iOverheid

De Wetenschappelijke Raad voor het Regeringsbeleid werd in voorlopige vorm ingesteld in 1972. Bij wet van 30 juni 1976 (Stb. 413) is de positie van de raad definitief geregeld. De huidige zittingsperiode loopt tot 31 december 2007.

Ingevolge de wet heeft de raad tot taak ten behoeve van het regeringsbeleid wetenschappelijke informatie te verschaffen over ontwikkelingen die op langere termijn de samenleving kunnen beïnvloeden. De raad wordt geacht daarbij tijdig te wijzen op tegenstrijdigheden en te verwachten knelpunten en zich te richten op het formuleren van probleemstellingen ten aanzien van de grote beleidsvraagstukken, alsmede op het aangeven van beleidsalternatieven.

Volgens de wet stelt de WRR zijn eigen werkprogramma vast, na overleg met de minister-president die hiertoe de Raad van Ministers hoort.

De WRR is gevestigd:
Lange Vijverberg 4-5
Postbus 20004
2500 EA Den Haag
Telefoon 070-356 46 00
Telefax 070-356 46 85
E-mail info@wrr.nl
Website http://www.wrr.nl

WRR

WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

iOverheid

SYNOPSIS VAN WRR-RAPPORT 86

Wetenschappelijke Raad voor het Regeringsbeleid, Den Haag 2011

Verantwoording

Deze publicatie is een samenvatting van het WRR-Rapport nr. 86 *iOverheid* van de Wetenschappelijke Raad voor het Regeringsbeleid.

Het rapport *iOverheid* (ISBN 978 90 8964 309 4) is op 15 maart 2011 door de Raad aangeboden aan de regering. Het rapport is te koop in de boekhandel en te bestellen bij Amsterdam University Press. Het rapport kan ook in PDF-formaat worden gedownload op www.wrr.nl of www.ioverheid.nu.

Samenstelling: WRR
Vormgeving cover en binnenwerk: Studio Daniëls, Den Haag
Illustraties: Silo-Strategie. Concept. Design.

INHOUD

I SAMENVATTING VAN IOVERHEID, WRR-RAPPORT NR. 86

1 INLEIDING IOVERHEID

De kernanalyse van het rapport getiteld *iOverheid* is dat - afhankelijk van de lens waar men doorheen kijkt - twee varianten van de digitale overheid zijn te ontwaren. Allereerst is dat de welbekende eOverheid. Deze overheid komen we tegen in de beleidsdocumenten en het politieke en maatschappelijke debat. Het is de overheid die denkt, discussieert en handelt vanuit applicaties. Het is het beeld van een overheid die digitalisering primair inzet voor het verbeteren van dienstverlening en redeneert langs de lijn dat de techniek beleid en uitvoering veel te bieden heeft. Het gaat over *de* OV-chipkaart, *de* Verwijsindex Risicojongeren en *het* Elektronisch Patiëntendossier. Maar er valt ook door een andere lens te kijken en het is deze andere lens die de WRR met dit rapport wil voorhouden. Wie deze lens oppakt, ziet een wereld waar de nadruk ligt op informatiestromen en ziet pas in het verlengde daarvan de technologie die deze informatiestromen mogelijk maakt. Kijken we naar de wereld achter al die individuele, in het kader van de eOverheid ingevoerde, applicaties en digitaliseringslagen, dan ontwaren we ontelbare informatiestromen. Informatiestromen die zich een weg banen binnen en tussen de verschillende overheden. Over de grenzen van beleidsterreinen heen. Over de grenzen ook die publieke en private sector scheiden. Het is de wereld van de informatie-Overheid.

Met de term iOverheid wil dit rapport echter niet alleen een andere manier van kijken bieden. Wellicht nog veel belangrijker is dat de WRR wil wijzen op het *feitelijke ontstaan* van een geheel andere werkelijkheid dan de werkelijkheid die momenteel op de politiek-bestuurlijke radar staat. De empirische analyse toont dat er zich stapje voor stapje, besluit na besluit, in de dagelijkse praktijk een kluwen van informatiestromen ontstaat. Op rijksniveau. Op lokaal en uitvoeringsniveau. En zeker ook op het internationale en Europese niveau. De iOverheid is meer dan een optelling van beslissingen over individuele applicaties en beleidsinitiatieven. In de praktijk blijken ze veel meer samenhang te hebben dan we zouden denken als we de welbekende discussies over individuele technieken en applicaties volgen. Juist hierom, wil de WRR met de lens van de iOverheid ook aan het licht brengen dat de Nederlandse overheid, ondanks enkele zeer bescheiden aanzetten, geen noemenswaardig besef heeft van het bestaan en de consequenties van de iOverheid. En dus ook niet vanuit dat besef de ontwikkelingen binnen en buiten de overheid kan beoordelen. Laat staan daarop kan sturen. Het ontbreken van een politiek besef een iOverheid te zijn, maakt dat deze nieuwe digitale werkelijkheid in feite geen 'natuurlijke' begrenzing kent. De iOverheid is onder de politieke radar ontstaan. En ze zal onbekommerd verder groeien wanneer ze onder de politieke radar blijft. Maar ondertussen brengt de iOverheid vergaande veranderingen in de relatie tussen

burgers en overheden met zich mee. Ook resulteert ze in nieuwe kwetsbaarheden, zowel voor burgers als ook voor de overheid zelf. Met andere woorden, alhoewel de iOverheid nog nauwelijks op de politiek-bestuurlijke radar is verschenen, is ze in de praktijk van beleid en uitvoering heel concreet en heeft daarmee reële gevolgen. Vanuit deze constatering bepleit dit rapport het verankeren van 'het besef een iOverheid te zijn' als een centrale en permanente opdracht voor alle lagen van de overheid. Hiertoe doet het rapport een reeks inhoudelijke en institutionele aanbevelingen om de noodzakelijke paradigmawisseling van eOverheid naar iOverheid in goede banen te leiden.

2 INFORMATISERING VAN SAMENLEVING EN OVERHEID

Informatisering is tot in de haarvaten van de overheid doorgedrongen en bepaalt in toenemende mate het reilen en zeilen van organisaties, de professionals die er werken en de relaties die zij met burgers onderhouden. De beleidsplannen voor de eOverheid – gericht op de (interne) bedrijfsvoering, de dienstverlening van de overheid en op de techniek zelf – ademen stuk voor stuk een groot vertrouwen in ICT als middel om de overheid effectiever, klantvriendelijker, toegankelijker, kwalitatief beter en voorbereid op de toekomst te maken. In toenemende mate wordt ICT enthousiast binnengehaald door beleid en politiek voor zowel de complexe administratieve opdracht van de overheid, als de aanpak van urgente maatschappelijke uitdagingen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg. Naast dienstverlening worden ook andere overheidstaken in snel tempo gedigitaliseerd.

Deze ontwikkelingen van informatisering of digitalisering staan niet los van de veranderingen die zich breder in de Informatiesamenleving (iSamenleving) afspelen. Burgers en bedrijven maken dankbaar gebruik van de mogelijkheden die smartphones, iPads, het internet en in het bijzonder web 2.0 bieden. In korte tijd zijn invloedrijke spelers zoals Google, Facebook en Twitter op het toneel verschenen, die zich richten op de behoeften van gebruikers om informatie te zoeken en te delen en om sociale interacties op het web aan te gaan. Het is niet vreemd dat de opmars van ICT in het dagelijks leven ook de verwachtingen van burgers aangaande de overheid beïnvloedt. Niet alleen ijveren digitale burgerrechtenbewegingen voor een overheid die meer transparant is, ook verwachten veel burgers dat de overheid de nieuwe technologische mogelijkheden oppakt en benut om zowel de dienstverlening als de veiligheid te verbeteren.

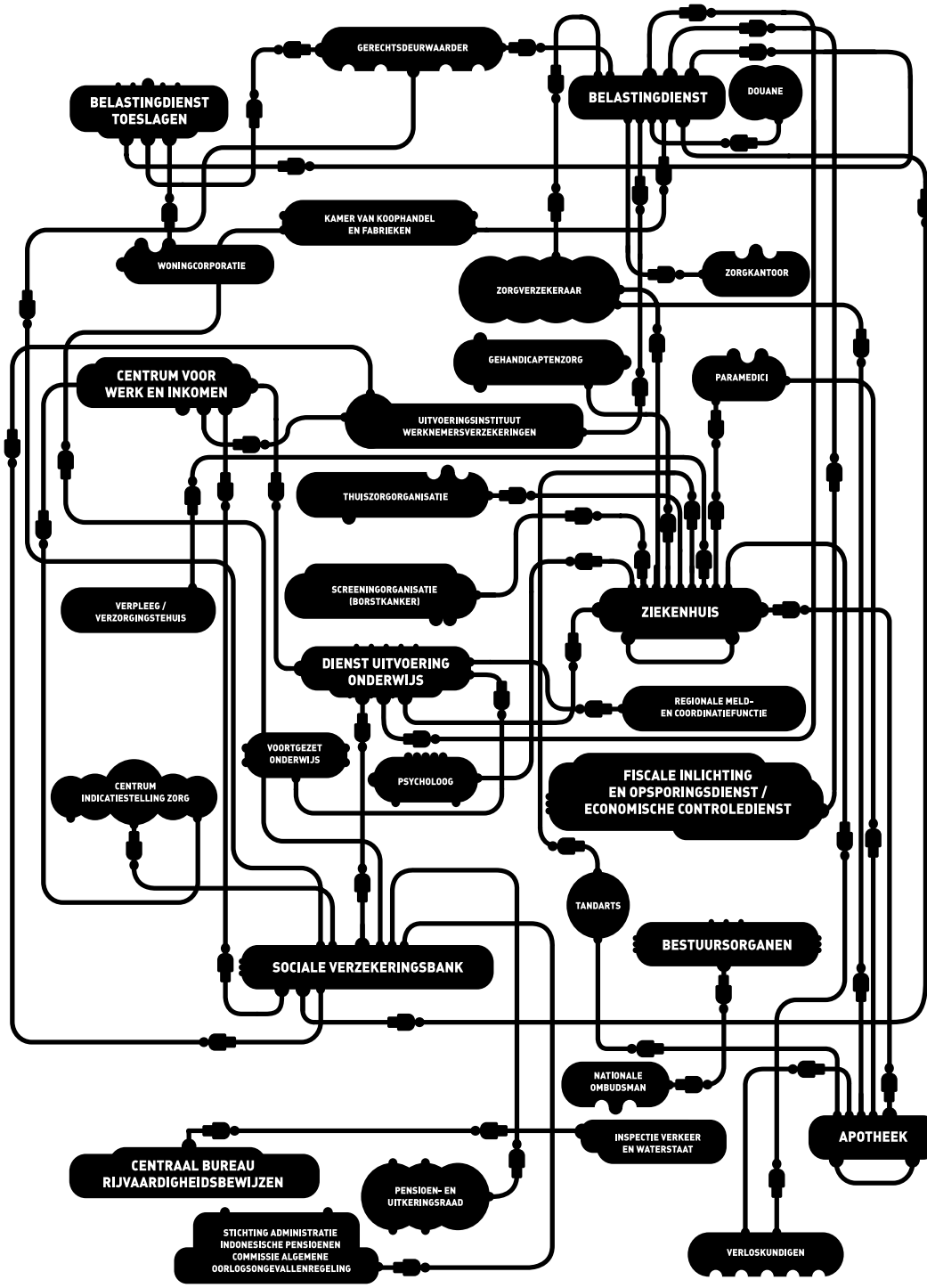
De WRR constateert dan ook dat de inzet van technologie op zowel nationaal, lokaal als Europees niveau als welhaast vanzelfsprekend wordt gezien. Technologie wordt 'uitgerold', praktijken worden 'gestroomlijnd' en diensten 'geüpdate'. Het 'technovertrouwen' van politiek en beleid vertaalt zich in grote ambities met ICT, niet alleen in technische, maar zeker ook in beleidsinhoudelijke zin. Huidige en populaire (beleids)doelen als 'maatwerk' en proactief beleid zijn ondenkbaar zonder

deze achtergrond van digitalisering. Op gebieden als veiligheid en zorg worden systemen ingezet en gekoppeld om de toekomst in kaart te brengen en daarop alvast te anticiperen. Zo moet de Verwijsindex Risicojongeren 'een nieuw Maasmeisje' voorkomen, dienen Europese migratiedatabanken te garanderen dat zich geen nieuwe illegalen in Nederland vestigen en zijn opsporingsdatabanken en grensoverschrijdend uitgewisselde passagiers- en bankgegevens er om de wereld te vrijwaren van een nieuwe terroristische aanslag. Plannen voor nieuwe systemen en de roep om meer en rijkere informatie ontstaan bovendien niet alleen in Den Haag. Op uitvoeringsniveau en binnen gemeenten groeit een wereld van verbonden systemen en informatieprocessen. En processen van globalisering zorgen ervoor dat het informatiebeleid van de Nederlandse overheid mede vorm krijgt in internationale en Europese applicaties en systemen. Ook op deze niveaus geldt een continue druk om de functies van de systemen uit te breiden, meer informatiecategorieën toe te voegen en om meer autoriteiten toegang te verlenen tot de opgeslagen informatie.

