mogelijk is, omdat ICT niet direct ingrijpt op de business, maar ingrijpt via de informatie en communicatie tussen het primaire proces en technologie (Maes 2003; Maes 2008).

Daarnaast kan gesteld worden dat ook het onderscheid tussen operationeel en strategisch niveau in een organisatie wat mager is. De afstemming of verbinding tussen de strategie en de uitvoering speelt zich af op het gebied van inrichting en structuur: de vertaalslag die gemaakt wordt van een strategie richting uitvoering. Hieruit kan geconcludeerd worden dat informatiemanagement van invloed is op drie niveaus in een organisatie: op het primaire proces, op de besturing van de organisatie en op de strategische planning (Maes 2003; Te Velde et al. 2005).

Een derde kanttekening die bij het model van stategic alignment gemaakt kan worden is het gebrek aan aandacht voor betekenisgeving. Maes (2008) waarschuwt voor een door de technologie gedreven, vormelijke benadering van informatiemanagement. Hij geeft aan dat informatie centraal zou moeten staan en dat afstemming tussen kolommen en niveaus geen doel op zich mag worden. Het is van belang dat men oog houdt voor de mechanismen en processen waarin informatie, door de organisatie heen, strategische betekenis kan krijgen en dat voldoende ruimte is voor een blik naar buiten, voor initiatief en innovatie (Introna 1997; Maes 2008).

Op basis van de genoemde literatuur kan de kern van informatiemanagement worden omschreven als het stroomlijnen van het gebruik van informatie in een organisatie en het organiseren van het samenspel van organisatie, informatie en technologie. Met informatie als bron of middel voor een organisatie om haar doelen te bereiken. Het op een juiste manier managen van deze informatie kan vervolgens een essentiële bijdrage leveren aan de gestelde doelen of een voordeel opleveren ten opzichte van andere organisaties. Organisaties lijken vaak voldoende kennis en expertise in huis te hebben, maar lijden aan een gebrek aan inzicht in en organisatie van de eigen informatieprocessen.

De CIO als spin in het web

In de literatuur wordt de CIO aangewezen als "the highest ranking executive with primary responsibility for information management" (Synnott 1987: 19). De verbinder die op zoek gaat naar de samenhang in alle informatieprocessen van een organisatie, zonder de betekenis ervan uit het oog te verliezen en te inspireren tot innovatie (Kirk 1999; Maes 2003; Maes 2008). Een volgende stap in de literatuur is het afbakenen van de rol die de CIO zou moeten vervullen. Zo omschrijft Emery (1991: 9) de rol van CIO "as a senior executive with both a business and technical perspective, who can contribute actively to the formulation of an effective amalgamation of business and IS strategies."[6] In aanvulling hierop geeft Gupta (1991) aan dat de CIO drie kernverantwoordelijkheden heeft. Zo moet de CIO het overzicht houden van en over alle technologische toepassingen in de organisatie, rapporteert hij aan een hoge bestuurder en concentreert zich op het plannen van een langetermijnstrategie (Gupta 1991; Iyengar 2007).

In een aantal empirische studies wordt bevestigd dat de rol van CIO een ontwikkeling doormaakt en de aandacht steeds meer verlegd wordt van operationeel naar strategisch niveau. De CIO rapporteert in toenemende mate aan de hoogste bestuurder van de organisatie. Deze ontwikkelingen maken dat de CIO is uitgestegen boven het niveau van middelmanagement en zijn rol meer gaat lijken op die van een CEO of CFO (Applegate et al. 1992; Stephens et al. 1992; Iyengar 2007). Maes (2003) geeft echter aan dat de focus van het werk van een CIO in de praktijk bij verschillende organisaties toch vaak nog ligt op het stroomlijnen van het ICT-landschap van de betreffende organisatie. De zorg voor het strategisch inzetten van informatie zodat deze waarde creëert voor de organisatie, waarbij ICT een handig instrument kan zijn, krijgt hierbij onvoldoende aandacht. Een CIO lijkt eerder een Chief Technology Officer (CTO), omdat hij vooral bezig is met het afstemmen van de informatietechnologie op de eisen van het bedrijf en de business, waardoor hij niet toekomt aan het strategisch benutten van de informatie (Maes 2003). Organisaties met een onduidelijke visie op de invulling van de CIO-functie lopen het gevaar dat informatiemanagement nog altijd niet de aandacht en managementverantwoordelijkheid krijgt die het vereist. Het bestaan van een CIO-functie kan als doel op zich worden beschouwd, terwijl achterliggende bewustwording en processen achterblijven. Daarnaast is de kans groot dat de CIO in dergelijke organisaties eindigt met een aanzienlijke, maar onderschatte verantwoordelijkheid, in het beste geval enig gezag, maar geen macht (Maes 2003). De afkorting CIO dreigt in dergelijke gevallen te duiden op Commander of Impossible Operations (Verhoef 2009) of Career Is Over (Maes 2003).

Hofman en Tuin (2006) spreken, gebaseerd op marktonderzoek en praktijkervaring in de private sector, van een vijftal kenmerkende thema's waar CIO's vaak mee te maken krijgen en de taken en verantwoordelijkheden die daarbij horen. Allereerst halen zij het bundelen van ondersteunende bedrijfsprocessen aan, effecti-

viteit en efficiëntie staan hierbij voorop. De CIO vervult een trekkersrol in de realisatie en ontwikkeling van een centrum waarin deze processen gebundeld worden (*shared service centre*) (Hofman et al. 2006). Daarnaast wordt de CIO geacht te komen tot een businessgerichte bedrijfs-, informatie- en ICT-architectuur. Hiervoor moet hij zich een weg weten te banen door de veelal complexe applicatielandschappen van organisaties (Dullemen et al. 2006). Een ander probleem is de oneindige hoeveelheid wet- en regelgeving waarmee een CIO wordt overstelpt en die, zij het vaak indirect, invloed heeft op informatietechnologie. De CIO wordt geacht de samenhang te bewaken, de uitdaging van naleving aan te gaan en kan het gebruiken om kwaliteitsverbeteringen in de organisatie door te voeren (Van Burk et al. 2006). Verder is het de taak van de CIO te bepalen hoe de organisatie gestructureerd kan innoveren en een bijdrage te leveren aan het innoverend vermogen van een organisatie (Aalbers et al. 2006). Tot slot behoort de inrichting van *demand management* tot de taken van een CIO; hij dient helder te hebben wie nu wat wil van de CIO, hoe een en ander wordt vormgegeven en wat zijn relatie is tot de andere bedrijfsonderdelen (Fresz et al. 2006).

Samenvattend zou een CIO als primair verantwoordelijke voor informatiemanagement in een organisatie en de verbinding met alle aangrenzende domeinen de volgende zes rollen moeten vervullen (Maes 2003; Smaltz et al. 2006). Allereerst is een CIO een informatiestrateeg, die de organisatie verrijkt met een informatiestrategie. Een strategie waarin bedrijfs- en ICT-kansen worden meegenomen en informatie als bedrijfsmiddel centraal staat. De volgende rol is die van strategische businesspartner. De CIO schuift aan in de *boardroom*, oftewel de bestuursraad van een departement. Hij zit aan tafel bij de DG's en (plaatsvervangend) SG en levert een bijdrage aan de bedrijfsstrategie vanuit het oogpunt van strategisch inzetten van informatie als bedrijfsmiddel en de kansen en risico's van ICT. Een derde rol is die van de CIO als portfoliomanager. Als portfoliomanager is de CIO verantwoordelijk voor het langetermijnbeleid met betrekking tot ICT-aanbod. Hij onderhoudt de relatie met interne of externe aanbieders van ICT en is op de hoogte van ontwikkelingen in de markt. Ten vierde is de CIO organisatiearchitect die vanuit de strategie de informatie- en organisatiearchitectuur ontwikkelt. Daarnaast legt de CIO als adviseur van het primaire proces de verbinding tussen strategie en operatie. Daarvoor werkt hij samen met bijvoorbeeld informatiemanagers of directeuren van beleidsafdelingen en weet hen te verbinden, inspireren en coördineren. Tot slot dient de CIO op de hoogte te zijn van trends en ontwikkelingen die betrekking hebben op informatiegebruik en -management. Hij weet trends en ontwikkelingen op waarde te schatten en vervult zodoende de rol van trendwatcher.

10.2.4 EEN TUSSENSTAND

In deze paragraaf is toegelicht wat voorafging aan de aanstelling van CIO's bij de verschillende departementen van de rijksoverheid. Tevens is aangegeven wat de

aanstelling van deze CIO's behelst en welke taken en bevoegdheden hem zijn toegekend. Vervolgens is kort een blik geworpen op de literatuur over informatisering, informatiemanagement en de rol van een CIO.

Concluderend kan gesteld worden dat informatiemanagement, door de veranderende rol van informatie en technologie, van steeds groter belang wordt voor organisaties. De CIO is theoretisch gezien de hoogst verantwoordelijke voor informatiemanagement in een organisatie. Hij of zij opereert op bestuursniveau naast een CEO en een CFO. Empirische studies laten zien dat informatiemanagement en dus ook de CIO nog lang niet altijd de benodigde plaats en erkenning krijgen. Organisaties lijken de rol, positie en werking hiervan niet altijd goed te hebben doordacht. De CIO loopt het risico om als Chief Technology Officer of Commander of Impossible Operations te eindigen.

Kijkend naar de taakomschrijving van de CIO bij de rijksoverheid en de rollen die de literatuur aan de CIO voorschrijft, valt een aantal zaken op. Ten eerste ligt de nadruk bij de invulling van de rol van CIO door het kabinet sterk op de besturing van ICT-projecten en het bewaken van de samenhang en architectuur van het departementale ICT-landschap. Dit in tegenstelling tot de literatuur waar de primaire verantwoordelijkheid van een CIO veel breder bij informatiemanagement ligt en het verbinden van de verschillende onderdelen in een organisatie die hiermee te maken hebben. De CIO lijkt niet zozeer te worden neergezet als informatiestrateeg, maar als ICT-strateeg. Daarnaast zijn de rollen als strategisch bedrijfsadviseur en trendwatcher niet terug te vinden in de taakomschrijving van de CIO bij de rijksoverheid.

Hiervoor zijn zes rollen van een CIO benoemd: informatiestrateeg, strategisch bedrijfsadviseur, portfoliomanager, organisatiearchitect, adviseur van het primaire proces en trendwatcher. Deze zes rollen zullen hierna terugkomen om op basis van de empirie (paragraaf 10.3) conclusies te kunnen trekken over de rol van de CIO bij het rijk.

10.3 VAN ONTWERP NAAR UITVOERING: CIO'S BIJ HET RIJK

Deze paragraaf geeft een overzicht van de overeenkomsten en verschillen in de invulling van de rol en het werkveld van de CIO's bij de verschillende departementen van de rijksoverheid. Als input zijn in de periode van september 2009 tot en met maart 2010 de CIO's van twaalf van de veertien departementen van de rijksoverheid geïnterviewd.[7] Naast de gegevens uit de interviews is voor de analyse gebruikgemaakt van documenten die door de CIO's beschikbaar zijn gesteld.

