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.