Het politieke enthousiasme voor nieuwe applicaties en koppelingen van systemen en informatiestromen gaat hand in hand met argumenten als het vergroten van de veiligheid en verhogen van effectiviteit en efficiëntie. Deze waarden zorgen, gecombineerd met het probleemoplossende 'imago' van ICT, als het ware voor zichzelf: per maatregel (een systeem, een koppeling) blijken ze in de regel zwaarder te wegen dan waarden als transparantie, privacy, keuzevrijheid of accountability. Veel bestuurlijke 'eigenaren' of pleitbezorgers van applicaties hebben de neiging om ICT als een instrument te zien, en nemen aan – en spreken dat ook regelmatig uit – dat het primaire proces niet verandert. Wie er van overtuigd is dat de inzet van technologie alleen maar van invloed is op vooropgestelde doelen als het verhogen van efficiëntie en het verbeteren van de veiligheid, heeft weinig oog voor, minder wenselijke, bijeffecten. Wanneer de ontwikkelfase van een applicatie echter achter de rug is, er heel veel in een applicatie is geïnvesteerd en het een bepaalde plaats heeft verkregen in de maatschappij vergt het veel inspanning om veranderingen door te voeren. Eenmaal 'ingeburgerd' in de dagelijkse praktijk kan een applicatie dan ook bepaalde situaties mee gaan bepalen. Zo beïnvloedt het werken met digitale dossiers in de gezondheidszorg, de manier waarop een consult verloopt. Hoewel de instrumentele dimensie van ICT belangrijk is, leidt deze houding bijgevolg ook tot een zekere armoede, die zich met name in (gebrek aan) evaluaties toont. Geloofwaardige evaluaties zijn zeldzaam en missen goede maatstaven voor de beoordeling van applicaties. De discussie blijft steken in de veiligheid van de technologie (OV-chipkaart) of in financiële debacles (zoals de diverse mislukte ICT-projecten).

Wie kijkt naar de ontwikkelingen ontwaart een aantal tendensen, die met een aantal concrete initiatieven zijn te illustreren. Als eerste is dat *function creep*. Van function creep spreekt men wanneer een systeem of een applicatie in eerste instantie functie X dient, maar daar gedurende de tijd ook functie Y of zelfs Z aan worden toegevoegd. Function creep treedt ook op als het systeem op een later tijdstip wordt

GEGEVENSSTROMEN TUSSEN (OVERHEIDS)INSTANTIES GEFACILITEERD DOOR BSN



BRON: WWW.BURGERSERVICENUMMER.NL

verbonden met andere systemen die een geheel andere functie hebben. We geven u als illustratie het SIS-systeem, een Europese databank voor politie en justitie met gegevens over mensen en objecten, zoals gestolen identiteitspapieren. Dat systeem moet het wegvallen van de fysieke grenscontroles in het Schengengebied compenseren. In eerste instantie had een relatief beperkte groep instanties toegang: de politie, grensbewaking, douane en immigratiediensten. Bij de ontwikkeling van een tweede versie van het systeem worden de mogelijkheden vervolgens sterk uitgebreid. Zo zijn ook vingerafdrukken opgenomen. Daarmee verandert het systeem al van karakter: niet meer alleen een signaleringssysteem, maar ook een opsporingssysteem. In de periode 2004-2007 krijgen bovendien diverse andere instanties toegang tot de gegevens in SIS - of delen daarvan. Instanties met geheel andere taken – antiterrorisme, opsporing van zware criminaliteit – krijgen toegang tot gegevens die in eerste instantie niet voor die taken zijn verzameld. Op Europees niveau haken Europol en Eurojust aan. Op nationaal niveau – de lidstaten van de EU – mogen instanties voor voertuigregistraties en een niet nader gedefinieerde groep van zogenaamde "nationale juridische organisaties" met het SIS koppelen. Welke organisaties dat precies zijn, mogen de lidstaten zelf uitwerken. Kortom, een bont gezelschap van nationale instanties krijgt toegang tot sis. Maar behalve langs de band van de aangekoppelde actoren, vertakt de informatiestroom zich ook op systeemniveau. Er is namelijk een koppeling met het Visum Informatie Systeem (VIS) – het systeem voor alle reizigers met een visum - beoogd. Wat we zien, is dat stap voor stap met het invoegen van nieuwe biometrische informatie en het aanhaken van nieuwe partijen en het VIS, zowel de functionaliteit als het karakter van SIS zijn veranderd.

De tweede tendens die de dagelijkse digitale praktijk ons toont is dat informatiestromen zich vrijwel niets lijken aan te trekken van bekende grenzen tussen de publieke en private sector. Discussiëren over gegevensgebruik door *de* overheid enerzijds en *het* bedrijfsleven anderzijds is kortom te simpel. Sprekend is de OV-chipkaart. Zoals u weet, sloegen vijf partijen enkele jaren geleden de handen ineen - Connexxion, het Amsterdamse GVB, het hier in Den Haag welbekende HTM, de Nederlandse Spoorwegen en de Rotterdamse RET. Ze richtten Trans Link Systems op om de OV-chipkaart gestalte te geven. Maar het bleef niet bij de partijen die destijds het voortouw namen. Een scala aan partijen oefent inmiddels invloed uit op de ontwikkeling van zowel de chipkaart als alle achterliggende informatiestromen. Allereerst heeft de overheid natuurlijk een flinke vinger in de pap. Niet alleen omdat de vijf genoemde vervoerders merendeels in publieke handen zijn (zo is Connexxion bijvoorbeeld voor 1/3 in handen van het Ministerie van Financiën). Maar ook omdat de rijksoverheid zich bemoeit met prijzen, betaalvormen en prestaties. En omdat het Openbaar Ministerie reizigergegevens opvraagt bij Trans Link. De private sector stuurt via de deelnemende openbaar vervoersbedrijven en de leveranciers die zijn verenigd in het speciaal opgerichte consortium East West e-ticketing. Dit levert een kluwen van partijen op, uit zowel het publieke en private domein. Soms zijn die verschillende belangen zelfs verenigd in één en dezelfde partij.

Maar niet alleen de grens tussen publiek en privaat wordt diffuus. Het rapport bespreekt een veelheid aan initiatieven waar ook de schotten binnen de overheid – dat wil zeggen tussen beleidsterreinen - afbrokkelen. Informatie die in eerste instantie wordt verzameld voor dienstverlening wordt vervolgens gebruikt voor controle en handhaving. Informatie uit het domein van de zorg komt terecht bij instanties die zich met controle bezighouden. Illustratief is de Verwijsindex Risicojongeren – de VIR. Dit systeem moet ervoor zorgen dat instanties die bemoeienis hebben met jongeren tijdig van elkaar weten dat een jongere een risico loopt. De VIR maakt het mogelijk dat organisaties elkaar via een signaal van hun bezorgdheid op de hoogte kunnen stellen. Tragische gebeurtenissen als 'het Maasmeisje' moeten zo worden voorkomen. Wie goed kijkt ziet dat instanties verdeeld over zes nogal verschillende domeinen signalen afgeven: jeugdzorg, jeugdgezondheidszorg, onderwijs, maatschappelijke ondersteuning, werk en inkomen, politie en justitie. Achter die domeinen gaan tientallen organisaties schuil. Stuk voor stuk met elkaar verbonden via de VIR. Natuurlijk is het systeem op de tekentafel sober en werkt louter op basis van signalen. Willen professionals over inhoudelijke informatie beschikken dan moeten ze persoonlijk contact leggen. Maar op de werkvloer wordt uitgewisselde informatie genoteerd, gedigitaliseerd en eindigt in leerdossiers, elektronisch kinddossiers, politiesystemen, etc.

Bovendien is de VIR illustratief voor nog meer tendensen. Plannen voor nieuwe systemen en de roep om meer en rijkere informatie ontstaan niet alleen hier in Den Haag. Op uitvoeringsniveau en binnen gemeenten groeit een wereld van verbonden systemen en informatieprocessen. Zo is de VIR slechts een landelijke paraplu boven vele lokale systemen. Dat zijn systemen als Zorg voor Jeugd, VIS2, Multisignaal en SISA in Rotterdam, dat gebruik maakt van Multisignaal. Wie goed naar dit lokale niveau kijkt, ziet een nog grotere rijkdom aan partijen die met elkaar in verbinding staan. Partijen die niet meldingsbevoegd zijn voor de nationale verwijsindex, maar op lokaal niveau wel signalen afgeven. Partijen ook, die in sommige situaties via het lokale systeem meer uitwisselen dan kale signalen. Allemaal partijen die gegevens delen om op basis daarvan weer nieuwe informatie samen te stellen. En dat betekent onherroepelijk dat informatie eerst wordt gede-contextualiseerd om vervolgens te worden hercontextualiseerd. Met, zo laat de WRR zien, alle risico's van dien. Niet alleen voor burgers. Zeker ook voor de overheid zelf. Zo is de verantwoordelijkheid voor de kwaliteit en betrouwbaarheid van informatie niet meegeëvolueerd met het koppelen en uitwisselen van informatie in combinatie met de erosie van schotten tussen beleidsterreinen, tussen overheidsorganisaties en in relatie tot de private sector. De verantwoordelijkheid voor (de juistheid van) informatie is niet scherp belegd waardoor burgers er rekening mee moeten houden dat 'hun' informatie in publieke en private handen een eigen leven kan gaan leiden. Bovendien, doordat het technisch steeds gemakkelijker wordt informatiestromen aan elkaar te knopen (daarbij gefaciliteerd door unieke nummers (BurgerServiceNummer) en authentieke regis-

traties), wordt informatie toegankelijker en, zeker wanneer het informatienetwerk heel uitgebreid is, tegelijk ook moeilijker te controleren. Persoonlijke informatie uit verschillende sferen – bijvoorbeeld gegevens bekend bij de Belastingdienst, gecombineerd met gegevens gevonden op het internet – kan tot een digitaal profiel leiden. Profielen kunnen op hun beurt dan weer gebruikt worden voor tal van doeleinden: van een vooraf ingevulde belastingaangifte tot persoonlijke reclame in de e-mailbox.

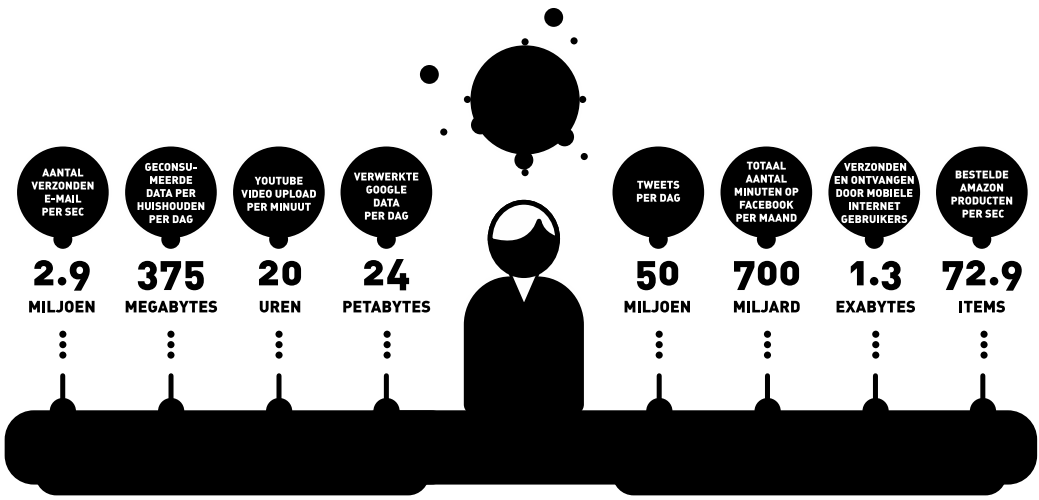
Alle hiervoor genoemde, maar ook tientallen andere initiatieven worden in het politieke debat gepropageerd, bediscussieerd en beoordeeld vanuit een scala aan motieven, ideeën en normatieve oriëntaties. De meest bekende daarvan zijn efficiëntie, effectiviteit, veiligheid, privacy en transparantie. De uiteindelijke vorm die een nieuw systeem of een nieuwe koppeling van informatiebronnen krijgt is de uitkomst van een complexe dynamiek tussen al deze maatstaven. Die uitkomst betreft niet alleen het technologisch ontwerp – vaak de focus van het debat –, maar vooral ook de sociale, bestuurlijke en juridische uitwerking die veel minder prominent aan bod komt. Om enerzijds meer helderheid binnen deze dynamiek aan te brengen en anderzijds handvatten te bieden voor de noodzakelijke afwegingen die tussen de motieven gemaakt dienen te worden, brengt de WRR ze onder in drie betekenisclusters: stuwende beginselen (zoals veiligheid, effectiviteit en efficiëntie), verankerende beginselen (privacy en keuzevrijheid) en procesmatige beginselen (transparantie en accountability).
Stuwende beginselen zijn verbonden met de *drive* van de overheid om ICT in tal van domeinen in te zetten en staan in het teken van verbetering en kwaliteitswinst. Verankerende beginselen staan voor het waarborgen van vrijheden, het in kaart brengen van 'stille verliezen' bij voortgaande digitalisering en voor het vrijwaren van de autonomie van het individu. Ze vormen als het ware een tegenwicht voor de stuwende beginselen. Procesmatige beginselen ten slotte staan voor de procedurele omlijsting die het mogelijk maakt dat afweging tussen de stuwende en verankerende beginselen met name inzichtelijk en toetsbaar is.

3 iOVERHEID ALS REALITEIT

Dit rapport laat zien dat de overheid stapje voor stapje, besluit na besluit, onder invloed van digitalisering fundamenteel van karakter verandert. Er is feitelijk en bijna ongemerkt een situatie ontstaan waarin samenhangende informatiestromen het karakter van de overheid domineren. En daarmee bepalen deze informatiestromen de nieuwe mogelijkheden, maar ook de afhankelijkheden en de kwetsbaarheden voor zowel de overheid als haar burgers. In de dagelijkse werkelijkheid van politiek en bestuur wordt echter allesbehalve vanuit het samenhangende idee van deze informatie-Overheid – *iOverheid* – gedacht en gewerkt. Het overgrote deel van de overheidsinitiatieven voor digitalisering en de informatiestromen die daaruit volgen worden los van elkaar bepleit, beoordeeld en ingevoerd. Individuele initiatieven worden niet of nauwelijks beoordeeld op hun (potentiële) invloed op de overheid

en de samenleving als geheel. Wat daardoor vooral ontbreekt is een perspectief op de snelgroeiende en vertakkende informatiestromen. De iOverheid staat niet op het netvlies van politiek en beleid en dat is gezien de gestaag verdergaande informatisering problematisch. Het ontbreekt paradoxaal genoeg aan een politiek besef van de implicaties van het hele bouwwerk van de iOverheid, terwijl toch (bijna) alle bouwstenen zijn voortgekomen uit politieke besluitvorming. Aan deze paradox zal een einde moeten worden gemaakt.