10.3.1 IEDER DEPARTEMENT EEN CIO

Uit de interviews en documenten blijkt dat ieder departement inmiddels één of meerdere CIO's heeft aangesteld. Naast deze departementale CIO's is binnen het directoraat-generaal Organisatie en Bedrijfsvoering Rijk een zogenaamde rijks-CIO aangesteld. Uit de gesprekken komt naar voren dat de meeste CIO's in de eerste helft van 2009 met hun taken zijn gestart. Een enkel departement, onder meer Landbouw, Natuur en Voedselkwaliteit (LNV), Buitenlandse Zaken (BZ) en Financiën, werkte al langer met de functie van CIO, evenals enkele taakorganisaties van het ministerie van Justitie. Het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is het enige departement dat na de maatregelen van het kabinet een nieuwe functie heeft gecreëerd voor de CIO, die per 1 februari 2010 gestart is.

10.3.2 VERSCHILLENDE POSITIES

In de praktijk is de rol van CIO vaak neergelegd bij de (plaatsvervangend of hoofd) directeur bedrijfsvoering, informatisering of informatievoorziening. Bij drie departementen is de rol van CIO toebedeeld aan de secretaris-generaal (SG) of plaatsvervangend secretaris-generaal (PSG). Bij het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) is de rol van CIO in tweeën gedeeld en zijn twee CIO's aangesteld. De CIO-taken met betrekking tot de bedrijfsvoering zijn belegd bij de PSG. De SG vervult hier de rol van CIO voor de beleidsdirecties.

Tabel 10.1 Schematisch overzicht van de positie van de cio in de organisatie (september 2009-maart 2010)

CIO als functie	CIO als rol	
	Onderdeel van functie (p)SG	*Onderdeel van functie directeur*
Buitenlandse Zaken (BZ)	Onderwijs, Cultuur en Wetenschap (OCW)	Algemene Zaken (AZ)
Financiën / Belastingdienst[1]	Sociale Zaken en Werkgelegenheid[2] (SZW)	Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Landbouw, Natuur en Voedselkwaliteit (LNV)	Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer (VROM)	Economische Zaken (EZ)
Volksgezondheid, Welzijn en Sport (VWS)		Justitie
		Verkeer en Waterstaat (VenW)
		Defensie[3]

[1] De CIO van de Belastingdienst vervult naar buiten toe de rol van CIO voor het gehele departement. De plaatsvervangende CIO neemt in de dagelijkse praktijk de CIO-taken waar voor het kerndepartement.
[2] Geen interview plaatsgevonden op basis van deskresearch.
[3] Geen interview plaatsgevonden op basis van deskresearch.

De meeste CIO's geven in het interview aan dat de nieuwe rol onderdeel is geworden van het takenpakket van de functie die zij reeds bekleden. De rol van CIO is één van de twee of meerdere rollen die zij vervullen. Slechts bij vier ministeries is sprake van een 'volledige' CIO-functie, vaak wordt hier al sinds langere tijd de functie van hoofddirecteur als CIO ingevuld of is daadwerkelijk een functie gecreëerd voor de CIO. De CIO-functie is in deze gevallen ondergebracht bij een directie bedrijfsvoering, informatisering of informatievoorziening. In tabel 10.1 is schematisch weergegeven waar de rol van CIO bij de verschillende departementen ten tijde van de interviews (september 2009-maart 2010) was ondergebracht.

Kijkend naar de verschillen tussen de departementen wat betreft de positie van de CIO in de organisatie valt een aantal zaken op. Allereerst is sprake van een verschil in organisatieniveau. De titel CIO suggereert een plaats aan tafel bij de bestuursraad[8] van een organisatie, naast de CEO/SG, CFO en andere *chief officers*. De SG en pSG's die de rol van CIO vervullen nemen plaats in de bestuursraad en adviseren ook op dat niveau. De andere CIO's nemen doorgaans geen plaats in de bestuursraad. Tijdens de interviews kwam naar voren dat de CIO van Buitenlandse Zaken tot anderhalf jaar geleden in de bestuursraad plaatsnam. Doordat de focus van de bestuursraad meer verschoof naar beleid, nemen alle ondersteunende directeuren inmiddels geen plaats meer in de raad. Hiervoor in de plaats vormen de ondersteunende directeuren en plaatsvervangend DG's nu een managementraad. De CIO van LNV rapporteert periodiek aan de bestuursraad over de toptien van grote ICT-projecten van het departement. De CIO van de Belastingdienst neemt wel direct plaats in het managementteam van de dienst. De CIO van VWS en de geïnterviewde CIO's die naast hun rol als CIO ook directeur zijn, schuiven niet direct aan in de bestuurskamer. Zij adviseren aan een projectleider, beleidsverantwoordelijk directeur, DG of plaatsvervangend secretaris-generaal. De directeuren met een CIO-rol hebben met andere woorden dus te maken met één of meerdere hiërarchische lagen tussen hen en de bestuursraad.

De CIO's die tevens de functie van (plaatsvervangend) SG vervullen, geven aan zich in de praktijk in (interdepartementale) overleggen meestal te laten vertegenwoordigen door een plaatsvervanger. Het is opvallend dat men in deze departementen het belang van een CIO op een hoge ambtelijke positie lijkt te erkennen door de rol bij de (plaatsvervangend) SG onder te brengen. Door zich echter in de praktijk vrijwel permanent te laten vertegenwoordigen door een plaatsvervanger wordt de rol van CIO vrijwel onmiddellijk weer minder belangrijk gemaakt.

10.3.3 EEN NETWERK VAN CIO'S

Een aantal departementen heeft gekozen voor een netwerk van CIO's binnen het ministerie. Dit houdt veelal in dat op de verschillende niveaus in de organisatie of

bij de verschillende organisatieonderdelen CIO's zijn aangesteld, met één coördinerende CIO op departementaal niveau. De aanstelling van meerdere CIO's per organisatie komt vooral voor bij departementen met relatief zelfstandige organisatieonderdelen of uitvoeringsorganisaties. Tijdens de interviews kwam ter sprake dat men er bij het ministerie van Verkeer en Waterstaat voor heeft gekozen een CIO aan te stellen op bestuursniveau, één op departementaal niveau van bedrijfsvoering en één bij alle uitvoerende organisaties (Rijkswaterstaat, KNMI en Inspectie Verkeer en Waterstaat). Ook bij het ministerie van Justitie kent men een soortgelijke structuur met een departementale CIO en een CIO bij alle diensten (Openbaar Ministerie, Rechtspraak, Dienst Justitiële Inrichtingen en de Immigratie en Naturalisatiedienst). Tot slot zijn binnen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ook meerdere CIO's actief. Zo is voor het domein Veiligheid een aparte CIO benoemd en neemt de directeur Dienstverlening, Regeldruk en Informatiebeleid de CIO-taken waar op interbestuurlijk vlak (eOverheid) en in de verbinding met de burger. Daarnaast is een departementale CIO benoemd en valt ook de CIO rijk onder het ministerie van BZK.

De CIO's geven aan dat een dergelijk stelsel van CIO's op verschillende niveaus in de organisatie is ingesteld om de afstand te verkleinen tussen het primaire proces en de CIO-taken en op alle niveaus van de organisatie de typische CIO-thema's de benodigde aandacht te geven. Opvallend is dat een aantal taakorganisaties van het ministerie van Justitie al drie tot vijf jaar eerder een CIO heeft aangesteld. Deze CIO's zijn destijds aangesteld vanuit het primaire proces en moeten zich nu gaan voegen naar 'nieuwe' departementale en interdepartementale standaarden, ideeën en regels. Deze CIO's staan hier logischerwijs niet direct om te springen als het voor de organisatie zelf geen directe meerwaarde oplevert, het wel een forse investering vergt en er niet is voorzien in een mechanisme om de 'investeerders' te laten compenseren door de organisaties die de baten van deze interdepartementale afspraken ondervinden. De departementale CIO staat dan als het ware tussen deze twee vuren in. Enerzijds kost het soms moeite de taakorganisaties mee te krijgen, anderzijds kan het nodig zijn om in interdepartementaal verband voor de taakorganisaties op te komen. Zo haalt de heer Papenhuijzen, CIO bij het ministerie van Justitie, het voorbeeld van de Digitale Werkomgeving Rijk aan, ook de taakorganisaties worden geacht hieraan mee te werken: "Daar moet je ook weer overtuigend kunnen zijn in de meerwaarde en soms ook even, mede namens de uitvoeringsorganisaties, tegenspel bieden." Bij het ministerie van Verkeer en Waterstaat werkte men reeds met een organisatiebrede stuurgroep informatievoorziening. Deze stuurgroep is intact gelaten en de leden van de stuurgroep vervullen op dit moment de rol van CIO op hun niveau in de organisatie.

10.3.4 AFSTAND TOT BELEIDSDIRECTIES

Naast verschillen in niveau is sprake van een zekere afstand tussen de CIO en de beleidsdirecties van een ministerie. Door de rol van de CIO onder te brengen bij de directie of directeur bedrijfsvoering of informatisering valt de CIO formeel onder een van de stafdirecties of centrale diensten van het departement. Hierdoor is een afstand waarneembaar tussen de positie van de CIO en het primaire proces van een departement. Ook bestaat het risico dat de CIO onvoldoende zicht heeft op deze processen om daadwerkelijk de benodigde verbinding te kunnen maken tussen de primaire processen van de organisatie en de directie bedrijfsvoering of informatisering van het departement. Daarnaast draagt deze formele positie het risico met zich mee dat men op weerstand of onbegrip stuit bij de beleidsafdelingen of uitvoeringsorganisaties en onvoldoende grip krijgt op wat zich daar afspeelt. Een aantal CIO's geeft in de interviews aan dat de betrokkenheid van CIO's bij projecten van beleidsafdelingen in de praktijk regelmatig discussie oplevert.

Daarnaast geeft een aantal CIO's aan dat een goed verloop van ICT- of informatiseringprojecten in zekere zin samenhangt met de afstand tot de uitvoering van een ICT-project. Beleidsafdelingen lijken van nature weinig 'feeling' te hebben met de consequenties die hun keuzes hebben voor de uitvoering van een project. Men kan nauwelijks inschatten wat de gevolgen zijn van de vragen die zij voorleggen aan de uitvoeringsorganisaties en zij zijn zich vaak onvoldoende bewust van de consequenties van initiatieven. Een aanzienlijke afstand tussen de afdeling waar de plannen gemaakt worden en de afdeling of uitvoeringsorganisatie die de plannen moet gaan realiseren, maakt dat de beleidsafdeling vervolgens ook weinig zicht heeft op de uitvoering. Mevrouw Borgers, CIO VROM, zegt hier het volgende over: "We hebben hier niet dat zelfcorrigerend vermogen in huis, we hebben niet de uitvoering die hier door de gangen heen loopt en zegt: Hé, dat bestek wat je hebt gemaakt is allemaal leuk achter je pc, maar als ik buiten sta, dan klopt dat ding niet." De heer Van der Steenhoven, CIO OCW, geeft aan dat de afstand tussen beleid en uitvoering een van de redenen is geweest om de IB Groep en CFI, twee uitvoeringsorganisaties die op afstand van het departement waren geplaatst, te laten fuseren en dichter bij het departement te plaatsen in de zogenaamde Dienst Uitvoering Onderwijs (DUO).