De opeenstapeling van ad-hocbesluiten over nieuwe technieken, het ontbreken van een besef van het ontstaan van een iOverheid en het gebrek aan debat daarover, maken dat de iOverheid zich als het ware 'grenzeloos' ontwikkelt. De grenzen aan de uitwaaiering van individuele applicaties en de verknoping van informatiestromen zijn niet gegeven, omdat niemand zich hoeder voelt van het geheel. Het verzamelen van steeds meer informatie en het aanleggen van koppelingen daartussen lijkt nauwelijks meer in het gareel te krijgen. Het resultaat is dat informatie vervuilt, onduidelijk is wie verantwoordelijk is voor informatiestromen en dat burgers, bedrijven en ook instanties binnen de overheid zelf, verst(r)ikt raken in de datakluwen van de overheid. Het meest bekende voorbeeld daarvan is de zaak van heer Kowsoleea, die vele jaren werd achtervolgd door het feit dat een ander, die zich met criminele activiteiten bezig hield, zich voor hem uitgaf. Het bleek onmogelijk om de zaken in de digitale 'backoffice' van de overheid weer recht te zetten. Maar er zijn veel meer voorbeelden te geven van de vervormingen waaraan informatie in digitale bestanden kan (gaan) lijden. Zo werd een grote groep zelfstandige ondernemers (zzp'ers) ten onrechte beschuldigd van fraude, nadat de Belastingdienst en het UWV een verkeerde interpretatie hadden gegeven aan de uitkomsten van een bestandskoppe-



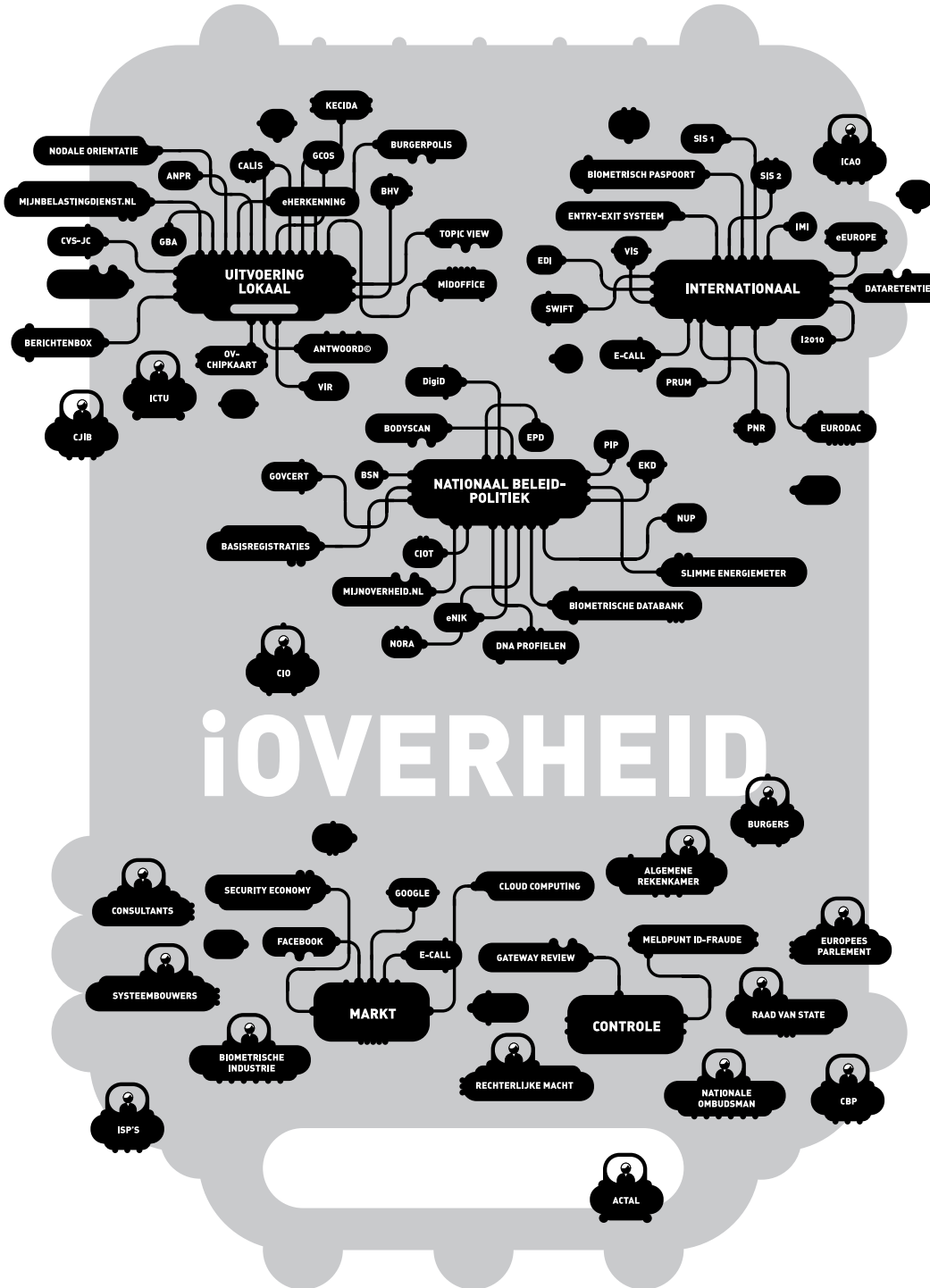
BRONVERMELDING: GOOD MAGAZINE/ OLIVER MUNDAY/ IBM
(GEBASEERD OP GEGEVENS VAN CISCO, COMSCORE, MAPREDUCE, RADICATI GROUP, TWITTER, YOUTUBE)

ling die ze hadden uitgevoerd om fraude op te sporen. Politieke en bestuurlijke vragen en afwegingen op het niveau van de samenhang van informatiestromen en de gevolgen daarvan blijven liggen. Dat maakt niet alleen burgers, maar zeer zeker ook de overheid zelf kwetsbaar. Het bredere perspectief van de iOverheid en een zorgvuldige en toetsbare afweging tussen de stuwende, verankerende en procesmatige beginselen ontbreekt in het Nederlandse politiek-bestuurlijke debat.
Alhoewel de iOverheid feitelijk nog sterk in opbouw en ontwikkeling is, en begripsmatig nog nauwelijks op de radar is verschenen, heeft ze wel degelijk al reële gevolgen, bijvoorbeeld voor de genoemde burgers die in de knel komen. Deze gevolgen worden vanwege het gebrekkige 'bewustzijn' van de karakteristieken van de iOverheid nauwelijks in de beleidsontwikkeling betrokken, en ontbreekt het aan een goed politiek-bestuurlijk besef van wat zich ontwikkelt, laat staan van een besef *hoe* die ontwikkeling in goede banen is te leiden. Wil de Nederlandse overheid de verdere digitalisering in zorgvuldige banen leiden, waarbij er tegelijkertijd ruimte is voor innovatie met behulp van ICT, dan zal ze in woord en daad de transformatie van een eOverheid naar een iOverheid dienen te maken. De centrale opdracht voor de overheid, of eigenlijk voor alle lagen van de overheid, is om te beseffen dat ze een iOverheid is geworden, met alle consequenties van dien. Deze opgave vereist een inhoudelijk andere oriëntatie, gecombineerd met de ontwikkeling van een bijbehorend institutioneel kader. Daarbij is het van groot belang dat afscheid wordt genomen van de nauwe blik op individuele applicaties en dat de aandacht zich verlegt naar de vernetwerkte informatiehuishouding van de overheid. Tot slot vergt de vormgeving van een iOverheid een open houding naar de ontwikkelingen binnen de informatiesamenleving (iSamenleving). De iOverheid kan niet vanuit een ivoren toren worden vormgegeven, en moet dus het credo "Betrek de iSamenleving bij de duurzame uitbouw van de iOverheid" volgen.

4 BESTUURLIJKE UITGANGSPUNTEN VOOR DE iOVERHEID

Bij de inhoudelijke opdracht voor de bestuurlijke transformatie naar een iOverheid zijn twee zaken van wezenlijk belang. Een zorgvuldige ontwikkeling van de iOverheid kan allereerst niet zonder een open afweging tussen de stuwende, verankerende en de procesmatige beginselen. Hiernaast geldt dat van de overheid bij zowel deze afweging als de verdere inrichting van beleid en uitvoering extra behoedzaamheid verlangd mag worden wanneer sprake is van een drietal in dit rapport gesignaleerde processen van informatieverwerking. Deze processen – symbolisch aangeduid als waarschuwingsvlaggen – houden verband met a) het vernetwerken van informatie, b) het samenstellen en verrijken van informatie en c) het voeren van preventief beleid op basis van informatie.

Het eerste bestuurlijke uitgangspunt is dat de drie in dit rapport gehanteerde clusters van beginselen – stuwend, verankerend en procesmatig – op alle niveaus waar beslissingen worden genomen met elkaar in balans moeten worden gebracht. Dit is


KECIDA
NODALE ORIENTATIE
CALIS
GCOS
BURGERPOLIS
ANPR
BHV
MIJNBELASTINGDIENST.NL
eHERKENNING
CVS-JC
GBA
TOPIC VIEW
UITVOERING LOKAAL
MIDOFFICE
BERICHTENBOX
OV-CHIPKAART
ANTWOORD©
ICTU
VIR
CJIB
SIS 1
ICAO
BIOMETRISCH PASPOORT
SIS 2
ENTRY-EXIT SYSTEEM
IMI
eEUROPE
EDI
VIS
INTERNATIONAAL
DATARETENTIE
SWIFT
i2010
E-CALL
PRUM
PNR
EURODAC
DigiD
BODYSCAN
EPD
PIP
EKD
GOVCERT
BSN
NATIONAAL BELEID-POLITIEK
NUP
BASISREGISTRATIES
CIOT
SLIMME ENERGIEMETER
MIJNOVERHEID.NL
BIOMETRISCHE DATABANK
eNIK
NORA
DNA PROFIELEN
CIO
iOVERHEID
BURGERS
ALGEMENE REKENKAMER
CONSULTANTS
SECURITY ECONOMY
GOOGLE
CLOUD COMPUTING
EUROPEES PARLEMENT
FACEBOOK
E-CALL
GATEWAY REVIEW
MELDPUNT ID-FRAUDE
SYSTEEMBOUWERS
MARKT
CONTROLE
RAAD VAN STATE
BIOMETRISCHE INDUSTRIE
RECHTERLIJKE MACHT
NATIONALE OMBUDSMAN
CBP
ISP'S
ACTAL

geen geringe opgave, aangezien een kwantitatief getint concept als efficiëntie, en een meer normatief concept als keuzevrijheid of een procesmatig concept als accountability, duidelijk in verschillende registers van analyse thuishoren. Toch vereist een evenwichtige ontwikkeling van de iOverheid een doordachte afweging tussen deze clusters van beginselen, waarbij ze geëxpliciteerd, toetsbaar en publiekelijk verantwoord moeten worden. Dat is nu te weinig het geval. De overheid moet haar eigen afwegingen zo expliciet mogelijk wereldkundig maken, en wel op alle niveaus: van de voorbereiding en introductie van een concrete toepassing tot aan de omvattende vertakking van processen en informatiestromen waaruit de iOverheid is opgebouwd. Dat geldt niet alleen voor het nationale niveau, maar ook voor de afwegingen die op het internationale, en met name op het Europese niveau worden gemaakt. Het expliciet en zoveel mogelijk toetsbaar maken van de beginselen zou een aantal zaken laten uitkomen en openlijk bespreekbaar maken. Bijvoorbeeld dat vaak sprake is van ongefundeerd politiek-bestuurlijk optimisme ten aanzien van de mogelijkheden van ICT, hetgeen een van de onderliggende redenen is voor onhaalbare deadlines en kostbare ICT-mislukkingen. Het maken van expliciete afwegingen zou ook duidelijk maken dat latere ad hoc uitbreidingen van de reikwijdte van een ICT-toepassing (de zogenaamde *spill* over en *function creep*) vaak vooraf al stilletjes zijn ingecalculeerd. Het werkelijke besef een iOverheid te zijn vereist dat de politiek de uitdrukking 'regeren is vooruitzien' ook serieus neemt in het digitale domein en toepast op de impliciete, maar voorzienbare toekomstige ontwikkelingen van informatisering. De overheid neemt in haar beleid vaker een voorschot op de toekomst en het zou haar sieren om dat in de politieke afweging ook, en met een open vizier, te doen.
De inhoudelijke opgave vereist als tweede bestuurlijke uitgangspunt dat de overheid bij de verdere informatisering een aantal kenmerken van informatie veel bewuster in acht neemt dan nu het geval is. Daarbij gaat het om *processen* van informatieverwerking en -gebruik, juist omdat die processen van grote invloed zijn op het karakter en de betrouwbaarheid van de informatie waarop de iOverheid draait. Aan drie, onderling gerelateerde, processen worden waarschuwingsvlaggen meegeven, die extra alertheid van de overheid vragen, vooral op de kwaliteit van informatie en op de vraag wie er verantwoordelijk is voor de juistheid daarvan.

- Het *vernetwerken* van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren.
- Het *samenstellen en verrijken* van informatie, i.e. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten.
- Het voeren van *preventief* en proactief beleid op basis van informatie, i.e. het actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicocalculatie.