De CIO's streven ernaar om de afstand tussen de verschillende organisatieonderdelen te verkleinen. De aanpak van de CIO's verschilt echter. Een aantal CIO's geeft specifiek aan vraag en aanbod van informatievoorziening binnen het departement op elkaar af te stemmen en samenhang te brengen in het geheel aan ICT-ondersteuning. Hiervoor is het noodzakelijk te sturen op de vraag en de dienstverlening op deze vraag aan te passen. Zij geven aan te sturen op nut en noodzaak van de vraag, helpen deze te verhelderen, denken mee over mogelijke oplossingen en verschaffen helderheid in de effecten van gemaakte of te maken keuzes.

In het verlengde daarvan spreken de meeste CIO's van een duidelijke verantwoordelijkheid om de verbinding te realiseren tussen de beleidsafdelingen van het departement en de informatievoorziening of ICT. De noodzaak om vanuit de beleidsafdelingen de verbinding met ICT te zoeken om gebruik te kunnen maken van de daar aanwezige kennis en expertise, wordt door de CIO's veelvuldig aangehaald. Een aantal CIO's geeft aan dat op het departement lange tijd een duidelijke afstand waarneembaar was tussen beide organisatieonderdelen. De CIO ziet het als zijn taak de verbinding te leggen en het samen optrekken en afstemmen te faciliteren. Bijna alle CIO's geven hierbij aan dat de beleidsvraag leidend is.

De CIO voedt de business ook ongevraagd met ideeën, kansen en mogelijkheden voor de organisatie op het gebied van informatiemanagement en het strategisch inzetten van (reeds beschikbare) informatie. Hiervoor is het volgens een van de CIO's van belang de politieke kansen te zien, de strategie van de organisatie te kennen en de verbinding te leggen met de vraag naar informatievoorziening in de organisatie.

Een enkele CIO gaat nog een stap verder in de invulling van zijn rol als verbinder en spreekt van het in lijn brengen van de organisatiedoelen en de inzet van informatietechnologie in de organisatie. Een van de CIO's geeft aan zich verantwoordelijk te voelen voor alle aspecten in de organisatie waar informatie en ICT in het geding zijn.

Wat opvalt is dat een aantal CIO's consequent spreekt van ICT, informatietechnologie of informatievoorziening. Deze CIO's lijken zich met andere woorden voornamelijk te richten op de technologie of voorziening. Dit in tegenstelling tot een aantal andere CIO's die meer spreken in termen van informatiemanagement en informatiebeleid. Sommige CIO's geven aan informatie en ICT als twee aparte zaken te beschouwen. Anderen geven zelfs aan dat ICT niet interessant is voor de CIO, maar dat zijn rol draait om organisatie- en verandermanagement en het samen met de business creëren van toekomstvaste oplossingen.

10.3.5 ADVISERENDE ROL

De CIO heeft, zo komt duidelijk naar voren uit de interviews, een adviserende rol. Hij of zij mag gevraagd en ongevraagd advies geven aan de eindverantwoordelijken voor projecten met een ICT-component. De CIO adviseert onder meer projectleiders, beleidsdirecteuren en DG's over de risico's van het project. Het advies van de CIO is echter niet bindend. Voor 'noodgevallen' heeft een CIO een directe lijn naar de bestuursraad, maar ook hier kan worden besloten het advies van de CIO, om bijvoorbeeld politieke redenen, naast zich neer te leggen. Mevrouw Borgers, CIO van het ministerie van VROM, zegt hierover: *"Uit die quickscan komen toch echt wel een aantal waarschuwingen. Ja, dan zit de rol voor de CIO en de (governance) board erop. Dan is het aan de SG en de DG."*

Er lijkt een tegenstrijdigheid te zijn ontstaan in de invulling van de rol van CIO. Veel departementen hebben voortvarend invulling gegeven aan de rol en deze toebedeeld aan een hoge ambtenaar. Echter, door de CIO een louter adviserende rol te geven wordt het belang dat aan de rol lijkt te worden gehecht in zekere zin ontkracht.

In de gesprekken met de CIO's wordt duidelijk dat zij het met name moeten hebben van het vertrouwen dat zij krijgen van de organisatie, de bijdrage en meerwaarde die zij leveren aan projecten en het inhoudelijke gezag dat zij zodoende opbouwen. Zo vertelt de heer Van Duijvenvoorden, CIO van het ministerie van AZ: "Om je rol als CIO te kunnen vervullen, dat heeft alles te maken met acceptatie en vertrouwen". Ook de heer Duijzer, CIO van het ministerie van LNV, geeft aan: "Mijn belangrijkste macht is mijn inhoudelijke gezag." Een enkele CIO voegt hier aan toe dat het 'rugnummer' CIO en de (politieke) aandacht voor de sturing van ICT-projecten wel meer gewicht in de schaal legt. Van Duijvenvoorden: "Het wordt nu veel makkelijker door een DG geaccepteerd als ik een zeer kritische noot aan hem geef over een project, als hoofd CID was me dat niet gelukt."

Al met al kan gesteld worden dat de CIO formeel wel toegang heeft tot de bestuursraad, maar in de praktijk nauwelijks macht heeft. De CIO is afhankelijk van het gezag en het vertrouwen dat hem of haar wordt toegekend vanuit de organisatie. Met name het besef in de beleidskern en de steun vanuit de bestuursraad blijken de positie van de CIO in de praktijk te sterken. Het is dan ook niet erg geruststellend dat een van de CIO's aangeeft dat men in de bestuursraad sceptisch is over de invulling van de rol van CIO, zoals mevrouw Borgers aanhaalt: "... er zit wel scepsis, in de bestuur(s)raad ook. (...) Ze vinden het allemaal maar franje."

10.3.6 RISICOMANAGEMENT

De aandacht van de CIO gaat in de praktijk vooral uit naar projecten met een potentieel hoog politiek of financieel risico. In de uitvoering blijkt dat de meeste CIO's werken met een aantal objectieve criteria om risico's van projecten in kaart te brengen. Op basis hiervan is bij sommige departementen een aantal prioritaire projecten benoemd. Bij de meeste departementen is een strategisch beraad of stuurgroep actief waarin de strategie wordt uitgezet, de prioriteiten worden bepaald en de beoordelingen worden gemaakt. Vaak is dit ook de plaats waar 'vraag' en 'aanbod' van ICT op hoog ambtelijk niveau samenkomen. Onder meer de ministeries van VenW, VROM, LNV, Financiën en VWS werken met zo'n stuurgroep. Hierin zijn dikwijls de directeuren van relevante beleidsdirecties of plaatsvervangend DG's en de CIO vertegenwoordigd.

Naast deze overlegstructuur op hoog niveau werken de CIO's nauw samen met de informatiemanagers van de verschillende beleidsafdelingen. Bij het ministerie

van BZ is een systeem opgezet waarbij projectplannen of voorstellen en jaarplannen van afdelingenen ambassades altijd eerst langs (de afdeling van) de CIO gaan en zijn er vaste momenten afgesproken waarop de CIO geraadpleegd wordt, bijvoorbeeld na afronding van projectonderdelen of de start van een nieuwe projectfase. Bij andere departementen is de betrokkenheid van de CIO afhankelijk van de mate waarin hij of zij op de hoogte is van de projecten die spelen binnen het departement. Veelal wordt per project bekeken hoe de rol van de CIO bij dat specifieke project wordt ingevuld, zo ook bij het ministerie van Verkeer en Waterstaat.

De wijze en momenten van betrokkenheid van de CIO bij projecten kan per departement verschillen. De heer Van der Stelt, CIO van het ministerie van VenW, geeft aan: "Het is niet zo dat men hier op de stoep staat en zegt: Oké, u bent CIO, vindt er maar wat van."

Enkele CIO's geven aan indirect verantwoordelijk te zijn voor de informatievoorziening aan de Tweede Kamer. De Tweede Kamer heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties opgedragen jaarlijks te rapporteren over de voortgang van grote ICT-projecten. De CIO's op hun beurt leveren informatie over de departementale projecten aan de minister van BZK. Een aantal CIO's geeft tijdens het interview aan toe te willen naar een verdergaande en actievere vorm van openbaarheid. Daarnaast geeft een van de CIO's aan dat het advies van een CIO de positie van de minister in de Tweede Kamer kan versterken op het moment dat de minister voldoende kennis van zaken heeft om kansen en risico's van bepaalde plannen aan te geven en de Kamer beargumenteerd kan adviseren.

Tot slot geeft een aantal CIO's aan dat het toezicht op de naleving van de Wet bescherming persoonsgegevens en toezicht op informatiebeveiliging in het takenpakket is opgenomen. Ook het waarborgen van de continuïteit van informatievoorziening en -systemen en het toezien op een efficiënte en effectieve inzet van die informatievoorziening wordt een aantal keren genoemd als taak van de CIO.

10.3.7 REIKWIJDTE

Naast het verbinden van de verschillende kolommen in de organisatie komen vrijwel alle CIO's te spreken over hun rol als 'toezichthouder' op grote ICT-projecten. Deze taken sluiten aan bij de formele taakomschrijving zoals de minister van Binnenlandse Zaken en Koninkrijksrelaties deze gedefinieerd heeft. Simpel gezegd moet de CIO ervoor zorgen dat er bij de overheid minder misgaat met ICT-projecten. Het advies van de CIO is formeel vereist bij projecten met een ICT-component van 20 miljoen euro of meer. Opvallend is echter dat slechts een deel van de ministeries dergelijke grote projecten heeft lopen. Dit gegeven blijkt aanleiding om

de criteria voor projecten die onder de aandacht van de CIO vallen nog eens te heroverwegen. De meeste departementen hanteren dan ook niet louter deze financiële grens, de CIO richt zich in de praktijk op alle risicovolle ICT-projecten.

Een aantal CIO's geeft aan dat naast de formele grens van 20 miljoen euro discussie bestaat over de reikwijdte van de verantwoordelijkheid van de CIO met betrekking tot projecten die niet onder directe ministeriële verantwoordelijkheid van de vakminister vallen. Projecten die uitgevoerd worden door een zelfstandig bestuursorgaan (ZBO) of een rechtspersoon met wettelijke taak (RWT) vallen staatsrechtelijk gezien niet onder directe ministeriële verantwoordelijkheid. In dat geval is geen sprake van een rapportageplicht van de minister aan de Tweede Kamer. Rapportage zou immers inhouden dat zij ter verantwoording kunnen worden geroepen over deze projecten.

10.3.8 CIO OFFICE

De meeste CIO's geven aan samen te werken met een team van adviseurs, de 'CIO office'. In vrijwel alle gevallen wordt de CIO office bemand door medewerkers die reeds werkzaam zijn op de afdeling of directie waar de CIO is aangesteld. De samenstelling van het team ter ondersteuning van de CIO verschilt sterk per departement. Zo heeft een van de CIO's een team van 15 tot 20 mensen tot zijn beschikking. Dit team voorziet de CIO van de benodigde informatie en maakt het mogelijk inhoudelijk gezag te verwerven in de organisatie. Dit in tegenstelling tot een andere CIO die slechts één ondersteuner ter beschikking heeft. Gemiddeld bestaat het team van de CIO uit zo'n drie tot acht medewerkers, die de taken ter ondersteuning van de CIO vaak naast andere taken uitvoeren.

De medewerkers van de CIO office zijn bij veel departementen, naast adviseur en ondersteuner van de CIO, ook de 'ogen en oren' van de CIO in de organisatie. Zij informeren de CIO over zaken die spelen in de organisatie en treden in sommige gevallen op als adviseur bij specifieke projecten. Bij sommige departementen lopen 'accountmanagers' of adviseurs regelmatig bij de verschillende organisatieonderdelen rond. Soms zijn zij ook direct betrokken bij, of hebben zij de leiding over, een aantal projecten met een ICT-component. Andere departementen hebben op de beleidsafdelingen informatiemanagers aangesteld.