Deze drie informatieprocessen vormen de kern van de iOverheid en stellen haar in staat om beleid te verfijnen, op maat te snijden, een omvattend beeld te verkrijgen van burgers en beleidsproblemen en daar waar nodig proactief op te handelen. Bij-

voorbeeld beginnen zogenaamde burgerprofielen een steeds grotere rol te spelen in het overheidshandelen, met name op terreinen waar van de overheid verwacht wordt dat zij gevaren afwendt nog voordat het misgaat, zoals in de jeugdzorg. Het is dan ook niet verwonderlijk dat profielen een belangrijk onderdeel vormen van de Verwijsindex Risicojongeren (VIR). Tegelijkertijd zijn dit ontwikkelingen die van invloed zijn op informatie zelf: op het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid van informatie. Veel meer dan nu het geval is dient het besef door te dringen dat het juist deze drie ontwikkelingen zijn die grote gevolgen hebben voor (a) de *inhoudelijke* kwaliteit van informatie en (b) voor de eisen aan de *organisatorische* inbedding van informatiestromen. Voortdurende rijksbrede en proactieve aandacht voor de kwaliteit en kwetsbaarheid van informatie en informatieprocessen is daarom van groot belang. Ook is een veel grotere mate van openheid en transparantie richting burgers noodzakelijk om hen inzicht te bieden in de informatie die over hen is vergaard, en hen tevens te faciliteren de informatie waar nodig te corrigeren. Burgers staan nu vrijwel machteloos als zij persoonlijk worden geconfronteerd met fouten in de uitgestrekte informatienetwerken van de iOverheid die soms grote gevolgen hebben. Tenslotte vraagt het 'geheugen' van de iOverheid expliciete aandacht. Zowel het belang van 'vergeten' – mensen moeten niet voor eeuwig afgemeten worden aan de informatie die de overheid over ze heeft opgeslagen – als dat van bewaren en archiveren verlangt een radicale cultuuromslag en een verankerde strategie.

5 GRENZEN AAN DE GROEI VAN DE iOVERHEID

Een onbewuste iOverheid zal de natuurlijke neiging hebben om verder te groeien: 'grenzen aan de groei' komen pas met bewustzijn in zicht. Zonder een besef van de iOverheid en wat deze betekent voor de verhouding overheid-burger is er weinig reden of gelegenheid om stil te staan bij de groei van het informatiebouwwerk dat de overheid in uitvoering heeft. Ook geeft het weinig reden tot het stellen van vragen: of dit nodig is, of er behoefte aan en noodzaak tot begrenzing is en hoe het zich verder dient te ontwikkelen. Een zorgvuldige inrichting en ontwikkeling van de iOverheid vereist echter het durven stellen van grenzen aan die overheid. Hoewel dit rapport die grenzen niet markeert – die zijn in essentie politiek – geeft het wel aan welke grensgebieden overwogen moeten worden. Allereerst dwingt de combinatie van een expliciete afweging van beginselen en het in acht nemen van de waarschuwingsvlaggen tot nadenken over de grenzen van de iOverheid. Ook de vermenging tussen service, care en control en de diffuse grenzen tussen publieke en private informatiestromen – die ongemerkt heel gewoon zijn geworden – kunnen aanleiding zijn tot het stellen van grenzen. Van groot belang is ook de constatering dat het internet een totaal andere informatieomgeving heeft gecreëerd waaraan ook de iOverheid zich niet kan onttrekken en waarbinnen ze heeft te functioneren. De snelheid waarmee informatie – ook als die de overheid onwelgevallig is – wordt

verspreid en gekopieerd, maakt bijvoorbeeld dat de overheid ook na zal moeten denken over haar eigen informatiemanagement. Dat heeft de WikiLeaks-affaire overtuigend laten zien. Ook in relatie tot deze 'buitenwereld' kunnen beredeneerde begrenzingen van groot belang zijn.

6 EEN INSTITUTIONELE AGENDA VOOR DE TRANSFORMATIE NAAR EEN iOVERHEID

Gericht werken aan een zorgvuldige uitbouw van de iOverheid vraagt niet alleen in inhoudelijke zin, maar ook op institutioneel niveau om de nodige aanpassingen. Een overheid die op digitaal vlak van gedaante is veranderd heeft zich ook in organisatorisch opzicht aan te passen. Een op informatieniveau verknoopte overheid verlangt een verantwoordelijkheidsstructuur die past bij de nieuwe realiteit en is voorzien van de nodige slagkracht. Het probleem is echter dat de kern van de iOverheid schuilt in de samenhang van informatiestromen en netwerken, en juist op dat punt geldt dat er geen organisaties zijn die zich om het geheel (kunnen) bekommeren. Er is geen 'ministerie van' of 'Kamercommissie voor Informatie'. Dat maakt dat het 'besef een iOverheid te zijn' geen rustig bezit is, maar een permanente opgave die uiteindelijk in alle lagen van de overheid moet worden verankerd, maar op de korte termijn centraal moeten worden aangejaagd. Om de doelen voor de iOverheid handen en voeten te geven is daarom een institutionele transformatie nodig die drie functies bij de overheid belegt en verankert.

a. De *strategische functie*, i.e. het waarborgen van een weloverwogen verdere ontwikkeling van de iOverheid.
b. De *maatschappelijke functie*, i.e. het versterken van de transparantie van de iOverheid voor burgers en het versterken van de accountability van de iOverheid ten opzichte van burgers die in informatienetwerken verstrikt raken.
c. De *operationele functie*, i.e. het verbeteren van de weloverwogen aansluiting tussen beleid, uitvoering, technologie en informatiestromen en netwerken. Het verbeteren van het opdrachtgeverschap van de overheid.

Deze drie functies vormen de absolute ondergrens van wat nodig is om het besef van de iOverheid vorm te geven en te handelen naar de consequenties die de nieuwe realiteit met zich meebrengt. Het is niet eenvoudig om de bij deze drie functies behorende instituties goed vorm te geven, maar het is wel zaak deze functies daadwerkelijk aan organisaties toe te vertrouwen en die organisaties 'tanden' te geven . In navolging van de empirische realiteit moet de overheid dus zelf in institutionele zin transformeren van een eOverheid naar een iOverheid. Daarbij moet in de gaten worden gehouden dat de institutionele transformatie als zodanig vele malen belangrijker is dan de in dit rapport voorgestelde (naambordjes van) instituties. Dàt de functies worden vervuld is belangrijker dan de vraag door wie ze worden vervuld. Op het strategische niveau stelt de WRR voor om een permanente commissie voor

de iOverheid in te stellen die processen van digitalisering beschouwt en beoordeelt in het licht van de iOverheid als geheel en die aan het parlement rapporteert. De centrale taak van deze commissie is om ontwikkelingen te signaleren, met elkaar in verband te brengen, en te doordenken vanuit het perspectief van de iOverheid, dat wil zeggen over grenzen van departementen en overheidslagen heen en in het perspectief van de mogelijke toekomstige ontwikkelingen. Ook de 'beweeglijkheid' van de iOverheid over de internationale grenzen en publiek-private scheidslijnen heen wordt in de analyse meegenomen. Op het niveau van de maatschappelijke functie bepleit de WRR de oprichting van een iPlatform om de transparantie van de iOverheid ten opzichte van burgers te centraliseren en vergroten. Net zoals de overheid bij haar dienstverlening streeft naar een één-loketgedachte, zou de overheid ook hier naar één ingang moeten streven. Het iOverheidsplatform moet een interactief informatiepunt zijn over informatisering in de relatie tussen de burger en de overheid. De accountability kan vorm en inhoud krijgen via een iAutoriteit die verantwoordelijk is voor de afhandeling van problemen die burgers ondervinden met de iOverheid. De iAutoriteit moet het probleem letterlijk uit handen van de burger nemen om het in de ketens en netwerken van de iOverheid recht te zetten en op te lossen. Om de dynamiek van het kastje naar de muur te doorbreken moet hier expertise en een persoonlijke behandeling worden gecombineerd met een stevige doorzettingsmacht ten opzichte van de organisaties die het netwerk van de backoffice van de iOverheid bevolken. Op het operationele niveau ten slotte is het van groot belang het opdrachtgeverschap te professionaliseren en kennis op het snijvlak van techniek en beleid te prioriteren in plaats van kennis van de techniek zelf. Op de tekentafels van de techniek en in de (internationale) gremia van de standaarden wordt immers bepaald hoe de iOverheid er in de praktijk uit komt te zien. Het besef dat dit in essentie politieke en beleidsmatige keuzes zijn, valt in de praktijk nu nog vaak weg tegen de gedachte dat techniek niet meer dan een instrument is.

In de kern gaat dit rapport over de verantwoordelijkheid van de overheid voor haar eigen gebruik van . Maar de overheid heeft uiteraard ook een rol te spelen in de informatiesamenleving. Behalve de verantwoordelijkheid voor de iOverheid berust bij de overheid ten principale ook een zekere verantwoordelijkheid voor het functioneren van de iSamenleving. Wat dient de overheid zich in de ontwikkeling van de informatiesamenleving aan te trekken en (hoe) heeft zij daarin te interveniëren? Burgers en bedrijven worden voortgestuwd door enthousiasme voor nieuwe technische mogelijkheden en overwegingen van winstgevendheid. Waar deze structureel onvoldoende worden afgewogen tegen verankerende beginselen en onvoldoende in balans worden gebracht met een uitwerking van procesmatige beginselen die informatiestromen voor burgers transparant en, indien nodig, bekritiseerbaar maken, dient de iOverheid zich in ieder geval af te vragen of ze aan zet is.

Tenslotte, in de dagelijkse praktijk zal de ontwikkeling van de iOverheid zonder twijfel onverminderd doorgaan. Zoveel kunnen we van de geschiedenis van de

digitalisering wel aflezen. Een halt toeroepen is kortom geen optie. Het is voor de WRR echter onontkoombaar dat politiek en bestuur de komende jaren de draai van een eOverheid naar een iOverheid hebben te maken. Evenzeer zal men de ogen niet langer kunnen sluiten voor de verantwoordelijkheid die een politiek bewuste en afgewogen verdere ontwikkeling van deze iOverheid met zich meebrengt en aan acties verlangt.

II AANBEVELINGEN: WERKEN AAN DE iOVERHEID

De overheid dient te beseffen dat ze een iOverheid is. Dat besef is van vitaal belang om enerzijds de uitdagingen van de almaar verdergaande digitalisering het hoofd te bieden en anderzijds innovatie met behulp van digitalisering te kunnen benutten. Redeneren vanuit het besef een iOverheid te zijn betekent dat de overheid verder kijkt dan naar de techniek en individuele applicaties, maar de blik verlegt naar het perspectief van de iOverheid. Vanuit dat perspectief dient de aandacht uit te gaan naar de informatiestromen die het resultaat zijn van de vele applicaties en koppelingen daartussen. Bovenal moet de aandacht zich richten op de maatschappelijke en beleidsmatige gevolgen van continue uitbouw en dynamiek van de iOverheid.

Het is verleidelijk om voor de noodzakelijke transformatie en de daarmee samenhangende maatregelen een departement, organisatie of ambt aan te wijzen: één centraal punt dat vanuit een totaaloverzicht op de iOverheid de verantwoordelijkheid daarvoor draagt. Dat is echter een grotendeels onbegaanbare weg, gezien de omvang, complexiteit en gedetailleerdheid van de implicaties van ICT voor de relatie burger-overheid. Dit rapport kan geen alomvattende strategie of een blauwdruk voor een evenwichtige ontwikkeling van de iOverheid leveren en verwacht ook niet dat 'de' overheid dat kan. Het besef van de iOverheid en de consequenties daarvan zullen moeten inzinken in de vele lagen en instituties van de overheid: departementen, agentschappen, gemeenten, politie, toezichthouders, burgers en, *last but not least*, politici. De iOverheid is de facto ontstaan op vele plekken binnen de overheid en het besef van de consequenties daarvan zal dezelfde weg moeten volgen. Dat gezegd zijnde geldt natuurlijk altijd dat sommigen meer gelijk zijn dan anderen. In dit laatste hoofdstuk wordt aan enkele organisaties een grote verantwoordelijkheid toebedeeld om dit besef uit te dragen en de consequenties van deze ontwikkelingen in goede banen te leiden. Deze 'taken' moeten worden gezien als de organisatorische uitwerking van een agenda van transformatie voor de Nederlandse overheid. De transformatie van een eOverheid naar een iOverheid is een paradigmawisseling die zich de facto al heeft ontvouwd, maar nu ook hoognodig ingebed moet worden in het denken en de instituties van de Nederlandse overheid. Daarbij geldt dat de transformatieve agenda veel belangrijker is dan de concrete suggesties voor de institutionele inbedding daarvan. Er zijn meerdere wegen die naar Rome leiden, maar de overheid kan het zich niet veroorloven om niet in Rome aan te komen.

Vanuit deze observatie wordt in de eerste drie paragrafen van dit hoofdstuk een aantal normatieve en procedurele aanbevelingen uitgewerkt. Paragraaf 1 formuleert daartoe allereerst aanbevelingen op het niveau van de driedeling in stuwende, verankerende en procedurele beginselen die eerder in dit rapport werden gepresenteerd en in de empirische analyse een belangrijke rol speelden. Paragraaf 2 on-

derscheidt vervolgens op basis van deze analyse een drietal karakteristieken van informatie die als 'waarschuwingsvlaggen' hebben te gelden voor een bewuste iOverheid. Het gaat daarbij niet om typen informatie, maar om *kenmerken* van informatie die om speciale waarborgen vragen, zowel voor de overheid zelf als in de relatie overheid-burger. Aan de hand van deze waarborgen worden in paragraaf 2 twee aanbevelingen geformuleerd, die daarmee ook de opmaat vormen tot de noodzakelijke reflectie, aangekaart in subparagraaf 2.3, over de begrenzing van de iOverheid. Ten slotte presenteren de paragraaf 3 de ingrediënten voor de institutionele inrichting om het 'besef een iOverheid te zijn' te verankeren.