10.3.9 ARCHITECTUUR EN PORTFOLIOMANAGEMENT

Praktisch alle CIO's geven expliciet aan dat het ontwerpen en bewaken van het geheel aan informatievoorziening en de samenhang tussen de verschillende onderdelen binnen deze voorziening een belangrijk onderdeel is van hun rol. Wel voegt een aantal CIO's hier onmiddellijk aan toe dat men nog bezig is hier invulling aan te geven. Zo geeft een van de CIO's aan dat men met een stuurgroep informa-

tievoorziening werkt aan een overzicht van de belangrijkste projecten binnen het departement. Daarnaast werkt men aan een architectuurplaat, waarmee men vanuit de prioriteiten van het departement, de (inter)departementale prioriteiten op het gebied van informatiemanagement en de ontwikkelingen in de sector kan toewerken naar een afwegingskader voor toekomstige projecten.

Het ministerie van Buitenlandse Zaken lijkt hierin voorop te lopen. Daar werkt men met een heldere architectuur, die inzicht geeft in de structuur en invulling van het 'grote geheel' van informatievoorziening van het departement. Tevens fungeert deze als leidraad bij het nemen van beslissingen die betrekking hebben op de inrichting van de organisatie en haar informatievoorziening. De strategie ten aanzien van informatievoorziening wordt eens in de twee tot drie jaar in overleg met de DG's herijkt. Daarnaast worden afdelingsplannen en relevante projectvoorstellen aan deze strategie getoetst.

10.3.10 OPDRACHTGEVERSCHAP

In vrijwel alle interviews komt 'goed opdrachtgeverschap' als aandachtspunt van de CIO ter sprake. Professioneel opdrachtgeverschap is, zo geven de CIO's aan, nog een punt van aandacht binnen de departementen. De CIO Rijk geeft aan dat men instrumenten inzet, zoals de *Gateway review*, om tot verbetering te komen. Een dergelijke review werkt twee kanten op. Enerzijds zorgt het voor inzicht en bewustwording richting het betreffende project. Anderzijds heeft het een vergelijkbaar effect op de reviewers, die op hetzelfde niveau functioneren als degene waarvoor ze een review uitvoeren en vaak zelf betrokken zijn bij eigen ICT-projecten. Een eerste vraag die bij veel reviews naar boven komt is de vraag wie opdrachtgever van het project is. Het is een taak van de CIO's om een bijdrage te leveren aan de professionaliteit van het opdrachtgeverschap in de organisatie. Een instrument als de *Gateway review* draagt bij aan een 'eenheid van taal' tussen de verschillende projecten en departementen. Die eenheid wordt ook gerealiseerd middels opleidingstrajecten, het eenduidig inrichten van portfoliomanagement en het standaardiseren van bijvoorbeeld overzichten van grote en risicovolle ICT-projecten. Hierdoor kan de CIO sturen op en in samenhang in ICT en wordt het mogelijk de door de Tweede Kamer gewenste rapportages over grote ICT-projecten op ieder gewenst moment te leveren.

In een interview geeft de heer Veenstra, CIO van het ministerie van EZ, aan dat de opdrachtgever van vlees en bloed duidelijk moet zijn, een 'overleg' kan deze rol niet vervullen: "Je moet iemand hebben die zegt: 'Ik ben ervan'." Daarnaast geeft hij aan dat een opdrachtgever op het juiste niveau moet worden aangesteld, namelijk het niveau waarop het resultaat moet worden behaald en waar hij of zij ook daadwerkelijk invloed heeft. Ook merkt een aantal CIO's op dat de opdracht in sommige gevallen onvoldoende duidelijk is vastgesteld of als gevolg van het

politieke proces of een vroegtijdige start van het project veelvuldig wordt aangepast. Ook hebben de CIO's het idee dat men de consequenties van de vraag onvoldoende weet in te schatten en onvoldoende heldere resultaatafspraken worden gemaakt, laat staan dat hierop gestuurd wordt. Een van de CIO's voegt hier nog aan toe dat de klantrelatie cruciaal is. Er moet met andere woorden iemand zijn die op de projectresultaten zit te wachten. Tot slot geven de CIO's aan dat de interne of externe aanbieders van ICT vaak pas laat in het proces betrokken worden en er nauwelijks sprake is van een dialoogrelatie met de aanbieders. In de samenwerking met en aansturing van de markt, lijken vooral kennis en expertise een rol te spelen. De CIO's geven aan dat kennis van de markt en de (on)mogelijkheden van informatietechnologie onontbeerlijk is, maar niet zelden ontbreekt bij de opdrachtgever.

De CIO van het ministerie van BZK, mevrouw Stolk, geeft aan dat men bij BZK bezig is een *toolbox* te ontwikkelen die de basis legt voor goed opdrachtgever- en goed opdrachtnemerschap. Deze toolbox geeft de minimale voorwaarden aan, een *baseline*. Daarnaast biedt de toolbox begeleiding bij het goed inrichten en organiseren van beide rollen.

10.3.11 INTERDEPARTEMENTALE SAMENWERKING

De Interdepartementale Commissie van Chief Information Officers, oftewel de ICCIO, wordt gevormd door alle CIO's en hun plaatsvervangers of vertegenwoordigers. De ICCIO wordt voorgezeten door de CIO Rijk, de heer Hillenaar. Hij geeft aan binnen de ICCIO te hebben toegewerkt naar manieren om gemeenschappelijk te besturen. Daartoe zijn nu verscheidene subcommissies benoemd die zich bezighouden met thema's als: grote ICT-projecten, *Gateway*, informatiebeveiliging, informatiehuishouding, Digitale Werkomgeving Rijk, taakstelling, regie en sourcing, kwaliteit en I-kolom en relatie ICT-bedrijfsleven. Ieder van deze subcommissies wordt getrokken door een van de (plaatsvervangend) CIO's. Daarnaast is men gestart met een gemeenschappelijk opleidingsprogramma. De heer Hillenaar geeft aan dat de kracht van de agenda van de ICCIO zit in de concrete doelen die men gesteld heeft. Het jaar 2009 stond voor de ICCIO in het teken van 'consolideren', oftewel de positie van de CIO in de verschillende departementen verstevigen. In 2010 heeft het ICCIO de verbinding gezocht met het primaire proces en toegewerkt naar een situatie waarin de CIO steeds meer de gewilde gesprekspartner van de beleidsmatig verantwoordelijken is. Pas dan zullen de CIO's naar verwachting in staat zijn hun strategischere rol op te pakken en toe te werken naar een aantal punten op de horizon.

De meeste CIO's zeggen de samenwerking met andere CIO's leerzaam en inspirerend te vinden. Een van de CIO's geeft aan dat de verschillende achtergronden van de departementale CIO's nog wat beter benut zouden kunnen worden in de ICCIO.

10.4 TOT SLOT

In deze slotparagraaf wordt de invulling van de CIO-rol in de praktijk bij de verschillende departementen van de rijksoverheid, afgezet tegen de in paragraaf 2 uitgezette theoretische lijnen. Daarnaast wordt de rol van de CIO kort vergeleken met de ervaringen met de rol van CIO bij de Amerikaanse federale overheid.

Als we allereerst kijken naar de taakomschrijving van de CIO en de invulling van de rol in de praktijk, lijken vrijwel alle CIO's hun rol breder op te vatten dan is voorgeschreven. De voorgeschreven controleachtige rol wordt door veel CIO's als beperkt gezien. De CIO's zien hun rol meer als verbinder van de technologie (ICT) en het primaire proces, veelal beleid. Het kabinet geeft aan informatiemanagement op de departementen naar een hoger niveau te willen tillen, mede door het aanstellen van CIO's. De taken die men de CIO vervolgens oplegt, hebben voornamelijk betrekking op het in de hand houden van grote ICT-projecten. Kortom de primaire focus van het kabinet ligt op de ICT-projecten en de samenhang hierin, terwijl de CIO's aangeven zich meer op de lange termijn te willen richten. Zij lijken zich, meer dan het kabinet, bewust van de noodzaak tot structurele verbeteringen in aanpak en processen.

Een volgende vraag die beantwoord moet worden is of de CIO ook echt de oplossing is voor de gesignaleerde problemen. Hierover kan op basis van het voorgaande geconcludeerd worden dat de invulling van een CIO-rol bij alle departementen van de rijksoverheid zeker een goede stap is in de richting van professionele besturing van ICT-projecten en professioneler informatiemanagement binnen het departement. Maar het valt te betwijfelen of de CIO met zijn huidige bevoegdheden ook echt in staat zal zijn om het ICT-enthousiasme van politiek en bestuurders te temperen en in staat is hen bewust te maken van de realiteit van de uitvoering van ICT-projecten. Hier speelt een aantal zaken een rol. Zolang (bureau)politieke redenen blijven prevaleren boven de urgente realiteit van ICT-projecten en ook dringende adviezen van de CIO om die reden aan de kant kunnen worden geschoven, zal de CIO wellicht nooit in staat zijn het gewenste resultaat te bereiken. Daarnaast doet het feit dat de rol van CIO slechts beperkt blijft tot een van de vele rollen van de betreffende ambtenaar, eveneens afbreuk aan de kracht van de CIO in de organisatie.

Een ander knelpunt zit in de reikwijdte van het werkveld van de CIO. De meeste en grootste ICT-projecten spelen veelal bij ZBO's of andere uitvoeringsorganisaties die op afstand van het departement staan. Zolang men geen zicht heeft op deze projecten zullen geen aanzienlijke verbeteringen optreden ten aanzien van de uitvoering van ICT-projecten bij deze organisaties.

Bovengenoemde punten betreffen cruciale keuzes in de inbedding van de CIO-rol in de organisatie. De aanstelling van de CIO kan worden aangemerkt als een louter

interne aangelegenheid. Het probleem waarvoor de CIO gesteld is, reikt echter verder dan zijn bevoegdheden. Deze constatering wekt het idee dat de CIO het risico loopt verantwoordelijk gesteld te worden voor zaken, maar daar in de praktijk nauwelijks tot geen invloed op heeft. Een voorbeeld hiervan is het al dan niet slagen van ICT-projecten bij het betreffende departement. Dit probleem zal naar verwachting niet opgelost zijn met de aanstelling van een CIO in zijn huidige vorm, omdat de oorzaak van het probleem zich deels buiten de invloedssfeer van de CIO bevindt.

Kijkend naar de rol van de CIO bij het rijk ten opzichte van de CIO-rol in de literatuur, valt een aantal zaken op. Aan de hand van de literatuur is een zestal rollen onderscheiden die allen deel uitmaken van de functie van een CIO. Een van de rollen is die van informatiestrateeg. In de huidige praktijk bij departementen kan slechts een deel van de CIO's aangemerkt worden als informatiestrateeg, dit zijn de CIO's die zich daadwerkelijk bezighouden met een informatiestrategie en verder kijken dan de ICT. Dit zijn ook de CIO's die zich meer op de lange termijn richten. De werkzaamheden van een ander deel van de CIO's beperken zich tot die van 'ICT-strateeg', deze CIO's zijn vooral (nog) druk met de ICT-projecten en het beheersbaar maken hiervan. Uit de interviews kwam het beeld naar voren dat het hier gaat om een aandachtspunt voor de CIO's, maar tevens een punt waar (interdepartementaal) aandacht voor is. Het werk van de CIO's en de ontwikkeling van de CIO-rol gaat een aantal fasen door, waarbij gestart wordt met zaken die spelen op de korte termijn en op beperkte schaal. De verwachting is dat na verloop van tijd en ontwikkeling meer tijd en aandacht zal zijn voor zaken die spelen op de lange termijn en breder in de organisatie, waarmee dit aandachtspunt aangemerkt kan worden als ontwikkelpunt voor de rol van CIO binnen de departementen.

Een tweede rol van de CIO is die van strategisch bedrijfsadviseur. Dit is overduidelijk een rol die zich uitstrekt over de lange termijn, waarbij de CIO vanuit informatiemanagement aanschuift in de bestuurskamer en meedenkt over de strategie van de organisatie. Kijkend naar de interviewresultaten kan gesteld worden dat er nauwelijks CIO's bij de rijksoverheid zijn die op dit niveau meedenken. Laat staan dat CIO's door weten te dringen op politiek niveau en hun adviezen hier richtinggevend zijn. Dit punt heeft deels betrekking op de inbedding van de rol in de organisatie en deels op de verdere ontwikkeling van de CIO-rol binnen de departementen.

De CIO als portfoliomanager komt in de huidige praktijk bij de rijksoverheid behoorlijk goed uit de verf. De meeste CIO's zijn directeur van de afdeling die de relatie met interne en externe ICT-aanbieders onderhoudt. Ook heeft een groot deel van de CIO's goed overzicht over de projecten die spelen en van belang zijn. Op deze wijze bewaakt de CIO de samenhang van projecten en beheert hij de ICT-portefeuille. Verdere ontwikkeling van de CIO-rol, wellicht tot een CIO-functie bij alle departementen zal dit punt naar verwachting versterken.

De rol van CIO als organisatiearchitect is een rol die in de huidige praktijk bij de rijksoverheid in ontwikkeling is. Met name met betrekking tot de informatiearchitectuur van de organisatie zijn de CIO's flink aan de weg aan het timmeren, terwijl nog weinig tekenen gesignaleerd zijn van een verregaandere betrokkenheid bij de organisatiearchitectuur.

De rol van de CIO heeft in 2010 een sterke ontwikkeling doorgemaakt. Met name de adviesrol van de CIO richting de primaire processen van de departementen is verstevigd. Dit heeft bijgedragen aan de verbinding tussen het primaire proces van de organisatie en de CIO en zijn afdeling. Bij de meeste departementen zijn heldere communicatielijnen en is de positie van de CIO fors verstevigd.

Ten slotte de rol van trendwatcher die de CIO in de literatuur krijgt toebedeeld. Uit de interviews met alle CIO's kan worden opgemaakt dat zij nog niet zover zijn dat zij hier invulling aan kunnen geven. Een enkele keer worden trends en ontwikkelingen aangehaald als een onderdeel dat moet worden meegenomen in de architectuur. Concrete invulling van deze rol is echter nog niet zichtbaar. Ook hier is sprake van een rol die door de CIO's op termijn zeker vervuld zal gaan worden.

Op basis van de literatuur kan geconcludeerd worden dat vooral de rol van trendwatcher en strategisch bedrijfsadviseur onderbelicht zijn in de huidige rol van CIO bij de rijksoverheid. Wat betreft de overige rollen kan gesteld worden dat de rol van CIO bij de rijksoverheid in een ontwikkelingsperspectief geplaatst moet worden. Over het geheel kan gesteld worden dat wel degelijk sprake is van bewustzijn van het belang van invulling van de verschillende rollen, zeker op rijksniveau (CIO Rijk). De huidige praktijk laat echter nog lang niet in alle gevallen zien dat deze rollen ook al echt ingevuld zijn, wel zijn vaak initiatieven genomen. Het feit dat het 'CIO-schap' voor velen een van de vele rollen is, werkt in dit opzicht complicerend. Zij hebben onvoldoende tijd om naast de waan van de dag tijd te investeren in de lange termijn, hier plannen voor te ontwikkelen en deze tot uitvoering te brengen.

Het voorbeeld van de CIO-rol op federaal niveau bij de overheid in de Verenigde Staten laat zien dat een aantal overeenkomsten bestaat tussen het ontwerp van de CIO-rol daar en in Nederland. Een van de meest in het oog springende punten is de vergelijkbare focus op beheersing van projecten en andere ICT-investeringen. Zowel hier als in de VS bestaat veel aandacht voor de financiële beheersaspecten. In de VS ligt de nadruk echter sterker op het efficiënt en effectief inzetten van ICT door de overheid, wat transparantie over dit thema mogelijk heeft gemaakt (Petri 2008). Dit komt ook duidelijk terug in de taken en bevoegdheden van de CIO. Waar CIO's in beide landen een adviserende functie hebben, ligt in de VS een sterke nadruk op het monitoren en evalueren van de doeltreffendheid van ICT-investeringen. Verder werken beide landen met een CIO-beraad op rijksniveau, is

in beide landen aandacht voor werken onder architectuur en is in beide landen de eindverantwoordelijkheid voor projecten expliciet bij bestuurders gelegd. Er is wel een verschil waarneembaar in de aandacht voor de kwaliteit van het personeel. Waar dit in de VS zeer hoog op de agenda staat en de CIO hier mede de verantwoordelijkheid voor draagt, lijkt de aandacht hiervoor in de Nederlandse situatie wat minder te zijn. Ten slotte ligt een duidelijk verschil in het feit dat de aanstelling, taken en bevoegdheden van de CIO in de VS zijn vastgelegd in de wet. De wettelijke basis heeft er in de Verenigde Staten toe geleid dat de focus van overheids-ICT niet langer ligt op inkoop maar op management, het heeft één managementframework voor alle overheids-ICT mogelijk gemaakt en de benodigde verankering voor beter projectmanagement geboden. Verder heeft het de ICT meer in lijn gebracht met de missie van de organisaties en de CIO een plaats aan de directietafel gegeven (Petri 2008).

Al met al lijkt de huidige invulling van de CIO-rol bij de rijksoverheid zeker een stap in de goede richting. Om deze stap echter het gewenste resultaat te laten hebben lijkt het in ieder geval van belang dat de CIO uitgerust wordt met meer bevoegdheden, zoals een bindend advies. Daarnaast lijkt het, zeker in de ontwikkelingsfase, van belang dat een CIO voldoende tijd heeft om een langetermijnstrategie te bepalen, zodat al zijn inspanningen in lijn zijn met de meer strategische doelen en langetermijnvisie. Tot slot is commitment van de bestuursraad van een departement een noodzakelijke voorwaarde voor het succes als CIO.

NOTEN

1 Onder grote ICT-projecten wordt verstaan: ICT-projecten van meer dan 20 miljoen euro en projecten met een ICT-component van meer dan 20 miljoen euro. ICT staat voor: informatie- en communicatietechnologie.

2 Sourcing: uitbesteden, zelf doen of een mengvorm (Algemene Rekenkamer 2008, blz. 59).

3 De 'I' in de afkorting staat voor 'Informatisering' (Kamerstukken 2007/08: 2).

4 De 'I' in de afkorting staat voor 'Informatisering' (Kamerstukken 2007/08a: 4).

5 Het op één lijn brengen van het primaire proces van de organisatie en het domein van de technologie kwam eerder aan de orde in paragraaf 2.2.1. als tweede fase in het model van Nolan. In deze fase wordt de CIO als 'bruggenbouwer' geïntroduceerd.

6 De afkorting IS staat voor 'Information Systems' (Emery 1991, blz. 9).

7 In de bijlage is een overzicht van de gesprekspartners opgenomen.

8 Bij de meeste departementen nemen in ieder geval de SG, pSG en DG's plaats in de bestuursraad.

LITERATUUR

Aalbers, R., R. van der Horst & E. Tuin (2006) 'Gestructureerd innoveren', blz. 79-99 in P. Hofman & E. Tuin (red.) (2006) *Het speelveld van de CIO. Omgaan met dilemma's,* 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Algemene Rekenkamer (2007) *Lessen uit ICT-projecten bij de overheid, Deel A*. Den Haag: Sdu Uitgevers.

Algemene Rekenkamer (2008) *Lessen uit ICT-projecten bij de overheid, Deel B*. Den Haag: Sdu Uitgevers.

Applegate, L.M. & J.J. Elam (1992) 'New Information Systems Leaders: A Changing Role in a Changing World', *Management Information Systems Quarterly* 16, 4: 469-490.

Bekkers, V. & V. Homburg (red.) (2005) *The Information Ecology of E-government. E-government as Institutional and Technological Innovation in Public Administration*, Amsterdam: IOS Press.

Bekkers, V. & V. Homburg (2009) 'The Myths and Ceremonies of E-Government: Beyond the Hype of a New and Better Government?', pp. 217-234 in A. Meijer, K. Boersma & P. Wagenaar (red.) *ICT's, Citizens and Governance: After de Hype!*, Amsterdam: IOS Press.

Boersma, K., A. Meijer & P. Wagenaar (2009) 'Unraveling and understanding the e-government hype', pp. 256- 265 in A. Meijer, K. Boersma & P. Wagenaar (red.) *ICT's, Citizens and Governance: After de Hype!*, Amsterdam: IOS Press.

Bouthillier, F. & K. Shearer (2002) 'Understanding knowledge management and information management: the need for an empirical perspective', *Information Research*, 8, 1: paper no. 141. Online beschikbaar, http://InformationR.net/ir/8-1/paper 141.html

Bovens, M.A.P. & S. Zouridis (2002) 'From Street Level to System Level Bureaucracies. How ICT is transforming administrative discretion and constitutional control', *Public Administration Review*, 62, 2: 174-183.

Broadbent, M. & E.S. Kitzis (2005) *The New CIO Leader. Setting the Agenda and Delivering Results,* Boston: Harvard Business School Press.

Bruijn, H. de, E. ten Heuvelhof & R.J. in 't Veld (2002) *Process Management (Why Project Management Fails in Complex Decision Makening Processes),* Boston: Kluwer.

Burk, D. van, R. van Es & J. Sturm (2006) 'IT compliancy als hefboom voor verbetering', blz. 61-78 in P. Hofman & E. Tuin (red.) *Het speelveld van de CIO. Omgaan met dilemma's,* 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Cavaye, A.L.M., P. Mantelaers, W. v.d. Berg & A. Zuurmond (1998) 'Towards guidelines for the development and management of transnational Information Systems', *Australian Journal of Information Systems* 5, 2: 13-21.

Ciborra, C. (2002) *The Labyrinths of Information: Challenging the Wisdom of Systems,* Oxford: Oxford University Press.

Contini, F. & G.F. Lanzara (red.) (2009) *ICT and Innovation in the Public Sector. European Studies in the Making of E-Government*, Hampshire: Palgrave Macmillan.

Dekker, V. (2007) 'Automatisering slokt miljarden euro's op. Overheid smijt met geld voor gebrekkige software', *Trouw*, 3 juni 2007.

Dekker, V. (2007) 'Automatiseringsramp lijkt onvermijdelijk. Overheid betaalt miljoenen voor systemen die gebrekkig werken of nooit worden gebruikt', *Trouw*, 3 juni 2007.