1 EXPLICIETE AFWEGING VAN STUWENDE, VERANKERENDE EN PROCEDURELE BEGINSELEN

De dynamiek tussen de stuwende beginselen – zoals effectiviteit & efficiëntie en veiligheid – en de verankerende beginselen – zoals privacy en keuzevrijheid – is, zo laat de empirie zien, sterk sturend voor de ontwikkeling van de iOverheid. Ook de invulling van procedurele noties zoals transparantie en accountability laat zien wat de moeilijkheden, mogelijkheden en (gemiste) kansen zijn om de ontwikkeling van de iOverheid normatief-institutioneel in te bedden. Op de persoon af gevraagd zal nagenoeg elke bestuurder, politicus en ambtenaar het belang van al deze beginselen onderschrijven. Ze appelleren immers allemaal aan gezond verstand, verantwoordelijkheid, grondwettelijke waarden en zorgvuldigheid. Niemand is faliekant tegen veiligheid of tegen privacy, om die twee begrippen die het vaakst tegen elkaar uitgespeeld worden maar als voorbeeld te nemen. Wederom op de persoon af gevraagd zal iedereen zeggen dat deze beginselen in een zorgvuldig proces onderling tegen elkaar afgewogen moeten worden. Besluitvorming moet immers altijd gebalanceerd zijn. In theorie althans kan men het in de regel wel met elkaar eens worden. De praktijk, zo blijkt uit de analyse in deel 2 van dit rapport, is echter vaak een heel andere. ICT is – het is eerder gezegd – vaak veel meer een politieke keuze dan een puur instrumentele oplossing voor een probleem. En politiek is nu eenmaal strijd. In de dagelijkse werkelijkheid van de iOverheid in wording is de afweging van de verschillende beginselen in de regel een minder evenwichtige en openbare aangelegenheid dan de theorie doet vermoeden. Dat heeft een aantal redenen: a) de beginselen worden zelden expliciet gemaakt en openlijk bediscussieerd, b) de beginselen zijn ongelijksoortig en daarom moeilijk te duiden en tegen elkaar af te wegen en c) er valt politiek en bestuurlijk wat te winnen bij een onevenwichtige voorstelling van zaken. Deze redenen worden hieronder uitgewerkt en in het licht geplaatst van een tweetal aanbevelingen om de afwegingen en het debat over de iOverheid op het niveau van de beginselen meer open, expliciet en realistisch vorm te geven.

De drie in dit rapport gehanteerde clusters van beginselen – stuwend, verankerend en procesmatig – moeten op alle niveaus waar beslissingen worden genomen met elkaar in balans worden gebracht. Dit is geen geringe opgave, aangezien een kwan-

titatief getint concept als efficiëntie enerzijds, en een meer normatief concept als keuzevrijheid of een procesmatig concept als accountability anderzijds, duidelijk in verschillende registers van analyse thuishoren. Stuwende beginselen zoals efficiëntie en veiligheid hebben bovendien, zo laat de empirie zien, weinig steun in de rug nodig om voor het voetlicht te treden.

Voor de verankerende beginselen ligt dat vaak anders. Zij zijn gegrond in de vrijheid en autonomie van burgers en uitgewerkt in de beginselen privacy en keuzevrijheid. Ondanks de absolute en grondrechtelijke klank van het begrip vrijheid, blijken deze noties in de praktijk van alledag veel plooibaarder dan de argumenten die aan de andere kant van de balans, in het domein van efficiëntie en veiligheid, worden neergelegd. Het argument voor verankering ligt veelal in de potentiële schending van individuele belangen die in een afweging soms eenvoudig het onderspit delven tegen de gepercipieerde belangen van het collectief. De privacy van individuen weegt daarmee vaak niet op tegen de veiligheid van het collectief. De spil van de toezichthoudende en rechterlijke toetsing wordt vrijwel altijd gevormd door de vraag of de inbreuk op een grondrecht evenredig is. Er is eigenlijk geen gemeenschappelijke eenheid of valuta die een quasimathematische afweging tussen deze ongelijksoortige categorieën van beginselen (stuwend enerzijds, verankerend anderzijds) mogelijk maakt. Wanneer toch wordt gepoogd de afweging in één bepaald keurslijf te dwingen – bijvoorbeeld in een kosten-batenanalyse – dan bestaat het risico dat de overwegingen (en de taal) van effectiviteit & efficiëntie de overhand krijgen.

Voor het vinden van een juiste balans tussen de stuwende en de verankerende beginselen van de iOverheid komt in de praktijk veel aan op de intermediaire procesmatige beginselen accountability en transparantie. Zonder een stevige invulling van deze noties dreigt elke afweging in de lucht te blijven hangen. De beginselen van accountability en transparantie moeten de toetsbaarheid van het proces van ontwikkeling van de iOverheid waarborgen. Ze eisen tezamen dat de vaak impliciete afwegingen die de overheid maakt, inzichtelijk, navolgbaar, bediscussieerbaar en aanvechtbaar worden gemaakt. Eigenlijk is de enige in deze context geloofwaardige manier om de verschillende beginselen tegen elkaar af te wegen een argumentatieve manier. Om die argumentaties het vrije spel te geven is het nodig dat de overheid haar eigen afwegingen zo expliciet mogelijk wereldkundig maakt. Een van de belangrijkste agendapunten voor de iOverheid is de eis dat de afwegingen op beginselniveau (die onvermijdelijk moeten plaatsvinden) expliciet worden gemaakt. Deze afweging moet op alle niveaus geëxpliciteerd worden: van de voorbereiding en introductie van een concrete toepassing tot aan de omvattende vertakking van processen en informatiestromen waaruit de iOverheid is opgebouwd. Dat geldt niet alleen voor het nationale niveau, maar ook voor de afwegingen die op het internationale, en met name op het Europese niveau worden gemaakt. Dat verlangt dat de Nederlandse regering in een tijdig stadium expliciteert met welke afweging zij aan de Europese vergadertafel plaatsneemt en met welk resultaat, in termen van afwe-

ging, zij wenst thuis te komen. Dit leidt tot de eerste aanbeveling op het niveau van de beginselen.

Een evenwichtige ontwikkeling van de iOverheid vereist een doordachte afweging tussen de stuwende, verankerende en procesmatige beginselen die geëxpliciteerd, toetsbaar en publiekelijk te verantwoorden is.

De noodzaak van een omvattende en publiek te verantwoorden afweging is groot, omdat een eenzijdige benadering van de beginselen en daarmee de iOverheid op den duur ongewenste gevolgen heeft. Voor alle beginselen geldt dat het eenzijdig najagen van een enkel beginsel (veiligheid/privacy/transparantie boven alles!) er uiteindelijk voor zorgt dat de iOverheid applicatie voor applicatie en koppeling na koppeling in een extreme, onwerkbare en kwetsbare vorm uitmondt. Het is daarom belangrijk om een open oog te houden voor signalen en indicaties dat een of meerdere van deze beginselen de overige gaan verstikken. Juist voor beginselen geldt dat de maatschappij er te weinig maar evengoed te veel van kan hebben. Dat potentiële gevaar van dominantie bestaat voor *alle* beginselen, zeker wanneer ze tot extremen worden opgevoerd. Stuwende beginselen als effectiviteit & efficiëntie verworden in extremis tot economisme, een verankerend beginsel als keuzevrijheid verwordt tot een keuzedelirium en zelfs een procesmatig beginsel als accountability resulteert in excessieve achterdocht en juridisering wanneer daar eenzijdig het zwaartepunt wordt gelegd. Maar ook op het 'middenveld' van de afweging – weg van de extremen – komt het aan op een goede balans. Excessieve nadruk op veiligheid gaat al snel ten koste van privacy en transparantie. Maar een excessieve nadruk op privacy kan ook ten koste gaan van transparantie en accountability, aangezien verantwoording ook altijd een zekere mate van openbaarheid nodig heeft. Bij te veel initiatieven heeft het aan een daadwerkelijke, zorgvuldige en toetsbare afweging tussen deze ongelijksoortige beginselen ontbroken. De bestaande afwegingen – zoals die bijvoorbeeld zijn te vinden in parlementaire stukken – zijn veelal gefragmenteerd en/of obligaat.

Dat ligt uiteraard niet alleen aan de aard van de beginselen zelf. De beginselen moeten ter hand worden genomen op verschillende momenten, op een variëteit aan niveaus en in de vele processen die tezamen resulteren in de iOverheid: in het parlementaire debat over een nieuwe toepassing, in het formuleren van de opdracht aan een ontwikkelaar van een toepassing, in de beslissing om bestanden te koppelen of om nieuwe organisaties op een netwerk aan te sluiten en in de uitspraken van rechters, toezichthouders en burgers over nieuwe ontwikkelingen en genomen besluiten. Op al die momenten staat er veel op het spel en wordt het gewicht van een enkel beginsel soms zwaar aangezet om het pleit te beslechten. Het empirisch materiaal laat zien dat het bij de ontwikkeling van de iOverheid meerdere malen is voorgekomen dat plannen voor een nieuwe toepassing werden gepresenteerd op manieren die het meest weg hadden van marketing. Technologievertrouwen is soms niet zozeer echt vertrouwen, maar eerder een politieke verkoopmethode. Met

termen als effectiviteit & efficiëntie en veiligheid zou wel iets minder magie mogen worden bedreven. Maar ook aan de andere kant van het spectrum, aan de zijde van de verankerende noties van privacy en keuzevrijheid, worden reële en toetsbare argumenten en afwegingen vaak evenzeer gemist. Als er aan deze kant iets ingeleverd moet worden – hetgeen zich zeer wel voor kan doen –, dan is het zaak dat deze 'incassering' als zodanig wordt erkend en gecommuniceerd. Met andere woorden, hoewel in de meeste gevallen niet op voorhand te zeggen is wat de 'juiste' inhoudelijke afweging is tussen de stuwende en verankerende beginselen, dient het debat op dit punt wel degelijk sterk verbeterd te worden.

Het realiteitsgehalte van de discussies over de verdere ontwikkeling van de iOverheid, en de rol die de beginselen daarbij spelen, moet drastisch omhoog, omdat het zowel bij hen die wijzen op de kansen als bij hen die wijzen op de gevaren daarvan ontbreekt aan een goede verantwoording van hun zaak. Hierbij is een belangrijke rol weggelegd voor de procesmatige beginselen van transparantie en accountability. Juist een stevige en geloofwaardige invulling van de procesmatige omlijsting van de iOverheid kan bijdragen aan de realiteitswaarde van de discussies die bepalen welke richting moet worden ingeslagen. Evengoed is het noodzakelijk dat de verankerende beginselen expliciet en zoveel mogelijk toetsbaar worden gemaakt. Realiteitszin aan deze kant van het spectrum zou vooral laten uitkomen dat beginselen als privacy en keuzevrijheid geen alles-of-nietskarakter hebben. Het is soms noodzakelijk om op deze beginselen iets in te leveren, mits dit expliciet en goed verantwoord gebeurt. De overheid mag immers ook geen mogelijkheden laten liggen om met behulp van moderne technologie en wetenschappelijk onderbouwde mogelijkheden van risicotaxatie, diagnose en interventie mensenlevens te beschermen (Buruma 2011). Een teveel aan privacy kan een kind in grote moeilijkheden buiten het gezichtsveld van de autoriteiten houden, een teveel aan keuzevrijheid kan in een dusdanig complexe situatie erin uitmonden dat de burger uiteindelijk toch met lege handen staat.

Het expliciet en zoveel mogelijk toetsbaar maken van de stuwende beginselen zou op zijn beurt vooral twee zaken laten uitkomen en dus ook openlijk bespreekbaar maken. Ten eerste, dat vaak sprake is van ongefundeerd politiek-bestuurlijk optimisme ten aanzien van de mogelijkheden van ICT, zoals het empirisch materiaal in dit rapport en vele studies die dit rapport zijn voorgegaan, hebben laten zien. Hoewel optimisme de motor is van veel innovatie, is het in Nederland ook de onderliggende reden geweest voor ondoordachte projecten, onhaalbare deadlines en kostbare ICT-mislukkingen. Ten tweede zou explicitering duidelijk maken dat 'verrommeling' vaak stilletjes is ingecalculeerd. *Spill over* en *function creep* worden in politieke discussies op gepaste afstand gehouden en formeel verworpen, in het volle besef dat de toekomst met een grote mate van waarschijnlijkheid precies datgene zal brengen wat op dat moment van regeringswege formeel wordt uitgesloten. Het formele argument is dan dat de politieke verantwoordelijkheid slechts reikt

tot het voorliggende voorstel en niet tot de mogelijkheden die daarin – impliciet, maar eenvoudig voorstelbaar – voor de toekomst besloten liggen. In een iOverheid, die ontstaat uit een aaneenschakeling van dit soort geïsoleerde besluiten is een dergelijke 'na ons de zondvloed' redenering onhoudbaar. Het werkelijke besef een iOverheid te zijn vereist dat de politiek de digitale variant van 'regeren is vooruitzien' serieus neemt en toepast op de impliciete, maar voorzienbare toekomstige ontwikkelingen van informatisering. De overheid neemt in haar beleid vaker een voorschot op de toekomst en het zou haar sieren om dat in de politieke afweging ook, en met een open vizier, te doen.

2 WAARSCHUWINGSVLAGGEN VOOR DE IOVERHEID

Het is van belang dat de overheid bij de verdere informatisering een aantal kenmerken van informatie veel bewuster dan nu het geval is in acht neemt. Daarbij gaat het niet, zoals vaak gebeurt, om een inhoudelijke karakterisering van informatie waarbij bijvoorbeeld DNA-gegevens een hogere bescherming vereisen dan biometrische gegevens, die weer een hogere bescherming vereisen dan eenvoudige persoonsgegevens als naam, adres en woonplaats. Hoewel dergelijke onderscheidingen in type gegevens van belang zijn – en in de bestaande wet- en regelgeving deels ook in belangrijke mate zijn verankerd –, verlegt dit rapport de blik liever richting *processen* van informatieverwerking en -gebruik, juist omdat die processen van grote invloed zijn op het karakter en de betrouwbaarheid van de informatie waarop de iOverheid draait en waarvan ze afhankelijk is. Deze processen hebben in het huidige digitale tijdperk een aantal karakteristieken die expliciet in overwegingen en beslissingen meegenomen moet worden om de iOverheid evenwichtig uit te kunnen bouwen of te beperken.