Dullemen, J., R. Teunissen & P.J. van de Venn (2006) 'Van applicatiecomplexiteit naar een businessgerichte architectuur', blz. 33-59 in P. Hofman & E. Tuin (red.) *Het speelveld van de CIO. Omgaan met dilemma's*, 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Emery, J.C. (1991) 'What role for the CIO?', *Management Information Systems Quarterly*, 1.

Fresz, P., P. Hofman, H. Stoffelen & E. Tuin (2006) 'Situationeel inrichten van Demand Management', blz. 101-115 in P. Hofman & E. Tuin (red.) *Het speelveld van de CIO. Omgaan met dilemma's*, 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Henderson, J.C. & N. Venkatraman (1999) 'Strategic alignment: Leveraging information technology for transforming organizations', *IBM Systems Journal*, 38, 2&3: 472-484.

Highbarger, J. (1988) 'What's The Proper Role For The CIO?', *Management Review* 77, 11: 53.

Hofman, P. & E. Tuin (red.) (2006) *Het speelveld van de CIO. Omgaan met dilemma's*, 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Hofman, P., J. Zwart & M. Zwiebel-Klaeijsen (2006) 'Groeien naar een succesvol Shared Service Centre', blz. 11-32 in P. Hofman & E. Tuin (red.) *Het speelveld van de CIO. Omgaan met dilemma's*, 's-Hertogenbosch: Uitgeverij Tutein Nolthenius.

Gupta, Y.P. (1991) 'The chief executive officer and the chief information officer: the strategic partnership', *Journal of Information Technology* 6, 3-4: 128-139.

Introna, L. (1997) *Management, Information and power: A narrative of the involved manager,* London: Macmillan.

Iyengar, K.P. (2007) *The effect of leadership style on CIO effectiveness*, Arlington: University of Texas.

Kirk, J. (1999) 'Information in organisations: directions for information management', *Information Research* 4, 3: paper 57. Online beschikbaar, http://informationr.net/ir/4-3/paper57.html

Macevičiute, E. & T.D. Wilson (2002) 'The development of the information management research area', *Information Research* 7, 3: paper 133. Online beschikbaar, http://InformationR.net/ir/7-3/paper133.html.

Maes, R. (2003) 'Informatiemanagement in kaart gebracht, *PrimaVera Working Paper 2003-02,* Amsterdam: Universiteit van Amsterdam.

Maes, R. (2008) 'Informatiemanagement of de kunde van het balanceren: van maakbaarheid naar taalbaarheid, *PrimaVera Working Paper 2008-06,* Amsterdam: Universiteit van Amsterdam.

Maes, R. & E.J. de Vries (2008) 'Information Leadership: The CIO as Orchestrator and Equilibrist', *ICIS 2008 Proceedings*, paper 58. Online beschikbaar, http://aisel.aisnet.org/icis2008/58.

Meijer, A., K. Boersma & P. Wagenaar (red.) (2009) *ICT's, Citizens and Governance: After de Hype!*, Amsterdam: IOS Press.

Millar, V.E. (1983) 'The emergence of the chief information officer', *Management Review* 72, 2: 29.

OECD (2003) *The e-Government Imperative*, Paris: OECD.

Petri, G. (2008) 'Clinger-Cohen Act voorbeeld voor Nederlandse overheid', *Automatisering Gids*, nr. 8.

Smaltz, D., V. Sambamurthy & R. Agarwal (2006) 'The Antecedents of CIO Role Effectiveness in Organizations: An Empirical Study in the Healthcare Sector', *IEEE Transactions on Engineering Management* 53, 2: 207-222.

Stephens, C.S., W.N. Ledbetter, A. Mitra & F.N. Ford (1992) 'Executive or Functional Manager? The Nature of the CIO's Job', *Management Information Systems Quarterly* 16, 4: 449-467.

Synnott, W.R. (1987) 'Putting a CIO in charge', *Institutional Investor: Financial Technology Forum Supplement* 21: 47-48.

United States General Accounting Office (2001) *Maximizing the Success of Chief Information Officers. Learning from leading organizations,* Washington: GAO-01-376G.

Velde, R. te, T. Dicks, P. Jörg & F. Polman (2005) 'Informatiemanagement in overheidsorganisaties', blz. 375-397 in M. Lips, V. Bekkers & A. Zuurmond (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Uitgeverij Lemma BV.

Venrooij, A. van (2002) *Nieuwe vormen van interorganisationele publieke dienstverlening,* Delft: Technical University of Delft.

Verhoef, C. (2002) 'De Clinger-Cohen Act', *Automatisering Gids*, nr. 13, Den Haag: Sdu Uitgevers.

Verhoef, C. (2007) 'Overheid mist de regie, en ook de kunde', *Automatisering Gids* 26.

Verhoef, C. (2009) 'Kamer scherpt ICT-toezicht aan', *PM* 20 februari 2009.

Verkooijen, P. (2002) 'Amerikaanse overheid verspilt minder door wet op ICT', *Digitaal Bestuur* 1, 2.

Vogels, P. (2007) 'Foute automatisering kost miljarden – bedrijven maken misbruik van onkunde over gecompliceerde software', *Nederlands Dagblad*, 15 juni 2007.

Wilson, T.D. (2002) 'The nonsense of "knowledge management"', *Information Research*, 8, 1: paper no. 144. Online beschikbaar, http://InformationR.net/ir/8-1/paper 144.html.

Zouridis, S. & M. Thaens (2005) 'Reflections on the Anatomy of E-Government', blz. 21-36 in V. Bekkers & V. Homburg (red.) *The Information Ecology of E-government. E-government as Institutional and Technological Innovation in Public Administration*, Amsterdam: IOS Press.

Zuurmond, A. (1994) *De Infocratie. Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk,* Den Haag: Uitgeverij Phaedrus.

Zuurmond, A. (1998), 'From bureaucracy to infocracy: are democratic institutions lagging behind?' in I.Th.M. Snellen (red.), *Public Administration in an Information Age, Handbook Informatization*, Amsterdam: IOS Press.

Zuurmond, A. & M. Meesters (2005) 'ICT en overheidsorganisatie', blz. 299-327 in M. Lips, V. Bekkers en A. Zuurmond (red.) *ICT en openbaar bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Utrecht: Uitgeverij Lemma BV.

KAMERSTUKKEN

Kamerstukken II 2006/07, 26 643, nr. 92.
Kamerstukken II 2006/07a, 26 643, nr. 95.
Kamerstukken II 2006/07b, 26 643, nr. 97.
Kamerstukken II 2006/07c, 26 643, nr. 100.
Kamerstukken II 2006/07d, 26 643, nr. 127.
Kamerstukken II 2007/08, 26 643, nr. 128.
Kamerstukken II 2007/08a, 26 643, nr. 135.

BIJLAGE

OVERZICHT INTERVIEWS EN ORIËNTERENDE GESPREKKEN

INTERVIEWS

Cees van Duijvenvoorden, Hoofd Informatiedienst, ministerie van Algemene Zaken
Nicole Stolk-Luyten, Directeur Bedrijfsvoering, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Jan Flippo, Hoofddirecteur Informatiseringsontwikkeling, ministerie van Buitenlandse Zaken
Tjeerd Veenstra, Plaatsvervangend Directeur Bedrijfsvoering, ministerie van Economische Zaken
Wim Sijstermans, Chief Information Officer, ministerie van Financiën
Bob Papenhuijzen, Directeur Informatisering, ministerie van Justitie
Jan Willem Duijzer, Coördinerend Directeur Informatie/CIO, ministerie van Landbouw, Natuur en Voedselkwaliteit
Koos van der Steenhoven, Secretaris-Generaal, ministerie van Onderwijs, Cultuur en Wetenschap
Hans van der Stelt, Directeur Bedrijfsvoering, ministerie van Verkeer en Waterstaat
Ron Roozendaal, Chief Information Officer, ministerie van Volksgezondheid, Welzijn en Sport
Madeleine Laqueur, Plaatsvervangend CIO, ministerie van Volksgezondheid, Welzijn en Sport
Saskia Borgers, Plaatsvervangend Secretaris-Generaal, ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
Maarten Hillenaar, Directeur Informatiseringbeleid Rijk, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Elly Bogerman, Directrice, ICT Uitvoeringsorganisatie (ICTU)
John Kuiperí, Medewerker, ICT Uitvoeringsorganisatie (ICTU)
Vincent Homburg, Hoogleraar, Erasmus Universiteit Rotterdam
Hennie Wesseling, Chief Information Officer, TNT
Rik Maes, Hoogleraar, Universiteit van Amsterdam
Jacob Verschuur, Adviseur, Ernst & Young
Leo Smits, Directeur, Het Expertise Centrum (HEC)

GESPREKKEN

Marcel Thaens, adviseur, Het Expertise Centrum (HEC)
Shane Arjun Sharma, beleidsmedewerker CIO Office, ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Akse Plaat, beleidsmedewerker CIO Office, ministerie van Justitie
Chris Verhoef, Hoogleraar Informatica, Vrije Universiteit Amsterdam

OVER DE AUTEURS

Dennis Broeders is senior wetenschappelijk medewerker en projectcoördinator bij de Wetenschappelijke Raad voor het Regeringsbeleid in Den Haag. Hij was bij de WRR eerder als coördinator verantwoordelijk voor de rapporten *Focus op functies* (2005) over de toekomst van het mediabeleid en *Identificatie met Nederland* (2007) over nationale identiteit. Hij is tevens als onderzoeker verbonden aan de vakgroep Sociologie van de Erasmus Universiteit Rotterdam waar hij in 2009 promoveerde. Zijn onderzoek richt zich op de toepassing van moderne surveillance technieken in het overheidsbeleid, in het bijzonder het migratiebeleid. Hierover publiceerde hij ondermeer in *American Behavioral Scientist, International Sociology, West European Politics, Punishment & Society* en *The British Journal of Criminology*. In 2009 verscheen zijn boek *Breaking Down Anonymity. Digital Surveillance of Irregular Migrants in Germany and the Netherlands* bij Amsterdam University Press.

Ybo Buruma is hoogleraar straf- en strafprocesrecht aan de Radboud Universiteit Nijmegen. Hij is redacteur van het *Nederlands Juristenblad* en van het strafrechtelijke tijdschrift *Delikt & Delinkwent* en als annotator becommentarieert hij rechterlijke uitspraken in de Nederlandse Jurisprudentie. In veel van zijn werk combineert hij strafrechtelijke en criminologische inzichten. Naast zijn wetenschappelijk werk verricht hij werkzaamheden als raadsheer plaatsvervanger bij het gerechtshof Arnhem en als voorzitter van de Toegangscommissie Evaluatie Afgesloten Strafzaken.

Tony Busker is als hoofddocent verbonden aan het instituut Communicatie, Media- en Informatietechnologie (CMI) aan de Hogeschool van Rotterdam en als systeemanalist bij het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) van het Ministerie van Veiligheid en Justitie. Hij studeerde in 1991 cum laude af in de Informatica. Na zijn studie is hij met name werkzaam geweest in de informatiebeveiliging en de systeemontwikkeling met als doel om (overheids)informatie uit gestructureerde en ongestructureerde databases te ontsluiten. Daarnaast doet hij onderzoek naar verbetering van algoritmen voor simulatietoepassingen met bijzondere aandacht voor de rol van gegevensstructuren.