Aan drie, onderling gerelateerde, processen worden daarom waarschuwingsvlaggen meegegeven. Die waarschuwing is niet bedoeld als een 'verbod', maar bedoeld om de alertheid van beleidmakers en politici te verscherpen. Het algemene 'besef een iOverheid te zijn' krijgt mede handen en voeten met de waarschuwingsvlaggen: wanneer informatie onderdeel dan wel resultaat is van deze processen dient de overheid alert te zijn op de kwaliteit van de informatie en op de vraag wie de verantwoordelijkheid voor de informatie draagt. In sommige gevallen moet mogelijk ook worden nagedacht over – het stellen van – grenzen aan informatiegebruik. Deze informatieprocessen verlangen expliciete aandacht als het gaat om een gebalanceerde verdere ontwikkeling van de iOverheid. De drie ontwikkelingen die deze drie vlaggen dragen zijn de volgende.

1. Het *vernetwerken* van informatie, i.e. het gezamenlijk gebruik en beheer van informatie in een netwerk van actoren.
2. Het *samenstellen en verrijken* van informatie, i.e. het creëren van nieuwe informatie en profielen op basis van verschillende bronnen uit verschillende contexten.

3. Het voeren van *preventief* en proactief beleid op basis van informatie, i.e. het actief beoordelen van en ingrijpen in de samenleving op basis van informatiegestuurde risicocalculatie.

Deze drie informatieprocessen vormen de kern van de iOverheid en stellen haar in staat om beleid te verfijnen, op maat te snijden, een omvattend beeld te verkrijgen van burgers en beleidsproblemen en daar waar nodig proactief op te handelen. Tegelijkertijd zijn het ontwikkelingen die van invloed zijn op informatie zelf: op het karakter, de betrouwbaarheid, de kenbaarheid, de contextualiteit en herleidbaarheid van informatie. Dat levert niet als zodanig onoverkomelijkheden of fundamentele bezwaren op. Het is wel van belang dat deze processen voldoende worden verdisconteerd in de omgang met, het gebruik van en de verantwoordelijkheid voor die informatie. Daaraan ontbreekt het vaak in de onbewuste iOverheid. Veel meer dan nu het geval is dient het besef door te dringen dat het juist deze drie ontwikkelingen zijn die grote gevolgen hebben voor (a) de *inhoudelijke* kwaliteit van informatie en (b) voor de eisen aan de *organisatorische* inbedding van informatiestromen. Hieruit volgt een aantal belangrijke randvoorwaarden voor de verdere ontwikkeling van de iOverheid.

2.1 Inhoudelijke kwaliteit van informatie

Alle drie de ontwikkelingen – vernetwerken, samenstellen en verrijken van informatie als ook informatiegestuurd preventief en proactief beleid – vereisen een scherpe en kritische blik op zowel kwaliteit als relevantie van de informatie die uit de systemen van de verschillende overheden rolt. In deel 2 is gewezen op tendenties en reflexen zoals het onbezorgd koppelen van informatiebestanden, het habitueel overschrijden van domeinafbakeningen zoals service, care en control, het zonder een duidelijk vooropgezet plan laten uitdijen van de zee van informatie, de voortdurende verwatering van informatie als gevolg van hergebruik op hergebruik, en ten slotte het stapelen en vermengen van alle soorten informatie. Binnen de iOverheid zoals die in de afgelopen jaren is ontstaan, gaat samengestelde informatie in netwerken eenvoudig over 'grenzen' heen. Dat geldt niet alleen voor de fysieke grenzen tussen nationaal en internationaal, maar in het bijzonder voor het onderscheid tussen publieke en private sectoren en 'hun' informatie, en voor het onderscheid tussen informatie gebruikt voor service, care en control. Bovendien wordt veel van deze informatie eerst gedecontextualiseerd wanneer het uit de oorspronkelijke informatieomgeving wordt gehaald en vervolgens gehercontextualiseerd wanneer het wordt gecombineerd met andere gegevens in een andere beleidscontext. Dat heeft uiteraard gevolgen voor de betrouwbaarheid en de kenbaarheid van informatie. Dat geldt voor de professionals die met deze gegevens moeten werken (en informatie uit een andere professionele context moeten interpreteren) en wordt nog versterkt wanneer het gaat om informatie die het resultaat is van technische bewerkingen, zoals profiling en data mining. Naarmate data- en informatiebestanden vervuilder zijn – en ze zijn vaak vervuild of vatbaar voor vervuiling – zorgen

netwerken er bovendien voor dat de risico's die samenhangen met de (verspreiding van) vervuilde informatie exponentieel groeien. Een vervuilde informatiehuishouding komt immers niet vanzelf tot stilstand. Integendeel. Vaak is eenvoudigweg niemand zich bewust van het kwaliteitsverlies van informatie en volgt bewerking op bewerking en hergebruik op hergebruik. Deze onwetendheid geldt zowel voor de betrokken overheidsfunctionarissen als voor de burgers in kwestie. Het gebrek aan kwaliteit van informatie onttrekt zich, juist in vernetwerkte situaties, maar al te gemakkelijk aan het zicht, zonder dat hiervoor altijd direct een 'schuldige' is aan te wijzen. Eerder is dit een onvermijdelijk risico van wat als het *multipliereffect* van ICT kan worden aangeduid: niet alleen correcte informatie heeft een enorme omloopsnelheid en effectieve distributie gekregen, maar ook foutieve informatie. De administratieve werkelijkheid en de 'werkelijke werkelijkheid' kunnen in de iOverheid veel sterker uiteenlopen dan voorheen, en fouten kunnen zich bovendien veel sneller verspreiden, waarna ze vervolgens veel moeilijker te herstellen zijn. Die fouten hebben in het dagelijkse leven soms grote gevolgen voor individuele burgers. Zeker als op basis van de foutieve gegevens via profilering verrijking van informatie plaatsvindt of proactief beleid wordt gevoerd.

De kwaliteit van de iOverheid vereist dus voortdurend rijksbrede aandacht en beleid. Over de hele linie moet de assumptie dat informatie juist is vervangen worden door het besef dat de informatie op onderdelen hoogstwaarschijnlijk niet accuraat, verouderd en soms zelfs misbruikt en gemanipuleerd zal zijn. Nu is de *default*-positie bij de overheid te sterk dat het systeem de waarheid in pacht heeft, worden de foutmarges genegeerd en verschuift de verantwoordelijkheid voor het probleem steeds meer richting burger. Men is zich onvoldoende bewust van de gevolgen van de iOverheid: het *multipliereffect* en de voortdurende decontextualisering vanwege de netwerken worden niet meegenomen in het bepalen van de kwaliteit van informatie. Of men staart zich juist blind op de positieve gevolgen van netwerken en samengestelde informatie. De aandacht voor de kwaliteit van informatie mag zich niet beperken tot de informatie zelf, maar moet zich ook op de metagegevens richten. Metagegevens zijn de onmisbare wegwijzers in de informatiehuishouding. Ze spelen een cruciale rol bij zowel het traceren van informatie als het duiden van de oorspronkelijke context en herkomst van deze informatie. De kwaliteit van een informatiehuishouding van de iOverheid staat of valt kortom met de aanwezigheid van kwalitatief goede metagegevens. Aandacht voor de kwaliteit van informatie vereist ook gedegen aandacht voor technische en organisatorische randvoorwaarden zoals beveiliging, werkprocessen en een betrouwbare authenticatie- en identificatie-infrastructuur.
Het vertrouwen in technologie moet veel beter dan nu het geval is worden afgezet tegen de empirische zekerheid dat alle systemen en informatiestromen naast bedoelde ook onbedoelde effecten sorteren die daarmee ook hun weerslag hebben op de inhoud van de informatie als zodanig. Te vaak houdt de overheid nog sterk – en vaak formeel – vast aan de juistheid van haar gegevens. Anders gezegd: de over-

heid heeft een te groot vertrouwen in de kwaliteit van informatie en een gebrek aan wantrouwen waar het de kwetsbaarheid van de iOverheid aangaat.

Een bewuste iOverheid benadert de eigen informatiehuishouding voortdurend vanuit een kritische houding. Deze houding kenmerkt zich door een realistisch wantrouwen ten opzichte van de kwaliteit van zowel informatie als informatieprocessen, waarbij beide constant op waarde worden geschat en waar nodig verbeteringen worden doorgevoerd.

De rol die informatie speelt in beleidsprocessen verandert onder de condities van digitalisering. Informatie wordt steeds meer ingezet om een voorschot te nemen op de toekomst en die ontwikkeling breidt zich bovendien verder uit over de terreinen van service, care en control. De klassieke variant daarvan, het gebruik van statistiek om het beleid te informeren en te verbeteren, wordt in toenemende mate aangevuld met een informatiegestuurd beleid dat zich toelegt op het voorspellen van *individueel* gedrag. Informatie en calculatie moeten bijvoorbeeld voorspellen welk kind gevaar loopt en welke reiziger een terrorist zal blijken. Op basis van die risicocalculatie wordt vervolgens gehandeld. De verschuiving naar individueel gedrag betekent dat de opbrengst potentieel zeer hoog is – er wordt een leven gered of een aanslag verijdeld –, maar betekent tegelijkertijd dat de repercussies als die inschatting fout blijkt te zijn ook zeer hoog zijn. Wie onterecht als potentieel terrorist, crimineel of falende ouder in de systemen en netwerken van de overheid wordt opgenomen zal daar de gevolgen van voelen in zijn dagelijkse leven. Het besef dat statistiek en kansberekening worden gebruikt voor individuen, en niet voor brede beleidscategorieën, en de potentiële gevolgen daarvan is zwak ontwikkeld bij de overheid.

De meest pregnante voorbeelden, met de meest verstrekkende gevolgen, zijn te vinden in de domeinen van de (staats)veiligheid en in die delen van de zorg waar het om levensbedreigende situaties gaat. Maar ook op minder precaire beleidsterreinen in de dienstverlening en de zorg geldt dat statistische benaderingen en de uitkomsten van vernetwerkte informatieverwerking soms individuele burgers in de verkeerde hokjes plaatst en daarin vaak langere tijd vasthoudt. Bovendien geldt dat deze domeinen onder invloed van informatisering steeds meer in elkaar vervloeien, zodat fouten zich verspreiden en diffuser worden. Ook blijkt in de dagelijkse praktijk van het informatiemanagement van de overheid het 'vergeten' van informatie – ondanks bewaartermijnen – onder druk te staan. In profielen en netwerken leidt bepaalde persoonsinformatie een hardnekkig bestaan met alle potentiële gevolgen van dien.

Een iOverheid zal dus een scherp oog moeten hebben voor de mogelijke negatieve en soms zelfs schadelijke effecten van informatiegestuurd beleid. Goede procedures om daarmee om te gaan zijn van groot belang voor individuele burgers die in de knel komen. Ook zijn ze van belang voor het in stand houden en versterken van

vertrouwen in de iOverheid. Die procedures vragen om een balans tussen de beginselen van accountability en transparantie enerzijds en om een balans tussen de rol en verantwoordelijkheid van de overheid en van de burger anderzijds. Het is daarbij van belang om een onderscheid te maken tussen de burgerrol van *citoyen* (politiek subject) en de burger als individu (juridisch subject). In het eerste geval gaat het om de burger als een productieve *countervailing power* die inzicht zou moeten hebben in de informatieprocessen van de overheid. In het tweede geval gaat het om de burger die toegang moet hebben tot zijn rechten wanneer hij door de overheid onjuist en/of onheus wordt bejegend of vast komt te zitten in de systemen van de iOverheid. Beide rollen vergen een zekere *vigilance* – een combinatie van waakzaamheid en assertiviteit – om een tegenwicht te bieden tegen de uitbreiding van de iOverheid. Dat is echter geen opstelling van burgers die voor lief kan worden genomen, maar één die ondersteuning vraagt in termen van procedures en rechten. Die moeten gevonden worden in praktische uitwerkingen van accountability en transparantie. Algemeen geformuleerd geldt dat voor de burger als *citoyen* transparantie een hoge prioriteit heeft, terwijl voor de burger als individu de hoogste prioriteit bij accountability ligt.

Om burgers in staat te stellen een *countervailing power* te zijn is een zekere openheid van zaken bij de iOverheid nodig. Zonder transparantie en zeker ook inzicht is reëel toezicht onmogelijk. Dat betekent dat de iOverheid meer openheid van zaken moet geven en burgers meer en vooral ook tijdig 'mee moet laten praten en denken' over de verdere ontwikkeling van de iOverheid. Dat moet ze zowel 'uit eigen beweging' doen als in reactie op vigilante burgers en burgerbewegingen die door middel van verzoeken en procedures informatie boven tafel proberen te krijgen. De platitude dat 'wie niets te verbergen heeft, ook niets te vrezen heeft' kan met een knipoog – het is immers ook echt een platitude – wel wat meer op de iOverheid zelf worden toegepast. De burger in de rol van toezichthouder veronderstelt terecht waakzaamheid en assertiviteit bij burgers die echter, even terecht, meer transparantie aan de kant van de overheid zouden mogen verwachten.

Als het gaat om de burger als individu, zeker als die zijn recht zoekt ten opzichte van de staat, is transparantie hoogstens een begin. Met alleen transparantie wordt de burger immers wel gefaciliteerd, maar ook verantwoordelijk gemaakt om zijn digitale zaakjes goed op orde te hebben, en daar onvermoeibaar over te waken. Dat zou, alleen al in termen van de digitale kloof, een grote ongelijkheid tussen burgers creëren. Bovendien heeft de burger de autoriteit noch de doorzettingsmacht om daadwerkelijk iets blijvend te wijzigen in de vernetwerkte backoffice van de iOverheid. De empirie heeft laten zien dat burgers in de praktijk slachtoffer worden van fouten in de backoffice en machteloos staan om die fouten te corrigeren. Die praktijk moet dus verder uitgewerkt worden met goede procedures voor eindverantwoordelijkheid en een kenbare ingang om verantwoordelijkheid bij de iOverheid neer te leggen. Daarbij moet een evenwicht gevonden worden tussen de

verantwoordelijkheid van de burger om onjuistheden aan te (kunnen) kaarten en de verantwoordelijkheid van de overheden om fouten ook daadwerkelijk recht te zetten. Zeker in de meer gevoelige domeinen van care en control (gekenmerkt door een grote winst voor de samenleving bij succes en grote repercussies voor het individu bij fouten) kan het niet zo zijn dat de burger voor (de gevolgen van) de foutieve of verouderde informatie van de overheid opdraait. Kortom, enerzijds is de verantwoordelijkheid van de overheid groot, omdat alleen zij de doorzettingsmacht heeft om fouten in het volledige netwerk van de iOverheid te corrigeren en niet alleen bij het loket waar het probleem is geconstateerd. Anderzijds moet de drempel voor de individuele burger ook niet te laag zijn, aangezien dan relatief (te) gemakkelijk grote inspanningen aan de kant van het bestuur worden gevraagd.

De iOverheid moet investeren in procedures om transparantie (ter ondersteuning van de burger als citoyen) en accountability (ter ondersteuning van de individuele burger als rechtzoekende) te verbeteren. Verantwoordelijkheid en verantwoordingsprocedures binnen de iOverheid zijn momenteel ontoereikend en onvoldoende effectief, en dienen daarom omvattender, explicieter en helderder te worden benoemd en belegd.

2.2 Organisatorische inbedding voor duurzame en rechtvaardige informatiestromen

Het 'besef een iOverheid te zijn' en in het bijzonder de drie waarschuwingsvlaggen van vernetwerken, samengestelde informatie en informatiegestuurd proactief beleid hebben uiteraard ook gevolgen voor de praktische en organisatorische vormgeving van de iOverheid. De inbedding van informatiestromen in de overheidsorganisatie laat in termen van beheer, kwaliteit en waarborgen, ondanks de steeds vaker gebezigde term 'informatiemanagement', nog veel lacunes zien. De ontwikkeling van de iOverheid tot op heden kan in termen van informatie nog te zeer worden gekenschetst als 'veel *flow*, weinig *management*'. De informatie stroomt steeds vrijelijker door de organisatie van de overheid (en daarbuiten), terwijl de randvoorwaarden voor een goed beheer en management van die informatiestromen achterblijven. De omzetting van papieren dossiers en ladekasten in digitale gekoppelde informatiebestanden biedt immers niet alleen nieuwe kansen, maar zet ook klassieke taken en verplichtingen van de overheid in een ander daglicht. De praktische organisatie en het management van al de informatie die in de databanken en netwerken van de overheid circuleert is een kwalitatief andere opgave dan die van het papieren tijdperk. Informatiemanagement gaat ook over het functioneren van het 'geheugen' van de iOverheid en dat hapert aan twee kanten. Enerzijds 'dementeert' de overheid en worden zaken vergeten die niet vergeten mogen worden. Anderzijds onthoudt de overheid meer en meer informatie over haar burgers vanuit de gedachte dat het ooit nog van pas kan komen. Het eerste is (onder meer) schadelijk omdat zonder goed geheugen transparantie en accountability onwerkbare beginselen worden. De archieffunctie stelt de overheid in staat haar eigen handelen over te dragen, te traceren, te openbaren en te verantwoorden. Dat is zowel intern, binnen de overheid, als

extern, ten opzichte van burgers, van vitaal belang. Archiveren in tijden van digitalisering vraagt echter om een radicaal andere aanpak van het informatiemanagement van de overheid. De Algemene Rekenkamer heeft hier al meerdere malen, en met grote nadruk, op gewezen en daartoe organisatorische handreikingen gedaan.

Tegelijkertijd lijkt de overheid op andere punten niet in staat of onwillig om informatie te vergeten. Het onbeperkt onthouden van informatie is echter ook schadelijk, omdat dit het risico in zich bergt dat burgers zich niet meer aan hun eigen verleden kunnen ontrekken. De overheid is soms niet bij machte om de eigen bewaartermijnen te respecteren en neigt er bovendien naar deze steeds verder op te rekken vanuit de gedachte dat meer informatie ook betere informatie is. Veiligheid en fraudebestrijding zijn daarbij de magische woorden bij uitstek. Er zijn echter ook goede redenen om niet elk deel van het verleden van burgers te betrekken bij het oordeel van de overheid over burgers in het heden of de toekomst. Het werken met 'burgerbeelden' en profielen voedt de informatiehonger van de overheid en maakt bewaren en onthouden een belang op zichzelf. Burgers worden immers veel sterker het product van hun verleden dan ze in het papieren tijdperk waren. 'Eens een dief, altijd een dief' loopt het gevaar een digitale eeuwigheidswaarde te krijgen. Het feit dat het technologisch mogelijk is om persoonsgegevens tot in lengte van dagen te bewaren is nog geen afdoende reden om dat ook daadwerkelijk te doen. Ook hier zal de specifieke context overigens om nadere en soms ook andere afwegingen ten aanzien van bewaren dan wel vernietigen van informatie vragen. Zo zal informatie in het domein van de opsporing bijvoorbeeld soms anders beoordeeld moeten worden dan informatie in het domein van de gezondheidszorg, waar het voor langere tijd bewaren van gegevens van onschatbare waarde kan zijn voor onderzoek en inschattingen van sterfterisico's en erfelijkheid. Op welke wijze gegevens vervolgens bewaard moeten worden, bijvoorbeeld al dan niet geanonimiseerd, is een volgende vraag die ook per categorie bekeken en beoordeeld moet worden. Het gaat er niet om één norm voor het bewaren of vergeten van alle (persoons)informatie te formuleren (het absolute recht op vergeten), het gaat er juist om dat de overheid hier een goede en beredeneerde afweging maakt die bovendien ook daadwerkelijk in acht genomen wordt.

Het is voor de verdere ontwikkeling van de iOverheid kortom van wezenlijk belang dat er aandacht is voor haar geheugen. De archieffunctie moet zonder meer versterkt worden, wat een radicale omslag in het denken verlangt. Wat de overheid van haar burgers dient te vergeten vereist een openlijke en voortdurende afweging tussen collectieve belangen, zoals die van veiligheid enerzijds en individuelei belangen als het recht op vergeving en vergetelheid anderzijds. Een rechtvaardig geheugen verlangt bovendien dat de overheid zich meer dan nu het geval is rekenschap geeft van de risico's die het gebruik van verouderde gegevens met zich mee kan brengen. De regering dient er daarom op toe te zien dat organisaties binnen de iOverheid structureel aandacht hebben voor het belang van vergeten. Organisaties

dienen de afwegingen tussen 'bewaren en vergeten' te doordenken, te expliciteren en het resultaat van deze afwegingen ook daadwerkelijk organisatorisch te verankeren. De iOverheid dient hiernaast naar wegen te zoeken om burgers structureel en laagdrempelig te faciliteren bij het verwijderen van verouderde, onjuiste en niet-accurate gegevens.

De iOverheid moet over een effectief, duurzaam, maar vooral ook rechtvaardig geheugen beschikken. Het belang van bewaren en archiveren verlangt een radicale cultuuromslag. Het belang van vergeten moet blijvend worden geagendeerd en vereist een inhoudelijke en organisatorisch verankerde strategie.

2.3 'Grenzen aan de groei' van de iOverheid?

Een onbewuste iOverheid zal de natuurlijke neiging hebben om verder te groeien: 'grenzen aan de groei' komen pas met bewustzijn in zicht. Tot die tijd worden informatieverzamelingen en koppelingen nauwelijks serieus begrensd, vervuilt informatie, sluiten organisaties en informatiestromen niet meer op elkaar aan, raken burgers en bedrijven, maar ook instanties binnen de overheid zelf verstrikt in de datakluwen van de overheid, wordt identiteitsvaststelling een probleem en wordt het voor burgers vrijwel onmogelijk zich te onttrekken aan de informatie die over hen wordt verzameld, bewerkt en uitgewisseld. Zonder een besef van de iOverheid en wat deze betekent voor de verhouding overheid-burger is er weinig reden of gelegenheid om stil te staan bij de groei van het informatiebouwwerk dat de overheid in uitvoering heeft. Ook geeft het weinig reden tot het stellen van vragen: of dit nodig is, of er behoefte aan en noodzaak tot begrenzing is en hoe het zich verder dient te ontwikkelen. Vragen en afwegingen op het niveau van de samenhang van informatiestromen en de gevolgen daarvan blijven liggen, terwijl de constructie van het bouwwerk van de iOverheid doorgaat. Daarmee doet de overheid zichzelf en haar burgers tekort. Bovendien maakt het niet alleen burgers, maar ook de overheid zelf kwetsbaar.

De dagelijkse praktijk van informatieverspreiding en koppeling en de redelijkerwijs te verwachten claims op eenmaal verzamelde informatie in de toekomst vereisen een bredere afweging die (a) voorbij het concrete beleidsinitiatief kijkt en (b) voorbij het concrete moment van het hier en nu kijkt. Het daadwerkelijk maken van afwegingen op het niveau van de iOverheid doet ook een fundamentelere vraag rijzen: is de iOverheid zoals die is ontstaan ook de iOverheid die we zouden wensen als we haar expliciet en in de volle besef van de samenhang hadden doordacht en ontworpen? Dat betekent daarmee ook dat de vraag op tafel ligt of er grenzen aan de uitbouw van de iOverheid zitten. Waar zitten die grenzen wel? Waar niet? En op basis waarvan wordt dat bepaald?

Deze vragen naar begrenzing hebben ook te maken met een kwetsbaarheid van de iOverheid die zich het best laat illustreren aan de hand van het karakter van het in-

ternet. Het fundamenteel ongereguleerde en open netwerkkarakter van het internet maakt het 'sturen' van het internet of het controleren van de informatie die daarop circuleert in de praktijk vrijwel onmogelijk. Iedereen heeft immers toegang tot informatie wanneer die eenmaal op het net is geplaatst. Wat onjuist of ongewenst is kan worden weggehaald op de eigen site of, na juridische actie, wellicht van de site van een ander, maar is dan vaak al gekopieerd en duikt als 'mirror' ergens anders op. De ontwikkelingen eind 2010 rondom WikiLeaks vormden bij uitstek een voorbeeld van een site die in snel tempo gekopieerd werd, juist omdat overheden en andere belanghebbenden de daarop geplaatste informatie ontoegankelijk wilden maken. Het onstuurbare karakter van het internet en de fundamentele gevolgen daarvan spelen in afgeleide vorm ook voor de iOverheid en wel op twee niveaus. In de eerste plaats voor de iOverheid zelf, dat wil zeggen de interne informatiehuishouding van de overheid. Die informatiehuishouding verschilt van het internet in die zin dat het om een semigesloten systeem gaat en niet een volledig open systeem als het internet. Dat betekent dat het in goede banen leiden van informatiestromen tot op zekere hoogte mogelijk is. De huidige dynamiek binnen de iOverheid zet die (fragiele) 'stuurbaarheid' van informatie echter onder druk. Zowel het vernetwerken van informatie als het laten vervloeien van informatiestromen over de grenzen van het publiek-private heen maakt dat het semigesloten systeem van de iOverheid *intern* steeds meer op het internet gaat lijken. Informatie is steeds meer van iedereen, in plaats van toebehorend aan één organisatie. Dat betekent ook dat het in goede banen leiden van informatiestromen binnen de iOverheid op dezelfde grenzen stuit als binnen het model van internet. Naarmate die ontwikkeling zich doorzet, wordt het problematischer voor de overheid om informatie te kanaliseren, te verifiëren en voor de betrouwbaarheid in te staan.

Naast het risico dat de internetlogica bij de iOverheid 'naar binnen slaat' is er nog een tweede risico, namelijk dat de iOverheid ongewild deel wordt van het internet. Wederom is de WikiLeaks-affaire, zoals die in het najaar van 2010 in alle hevigheid losbarstte, een aansprekend voorbeeld en een voorbode van wat in de toekomst ongetwijfeld vaker zal gaan gebeuren. Door WikiLeaks kwam de interne informatiehuishouding van overheden ineens op de digitale straten van het internet te liggen: oncontroleerbaar door het vele kopiëren en de snelle migratie van de informatie van *server* naar *server*, van *cloud* naar *cloud*. Inmiddels worden ook lokale varianten gelanceerd die anoniem en vertrouwelijk (overheids)documenten onthullen, zoals www.opennu.nl.

Alleen Chinese methoden zouden de geest wellicht terug in de fles kunnen krijgen, maar zelfs dat is de vraag. Om van de wenselijkheid daarvan nog maar te zwijgen. Voordat een dergelijk 'lek' van overheidsinformatie naar het internet realiteit wordt, wordt het risico gezien als een kwestie van beveiliging van data en van techniek en beleid om dat te bewerkstelligen. Zodra een lek resulteert in het verspreiden van gevoelige informatie op internet, is er echter geen beleid meer voorhanden,

gaan overheden improviseren om de controle terug te winnen, maar dat biedt een weinig verheffende aanblik. De grote druk die de Amerikaanse overheid op service providers uitoefende om WikiLeaks uit de lucht te halen, bracht Amy Davidson van de *New Yorker* tot de vraag of "Lieberman feels that he, or any Senator, can call in the company running the *New Yorker's* printing presses when we are preparing a story that includes leaked classified material, and tell it to stop us. The circumstances are different, but not so different as to be really reassuring."[2] Toch zijn dergelijke lekken juist door digitalisering nagenoeg onvermijdelijk en zullen ook onvermijdelijk vaker voorkomen in de toekomst: de 250.000 pagina's van WikiLeaks waren in papieren vorm nooit op deze manier en op deze schaal uitgelekt. Het is de gecomprimeerde digitale vorm die informatie mobiel doet zijn en lekken van deze omvang mogelijk maakt: in veel van de eerdere geruchtmakende gevallen van informatielekken in onder meer het Verenigd Koninkrijk ging het ook om enorme aantallen persoonsgegevens die op een verloren USB-stick, kleiner dan een aansteker, stonden. Ook de onvermijdelijkheid van lekken naar internet, of dat nu intentioneel is of het gevolg van fouten, slordigheden of grove nalatigheid, maar zeker ook de verdere consequenties die dergelijke lekken met zich meebrengen, zijn redenen om stil te staan bij de grenzen van de groei van de iOverheid.