Colette Cuijpers is werkzaam als universitair docent bij TILT – Tilburg Institute for Law, Technology, and Society waar zij in 2004 promoveerde. Haar onderzoek richt zich op regulering van en door technologie, met een focus op privacyrecht, het onderwerp van haar proefschrift. Zij publiceerde in verschillende nationale en internationale tijdschriften en boeken. Daarnaast is zij actief betrokken (geweest) bij Europese projecten als Breaking Barriers to Egovernment, FIDIS, PRIME en VIRTUOSO. Zij doceert en doceerde onder meer Privacy & Data Protection, eCommerce en Aansprakelijkheid op Internet. In 2010 was zij tevens verbonden aan de

Wetenschappelijk Raad voor het Regeringsbeleid als wetenschappelijk medewerker.

Sunil Choenni is afgestudeerd in theoretische informatica aan de TU Delft en gepromoveerd in databasetechnologie aan de Universiteit Twente. Na zijn promotie is hij werkzaam geweest aan verschillende onderzoeksinstituten en universiteiten op het gebied van informatica en toepassingen van informatica. Thans is hij hoofd van de afdeling Statistische Informatievoorziening & Beleidsanalyse bij het WODC en lector Human Centered ICT aan de Hogeschool Rotterdam.

Michel van Eeten is hoogleraar Bestuurskunde bij de Faculteit Techniek, Bestuur en Management van de TU Delft. Hij is tevens verbonden als kerndocent aan de Nederlandse School voor Openbaar Bestuur in Den Haag. Zijn leerstoel richt zich op de governance van infrastructuren, met speciale aandacht voor de veiligheid van internet. Op dit terrein heeft hij beleidsonderzoek verricht voor diverse Nederlandse ministeries, Rabobank, KPN, de California Energy Commission, de United Nations International Telecommunications Union en de OESO.

Paul de Hert is verbonden aan de universiteiten van Tilburg en Brussel (respectievelijk TILT en LSTS). Hij schreef meer dan 500 bijdragen (in boeken en tijdschriften) over juridische actuele onderwerpen en is lid van meerdere juridische tijdschriften, waaronder *Computer, Law Security Review, Criminal Law and Philosophy* en *Panopticon*. Hij doceert en doceerde onder meer Privacy & Data Protection, (internationaal en Europees) strafrecht, Rechten van de mens en Rechtstheorie.

Anne-Greet Keizer is wetenschappelijk medewerker bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en als lid van de projectgroep BIT betrokken bij het rapport iOverheid. Anne-Greet heeft een achtergrond in de Bestuurskunde en Kunst- en cultuurwetenschappen. Ze werkt sinds 2005 bij de WRR en was betrokken bij diverse projecten. Samen met Paul den Hoed was ze redacteur van de publicatie *Op Steenworp afstand* (2007), en schreef daarin een deel getiteld *Evenwichtskunstenaars tussen beleid en wetenschap*. Ze publiceert o.a. over adviesorganen vanuit een internationaal vergelijkend perspectief.

Esther Keymolen MA is wetenschappelijk medewerker bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en betrokken bij het rapport *iOverheid.* Als PhD-student is zij tevens verbonden aan de vakgroep Wijsgerige Antropologie-Filosofie van Mens en Cultuur van de Erasmus Universiteit Rotterdam, waar zij aan een proefschrift werkt. Haar onderzoek richt zich op de implicaties van ICT voor persoonlijke interacties en meer in het bijzonder de wijze waarop ICT vertrouwen binnen deze interacties beïnvloedt en vorm geeft.

Erik Leertouwer heeft econometrie gestudeerd en is gepromoveerd in de politieke economie, beide aan de Rijksuniversiteit Groningen. Hij is als senior onderzoeker verbonden aan de afdeling Statistische Informatievoorziening en Beleidsanalyse van het WODC, waar hij onderzoek op het gebied van informatiemanagement coördineert. Tevens is hij plaatsvervangend afdelingshoofd. Zijn onderzoeksinteresses betreffen het modelleren van complexe processen in de justitieketen en de (mogelijke) bijdrage van ICT aan het verkrijgen van inzicht in criminaliteit en veiligheid.

Albert Meijer (1967) is als universitair hoofddocent verbonden aan het departement bestuurs- en organisatiewetenschap van de Universiteit Utrecht. Hij publiceert regelmatig in nationale en internationale tijdschriften over onderwerpen van technologie en bestuur. Speciale aandachtsgebieden zijn transparantie, verantwoording, controle en participatie. In samenwerking met Huub Dijstelbloem en het Rathenau Instituut publiceerde hij in 2009 het boek *De Migratiemachine* over gebruik van technologie in het migratiebeleid. Ook redigeerde hij samen met Kees Boersma en Pieter Wagenaar het in 2009 verschenen boek *ICTs, Citizens and Governance: After the Hype* over de beloften en realisatie van informatietechnologie in het openbaar bestuur. Momenteel werkt hij aan een Engelstalig boek over internet en transparantie.

Corien Prins is sinds 2008 lid van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Aan de Universiteit van Tilburg is zij als hoogleraar Recht en Informatisering verbonden aan het Tilburg Institute for Law, Technology, and Society (TILT). Prins was tussen 1994 en 2008 voorzitter/directeur van dit onderzoeksinstituut. Corien Prins studeerde aan de Rijksuniversiteit Leiden Slavische Taal- en Letterkunde alsmede Rechtsgeleerdheid en promoveerde aan deze universiteit in november 1991. Na haar promotie was zij als visiting professor verbonden aan Hastings College of Law, University of California, San Francisco. Prins is lid van de Koninklijke Akademie van Wetenschappen (KNAW).

Tamara Snijders studeerde Bestuurskunde aan de Vrije Universiteit in Amsterdam. In 2008 studeerde zij af met een onderzoek naar de leereffecten van bezwaarprocedures en klachtprocedures bij gemeentelijke sociale diensten. Van september 2009 tot en met maart 2010 was zij als rijkstrainee verbonden aan de WRR. Zij maakte deel uit van de wetenschappelijke staf en was werkzaam voor de projectgroep Beleid, Informatie en Technologie. Op dit moment is zij werkzaam als teamleider bij het ministerie van Infrastructuur en Milieu.

RAPPORTEN AAN DE REGERING

Eerste raadsperiode (1972-1977)

1 Europese Unie
2 Structuur van de Nederlandse economie
3 Energiebeleid
Gebundeld in één publicatie (1974)
4 Milieubeleid (1974)
5 Bevolkingsgroei (1974)
6 De organisatie van het openbaar bestuur (1975)
7 Buitenlandse invloeden op Nederland: Internationale migratie (1976)
8 Buitenlandse invloeden op Nederland: Beschikbaarheid van wetenschappelijke en technische kennis (1976)
9 Commentaar op de Discussienota Sectorraden (1976)
10 Commentaar op de nota Contouren van een toekomstig onderwijsbestel (1976)
11 Overzicht externe adviesorganen van de centrale overheid (1976)
12 Externe adviesorganen van de centrale overheid (1976)
13 Maken wij er werk van? Verkenningen omtrent de verhouding tussen actieven en niet-actieven (1977)
14 Interne adviesorganen van de centrale overheid (1977)
15 De komende vijfentwintig jaar – Een toekomstverkenning voor Nederland (1977)
16 Over sociale ongelijkheid – Een beleidsgerichte probleemverkenning (1977)

Tweede raadsperiode (1978-1982)

17 Etnische minderheden (1979)
A. Rapport aan de Regering
B. Naar een algemeen etnisch minderhedenbeleid?
18 Plaats en toekomst van de Nederlandse industrie (1980)
19 Beleidsgerichte toekomstverkenning
Deel 1: Een poging tot uitlokking (1980)
20 Democratie en geweld. Probleemanalyse naar aanleiding van de gebeurtenissen in Amsterdam op 30 april 1980
21 Vernieuwingen in het arbeidsbestel (1981)
22 Herwaardering van welzijnsbeleid (1982)
23 Onder invloed van Duitsland. Een onderzoek naar gevoeligheid en kwetsbaarheid in de betrekkingen tussen Nederland en de Bondsrepubliek (1982)
24 Samenhangend mediabeleid (1982)

Derde raadsperiode (1983-1987)

25 Beleidsgerichte toekomstverkenning
Deel 2: Een verruiming van perspectief (1983)
26 Waarborgen voor zekerheid. Een nieuw stelsel van sociale zekerheid in hoofdlijnen (1985)
27 Basisvorming in het onderwijs (1986)
28 De onvoltooide Europese integratie (1986)
29 Ruimte voor groei. Kansen en bedreigingen voor de Nederlandse economie in de komende tien jaar (1987)
30 Op maat van het midden- en kleinbedrijf (1987)

Deel 1: Rapport aan de Regering

Deel 2: Pre-adviezen

31 Cultuur zonder grenzen (1987)

32 De financiering van de Europese Gemeenschap. Een interimrapport (1987)

33 Activerend arbeidsmarktbeleid (1987)

34 Overheid en toekomstonderzoek. Een inventarisatie (1988)

Vierde raadsperiode (1988-1992)

35 Rechtshandhaving (1988)

36 Allochtonenbeleid (1989)

37 Van de stad en de rand (1990)

38 Een werkend perspectief. Arbeidsparticipatie in de jaren '90 (1990)

39 Technologie en overheid (1990)

40 De onderwijsverzorging in de toekomst (1991)

41 Milieubeleid. Strategie, instrumenten en handhaafbaarheid (1992)

42 Grond voor keuzen. Vier perspectieven voor de landelijke gebieden in de Europese Gemeenschap (1992)

43 Ouderen voor ouderen. Demografische ontwikkelingen en beleid (1993)

Vijfde raadsperiode (1993-1997)

44 Duurzame risico's. Een blijvend gegeven (1994)

45 Belang en beleid. Naar een verantwoorde uitvoering van de werknemersverzekeringen (1994)

46 Besluiten over grote projecten (1994)

47 Hoger onderwijs in fasen (1995)

48 Stabiliteit en veiligheid in Europa. Het veranderende krachtenveld voor het buitenlands beleid (1995)

49 Orde in het binnenlands bestuur (1995)

50 Tweedeling in perspectief (1996)

51 Van verdelen naar verdienen. Afwegingen voor de sociale zekerheid in de 21e eeuw (1997)

52 Volksgezondheidszorg (1997)

53 Ruimtelijke-ontwikkelingspolitiek (1998)

54 Staat zonder land. Een verkenning van bestuurlijke gevolgen van informatie- en communicatietechnologie (1998)

Zesde raadsperiode (1998-2002)

55 Generatiebewust beleid (1999)

56 Het borgen van publiek belang (2000)

57 Doorgroei van arbeidsparticipatie (2000)

58 Ontwikkelingsbeleid en goed bestuur (2001)

59 Naar een Europabrede Unie (2001)

60 Nederland als immigratiesamenleving (2001)

61 Van oude en nieuwe kennis. De gevolgen van ICT voor het kennisbeleid (2002)

62 Duurzame ontwikkeling. Bestuurlijke voorwaarden voor een mobiliserend beleid (2002)

63 De toekomst van de nationale rechtsstaat (2002)

64 Beslissen over biotechnologie (2003)

65 Slagvaardigheid in de Europabrede Unie (2003)

66 Nederland handelsland. Het perspectief van de transactiekosten (2003)
67 Naar nieuwe wegen in het milieubeleid (2003)

Zevende raadsperiode (2003-2007)

68 Waarden, normen en de last van het gedrag (2003)
69 De Europese Unie, Turkije en de islam (2004)
70 Bewijzen van goede dienstverlening (2004)
71 Focus op functies. Uitdagingen voor een toekomstbestendig mediabeleid (2005)
72 Vertrouwen in de buurt (2005)
73 Dynamiek in islamitisch activisme. Aanknopingspunten voor democratisering en mensenrechten (2006)
74 Klimaatstrategie – tussen ambitie en realisme (2006)
75 Lerende overheid. Een pleidooi voor probleemgerichte politiek (2006)
76 De verzorgingsstaat herwogen. Over verzorgen, verzekeren, verheffen en verbinden (2006)
77 Investeren in werkzekerheid (2007)
78 Europa in Nederland (2007)
79 Identificatie met Nederland (2007)
80 Innovatie vernieuwd. Opening in viervoud (2008)
81 Infrastructures. Time to Invest (2008)

Achtste raadsperiode (2008-2012)

82 Onzekere veiligheid. Verantwoordelijkheden rond fysieke veiligheid (2008)
83 Vertrouwen in de school. Over de uitval van 'overbelaste' jongeren (2009)
84 Minder pretentie, meer ambitie. Ontwikkelingshulp die verschil maakt (2010)
85 Aan het buitenland gehecht. Over verankering en strategie van Nederlands buitenlandbeleid (2010)
86 iOverheid (2011)

Rapporten aan de Regering nrs. 1 t/m 67 en publicaties in de reeks *Voorstudies en achtergronden* zijn niet meer leverbaar. Alle studies van de WRR zijn beschikbaar via de website www.wrr.nl.
Rapporten aan de Regering nrs. 68 t/m 86 zijn verkrijgbaar in de boekhandel of via Amsterdam University Press, Herengracht 221, 1016 BG Amsterdam (www.aup.nl).

VERKENNINGEN

Zevende raadsperiode (2003-2007)

1 J. Pelkmans, M. Sie Dhian Ho en B. Limonard (red.) (2003) Nederland en de Europese grondwet
2 P.T. de Beer en C.J.M. Schuyt (red.) (2004) Bijdragen aan waarden en normen
3 G. van den Brink (2004) Schets van een beschavingsoffensief. Over normen, normaliteit en normalisatie in Nederland
4 E.R. Engelen en M. Sie Dhian Ho (red.) (2004) De staat van de democratie. Democratie voorbij de staat
5 P.A. van der Duin, C.A. Hazeu, P. Rademaker en I.J. Schoonenboom (red.) (2004) Vijfentwintig jaar later. De Toekomstverkenning van de WRR uit 1977 als leerproces
6 H. Dijstelbloem, P.L. Meurs en E.K. Schrijvers (red.) (2004) Maatschappelijke dienstverlening. Een onderzoek naar vijf sectoren
7 W.B.H.J. van de Donk, D.W.J. Broeders en F.J.P. Hoefnagel (red.) (2005) Trends in het medialandschap. Vier verkenningen
8 G. Engbersen, E. Snel en A. Weltevrede (2005) Sociale herovering in Amsterdam en Rotterdam. Eén verhaal over twee wijken
9 D.J. Wolfson (2005) Transactie als bestuurlijke vernieuwing. Op zoek naar samenhang in beleid en uitvoering
10 Nasr Abu Zayd (2006) Reformation of Islamic Thought. A Critical Historical Analysis
11 J.M. Otto (2006) Sharia en nationaal recht. Rechtssystemen in moslimlanden tusssen traditie, politiek en rechtsstaat
12 P.L. Meurs, E.K. Schrijvers en G.H. de Vries (red.) (2006) Leren van de praktijk. Gebruik van lokale kennis en ervaring voor beleid
13 W.B.H.J. van de Donk, A.P. Jonkers en G.J. Kronjee (red.) (2006) Geloven in het publieke domein. Verkenningen van een dubbele transformatie
14 D. Scheele, J.J.M. Theeuwes, G.J.M. de Vries (red.) (2007) Arbeidsflexibiliteit en ontslagrecht
15 P.A.H. van Lieshout, M.S.S. van der Meij en J.C.I. de Pree (red.) (2007) Bouwstenen voor betrokken jeugdbeleid
16 J.J.C. Voorhoeve (2007) From War to the Rule of Law. Peace Building after Violent Conflicts
17 M. Grever en K. Ribbens (2007) Nationale identiteit en meervoudig verleden
18 B. Nooteboom and E. Stam (eds.) (2008) Micro-foundations for Innovation Policy
19 G. Arts, W. Dicke and L. Hancher (eds.) (2008) New Perspectives on Investments in Infrastructures

Achtste raadsperiode (2008-2012)

20 D. Scheele, R. van Gaalen en J. van Rooijen (2008) Werk en inkomsten na massaontslag: de zekerheid is niet van de baan
21 Monique Kremer, Peter van Lieshout and Robert Went (eds.) (2009) Doing Good or Doing Better. Development Policies in a Globalizing World
22 W.L. Tiemeijer, C.A. Thomas en H.M. Prast (red.) (2009) De menselijke beslisser. Over de psychologie van keuze en gedrag
23 Huub Dijstelbloem, Paul den Hoed, Jan Willem Holtslag en Steven Schouten (red.) (2010) Het gezicht van de publieke zaak. Openbaar bestuur onder ogen
24 M.B.A. van Asselt, A. Faas, F. van der Molen en S.A. Veenman (red.) (2010) Uit zicht. Toekomstverkennen met beleid

Alle *Verkenningen* zijn verkrijgbaar in de boekhandel of via Amsterdam University Press, Herengracht 221, 1016 BG Amsterdam (www.aup.nl).

WEBPUBLICATIES

Zevende raadsperiode (2003-2007)

WP 01 Opvoeding, onderwijs en jeugdbeleid in het algemeen belang
WP 02 Ruimte voor goed bestuur: tussen prestatie, proces en principe
WP 03 Lessen uit corporate governance en maatschappelijk verantwoord ondernemen
WP 04 Regulering van het bestuur van maatschappelijke dienstverlening: eenheid in verscheidenheid
WP 05 Een schets van het Europese mediabeleid
WP 06 De regulering van media in internationaal perspectief
WP 07 Beleid inzake media, cultuur en kwaliteit: enkele overwegingen
WP 08 Geschiedenis van het Nederlands inhoudelijk mediabeleid
WP 09 Buurtinitiatieven en buurtbeleid in Nederland anno 2004: analyse van een veldonderzoek van 28 casussen
WP 10 Geestelijke gezondheid van adolescenten: een voorstudie
WP 11 De transitie naar volwassenheid en de rol van het overheidsbeleid: een vergelijking van institutionele arrangementen in Nederland, Zweden, Groot-Brittanië en Spanje
WP 12 Klassieke sharia en vernieuwing
WP 13 Sharia en nationaal recht in twaalf moslimlanden
WP 14 Climate strategy: Between ambition and realism
WP 15 The political economy of European integration in the polder: Asymmetrical supranational governance and the limits of legitimacy of Dutch EU policy-making
WP 16 Europe in law, law in Europe
WP 17 Faces of Europe: Searching for leadership in a new political style
WP 18 The psychology and economics of attitudes in the Netherlands
WP 19 Citizens and the legitimacy of the European Union
WP 20 No news is bad news! The role of the media and news framing in embedding Europe
WP 21 Actor paper subnational governments: Their role in bridging the gap between the EU and its citizens
WP 22 The Dutch third sector and the European Union: Connecting citizens to Brussels
WP 23 Europe in parliament: Towards targeted politicization
WP 24 Europe in the Netherlands: Political parties
WP 25 The EU Constitutional Treaty in the Netherlands: Could a better embedding have made a difference?
WP 26 How to solve the riddle of belated Euro contestation in the Netherlands?
WP 27 Connection, consumer, citizen: Liberalising the European Union gas market
WP 28 Dutch EU-policies with regard to legal migration – The directive on family reunification
WP 29 The accession of Turkey to the European Union: The political decision-making process on Turkey in The Netherlands
WP 30 The Habitats Directive: A case of contested Europeanization
WP 31 Encapsulating services in the 'polder': Processing the Bolkestein Directive in Dutch Politics
WP 32 Zorgen over de grens
WP 33 De casus Inburgering en Nationaliteitswetgeving: iconen van nationale identiteit
WP 34 In debat over Nederland

Achtste raadsperiode (2008-2012)

WP 35 Veel voorkomende criminaliteit
WP 36 Gevaarlijke stoffen
WP 37 ICT en internet
WP 38 Voedsel en geneesmiddelen
WP 39 Waterbeheer en waterveiligheid
WP 40 Verschuivende vensters: veranderingen in het institutionele landschap van de Nederlandse ontwikkelingssamenwerking
WP 41 Internationale publieke goederen: karakteristieken en typologie
WP 42 Het Nederlandse veiligheidsbeleid in een veranderende wereld
WP 43 Internationalisering en Europeanisering van strafrechtelijke rechtshandhaving in Nederland
WP 44 Praktijken van beleidsgerichte toekomstverkenning : een inventarisatie
WP 45 Het landelijk EPD als blackbox: besluitvorming en opinies in kaart
WP 46 Happy Landings? Het biometrische paspoort als zwarte doos
WP 47 Over de rolverdeling tussen overheid en burger bij het beschermen van identiteit
WP 48 eCall Blackbox
WP 49 Blackbox-onderzoek veiligheidshuizen
WP 50 Goed opdrachtgeverschap jegens ICTU
WP 51 Het biometrische paspoort in Nederland: crash of zachte landing?
WP 52 De prijs van heupen en knieën
WP 53 Vitaal en bevlogen
WP 54 Procedures en problemen op de markt voor reïntegratiedienstverlening
WP 55 Securization in the Netherlands shaped by and shaping regulation
WP 56 Hallmarking Halal
WP 57 Markets and public values in healthcare
WP 58 Het buitenlandse beleid van middelgrote mogendheden
WP 59 'Location based privacy' in constellaties van publiek-private verantwoordelijkheid

WRR VERKENNINGEN 25

De staat van informatie

In tijden van informatisering veranderen het functioneren en het karakter van zowel de samenleving als de overheid. Soms is dit duidelijk aanwijsbaar, maar soms gebeurt het ook op een meer sluipende wijze. De inzet van ICT biedt kansen voor beleidsterreinen zoals de zorg, het jeugdbeleid en het immigratiebeleid, maar stelt het openbaar bestuur ook voor nieuwe fundamentele vragen. Hoe om te gaan met risico's en kwetsbaarheden rondom de inzet van nieuwe ICT? Wat betekent 'vergeten' in het tijdperk van onbeperkte opslagcapaciteit, of is het 'eens een digitale dief, altijd een digitale dief'? Hoe kan de overheid haar verantwoordelijkheid nemen voor het netwerk aan informatiestromen waaruit de digitale overheid steeds meer is opgebouwd?

In *De staat van informatie* gaan auteurs als Ybo Buruma, Paul de Hert, Michel van Eeten, Corien Prins en Albert Meijer in op deze en andere vragen. De bundel is een belangrijke bouwsteen voor het WRR-rapport *iOverheid* (2011).

ISBN 978 90 8964 310 0

Amsterdam University Press • www.aup.nl