Hoewel dit rapport de grenzen van de iOverheid niet zal markeren, aangezien dat in essentie politieke keuzes zijn, kan het wel aangeven welke grensgebieden in die afweging betrokken moeten worden. Het gaat hier kortom om de bewustmaking en de aanzet tot een debat over begrenzing en niet om de exacte vaststelling van die grens. De belangrijkste waarde van het rapport *Grenzen aan de groei* van de Club van Rome lag immers ook eerder in het politiek agenderen van de milieuproblematiek en dan in de exacte voorspellingen en extrapolaties in het rapport. De afbakeningen die hierboven zijn gegeven kunnen een eerste aanzet zijn voor het benoemen van grenzen: de combinatie van een expliciete afweging van beginselen en het in acht nemen van de waarschuwingsvlaggen dwingt tot nadenken over de grenzen van de iOverheid. Ook de vermenging tussen service, care en control en de publiek-private vermengingen die ongemerkt heel gewoon zijn geworden, zijn bij nadere beschouwing en vanuit het perspectief van de iOverheid vaak problematisch. Tenslotte vormt de constatering dat het internet een totaal andere informatieomgeving heeft gecreëerd waarbinnen ook de iOverheid heeft te functioneren, alle aanleiding om het karakter van de iOverheid verder te doordenken en daarnaar te handelen. Hier zijn beredeneerde begrenzingen van groot belang. Niet in de laatste plaats om overheden houvast te geven in het bepalen van wat een juiste omgang is met informatie en het delen daarvan met andere (overheids)partijen. Dat is nu vaak onbepaald. Zo besloot de Belastingdienst niet mee te werken aan de informatie-uitwisseling binnen een divers samengesteld samenwerkingsverband van partijen dat door een gemeente was geïnitieerd met het oog op de ontruiming van een woonwagencentrum.[3] De Belastingdienst achtte zich niet gerechtigd om gevoelige informatie te delen met private partijen als elektriciteitsbedrijven, trok als grote zelfstandige

overheidsdienst de eigen 'absolute' grens en verliet de tafel. Ook het in hoofdstuk 7 genoemde arrest van de Hoge Raad waarin grenzen werden gesteld aan het opvragen door het Openbaar Ministerie van reizigersgegevens bij Trans Link Systems is een illustratie.[4] Het stellen van dit soort grenzen en het bepalen van kaders voor de verdere ontwikkeling van de iOverheid zou echter niet af mogen hangen van dergelijke bottom-upacties en geïsoleerde rechterlijke uitspraken. Als de Belastingdienst dan wel Trans Link Systems immers wel met de verstrekking had ingestemd, had het proces van gegevensuitwisseling zich geruisloos en zonder nadere discussie verder voltrokken.

Een bewuste iOverheid kan niet zonder een beredeneerde visie op de grenzen van diezelfde iOverheid. Zowel de dynamiek binnen de iOverheid als de dynamiek in de iSamenleving dwingt daartoe: zonder begrenzing zal de overheid uiteindelijk het vermogen kwijtraken om de verdere ontwikkeling van de iOverheid in werkbare banen te leiden.

2.4 Een agenda voor de transformatie naar een bewuste iOverheid

Het breed in het denken en de organisatie van de overheid verankeren van het 'besef een iOverheid te zijn' is een urgente opdracht. Deze kan potentieel echter eenvoudig tegen de politieke waan van de dag wegvallen. En dat is gezien wat er op het spel staat een ongelukkige situatie. Om de inhoudelijke aanbevelingen uit de voorgaande paragrafen te kunnen realiseren dient het bestaande bestuurlijk bestel te transformeren naar een bestel dat in staat is om de uitdagingen van de iOverheid te signaleren en op te pakken. Om dit organisatorisch en bestuurlijk vorm te geven is de betrokkenheid van vele organisaties en lagen van de overheid nodig. Daarmee is het niet alleen de regering die in dit rapport direct wordt aangesproken. Oplossingen kunnen echter wel centraal worden *aangejaagd*. Bovendien geldt dat de dynamiek van de iOverheid dusdanig groot is dat er ruimte moet zijn om snel nieuwe ontwikkelingen en reacties daarop in het denken te kunnen integreren. Het 'besef een iOverheid te zijn' is geen rustig bezit, maar een permanente opgave. Maar juist in een wereld van snelle en dynamische informatisering is het van belang om ankerpunten in te richten die (a) hoeder zijn van het 'besef een iOverheid te zijn' en (b) de iOverheid van een duidelijk en daadkrachtig aanspreekpunt en gezicht voorzien.

Het huidige institutionele landschap is niet op het beleggen van die ankerpunten toegerust. De kern van de iOverheid schuilt in de samenhang van informatiestromen en netwerken en juist op dat punt geldt dat er geen organisaties zijn die zich om het geheel (kunnen) bekommeren. Het politieke debat is verkaveld in wetten, beleidsterreinen, Kamercommissies en technieken, maar beziet informatie zelden in samenhang, laat staan met het oog op verwevenheid, toekomstige verwevenheden en de gevolgen daarvan. Dezelfde verkokering geldt voor de financiële stromen die met digitaliseringsprojecten verbonden zijn en daarmee ook de mogelijkheden voor aansturing en beïnvloeding daarvan. Er is geen 'ministerie van' of 'Kamer-

commissie voor Informatie'. Departementen, uitvoeringsorganisaties en lagere overheden bekommeren zich primair om hun eigen beleidsproblemen en hebben weinig oog voor de gevolgen van inkomende en uitgaande informatiestromen die verder reiken dan de 'grenzen' van hun eigen taak en organisatie. Eenzelfde beeld valt in een grensoverschrijdende context waar te nemen. In Europa wordt het netwerk van informatiestromen en persoonsgegevens steeds verder uitgebouwd en vertakt zonder een open discussie over de vraag of, op welke manier en onder welke voorwaarden Nederland wil aansluiten op een iEuropa in aanbouw. Uitvoeringsorganisaties gebruiken de informatie die ze krijgen in het contact met de burger, maar zijn niet bij machte om fouten in informatiestromen te traceren en voor de gehele keten of het netwerk op te lossen als burgers vastlopen. De vele toezichthouders, zoals het CBP en de Nationale Ombudsman, en meldpunten als het Meldpunt Identiteitsfraude, die sommige uitwassen van de iOverheid voor burgers en overheid benoemen en proberen op te lossen, hebben daar vaak niet de taakopdracht voor (te weinig omvattend) en zijn in de praktijk ook niet in staat (structurele) oplossingen te leveren. Daar waar via programma's en andere arrangementen departementsoverstijgend wordt samengewerkt, zoals binnen het beleidsprogramma Versterking Identiteitsketen Publieke Sector (VIPS), is dat slechts op tijdelijke basis en lang niet altijd op voldoende hoog ambtelijk niveau opgehangen. In alle gevallen ontbreekt het aan doorzettingsmacht om de aanpak en oplossingen over de grenzen van de departementen en instanties heen permanent door te voeren. Het ontbreekt de overheid ook aan de juiste kennis op het snijvlak van beleid en techniek om nieuwe systemen 'iOverheidsproof' te ontwikkelen. Op al deze niveaus worden soms dappere pogingen ondernomen om het geheel van de iOverheid in ogenschouw te nemen, te beoordelen en naar oplossingen voor problemen te zoeken. Maar voor alle bestaande organisaties en arrangementen geldt dat hun wettelijke taak en het gebrek aan doorzettingsmacht simpelweg niet aansluiten op de uitdagingen van de iOverheid. Vandaar de dringende noodzaak voor een agenda voor institutionele transformatie. In navolging van de empirische realiteit moet de overheid zelf in institutionele zin transformeren van een eOverheid naar een iOverheid. De overheid heeft instituties nodig die haar in staat stellen om de discussie over de verdere ontwikkeling van de iOverheid in goede banen te leiden, om verantwoordelijkheid te nemen voor de eigen genetwerkte informatiehuishouding en burgers te voorzien van bescherming die is geënt op de kenmerken van de iOverheid.

Om de doelen voor de iOverheid handen en voeten te geven, is een institutionele transformatie nodig die drie functies bij de overheid belegt en verankert.

a. De *strategische functie*, i.e. het waarborgen van een weloverwogen verdere ontwikkeling van de iOverheid.
b. De *maatschappelijke functie*, i.e. het versterken van de transparantie van de iOverheid voor burgers en het versterken van de accountability van de iOverheid ten opzichte van burgers die informatienetwerken verstrikt raken.

c. De *operationele functie*, i.e. het verbeteren van de weloverwogen aansluiting tussen beleid, uitvoering, technologie en informatiestromen en netwerken. Het verbeteren van het opdrachtgeverschap van de overheid.

Deze drie functies vormen de absolute ondergrens van wat nodig is om het besef van de iOverheid vorm te geven en te handelen naar de consequenties die de nieuwe realiteit met zich meebrengt. In de volgende paragraaf worden specifieke voorstellen gepresenteerd die de drie functies voorzien van de noodzakelijke 'institutionele tanden'. Daarbij moet worden opgemerkt dat een solide verankering van de doelen en het daadwerkelijk faciliteren van de uitvoering daarvan uiteindelijk belangrijker is dan het naambordje van de organisatie die figureert in de voorgestelde institutionele uitwerkingen.

De iOverheid noodzaakt tot een transformatie van het bestuurlijk bestel, waarbij bestaande arrangementen op het strategische, maatschappelijke en operationele niveau opnieuw moeten worden ingericht.

3 INSTITUTIES VOOR DE IOVERHEID

Het is zeker niet zo dat de iOverheid zoals die zich in de afgelopen jaren heeft ontwikkeld, wordt gekenmerkt door een gebrek aan instituties. In deel 2 van dit rapport is een bonte stoet van overheidsorganisaties de revue gepasseerd. Een minstens even groot aantal organisaties dat zich bezighoudt met verschillende aspecten en elementen van informatisering en overheid is daarbij niet eens genoemd. Al deze instituties en organisaties kwijten zich zo goed als ze kunnen van hun opdracht op hun eigen specifieke terrein. Het probleem met deze instituties is dat zij, net zoals de iOverheid goeddeels onbewust is ontstaan, voor een groot deel onbewust met die ontwikkeling zijn meegegroeid of gaandeweg aan het palet zijn toegevoegd. Net zoals de iOverheid is ontstaan door toepassing op toepassing en koppeling op koppeling te stapelen, is het institutionele landschap gegroeid in het licht van individuele toepassingen en de kansen en problemen die zich daarbij voordeden. Het zijn echter de instituties van de eOverheid. De onderlinge samenhang en verwevenheid die kenmerkend is voor de iOverheid is nergens institutioneel belegd. Dat geldt zowel voor de ontwikkeling als het toezicht en handhaving. Ondanks het feit dat vele organisaties vol overgave staan voor de kansen van informatisering of aandacht vragen voor de nadelen en gevaren daarvan: hun handelen blijkt niet krachtig genoeg in z'n geheel. De samenhang wordt nauwelijks gezien, laat staan dat het in de opdracht en het handelen van verschillende organisaties is meegenomen.

Een belangrijke consequentie van de boodschap van dit rapport is dat de iOverheid zich, vanwege haar netwerkkarakter, zeer moeilijk centraal laat aansturen. Hiërarchieën en netwerken vormen een ongemakkelijk huwelijk. Tegelijkertijd zal iets of iemand het besef moeten aanjagen, hetgeen een centrale actor met doorzettings-

macht impliceert. Er zal dus een institutionele verbinding gezocht moeten worden tussen netwerken en beslissingsmacht, zowel binnen de overheid als in verbinding met de bredere maatschappelijke context van de iOverheid. De iOverheid functioneert tegen de achtergrond van een iSamenleving die door informatisering wordt beïnvloed en deze op haar beurt zelf beïnvloedt. Bovendien vloeien de publieke informatienetwerken van de overheid aan de randen vaak over in de private netwerken van bedrijven en burgers. De iOverheid kan niet eigenstandig en in een isolement worden vormgeven. Het heeft daarbij alle relevante actoren te betrekken – dus behalve verschillende niveaus binnen de overheid, zeker ook de private sector en burgers. Het credo zou moeten zijn: "Betrek de iSamenleving bij de duurzame uitbouw van de iOverheid."

Wanneer de boodschap van dit rapport tot zijn uiterste consequentie wordt doorgeredeneerd, is de enige echte institutionele aanbeveling dat het besef een iOverheid te zijn, moet inzinken in alle organisaties van de overheid en op alle vitale momenten in het proces van informatisering: vanaf de eerste plannen op nationaal of internationaal niveau, de prille gedachten over een nieuwe applicatie, via een concrete opdracht of aanbesteding tot het enthousiast koppelen van informatie in een later stadium. De iOverheid moet indalen als een breed verankerd besef. Dat is het gewenste toekomstbeeld. Het ontwikkelen van dat besef zal een evolutionair proces zijn dat mogelijk versneld wordt door externe schokken – de ophef over de publicatie van vertrouwelijke overheidsdocumenten via WikiLeaks of een groot schandaal rondom informatiebeheer, zoals voorbeelden in het buitenland wel hebben laten zien. Maar het ontwikkelen van het besef kan ook door het instellen van instituties die een aanjagende functie hebben. Wat dat betreft is de ambitie van het kabinet-Rutte om een nationale toezichthouder in te stellen voor het melden van datalekken bij de overheid, een duidelijke stap in de richting die de wrr bepleit (Regeerakkoord 2010: 42). Maar de opgave voor iOverheid reikt verder dan alleen een toezichthouder voor datalekken.

In deze laatste paragraaf van dit rapport worden bij wijze van voorbeeld de contouren geschetst van een viertal instituties die deze aanjagende functie kunnen vervullen. De strategische, maatschappelijke en de operationele functie worden op die manier belegd bij een viertal nieuwe organisaties die in staat moeten worden gesteld om de transformatie naar een iOverheid gestalte te geven. De institutionele voorstellen zijn realistische opties, maar zijn ook een middel om de urgentie van hetgeen gedaan moet worden te expliciteren en uit werken. Zoals eerder gezegd is de urgentie, en de agenda die daaruit voortvloeit, daarbij belangrijker dan de specifieke uitwerking. Het beleggen van strategische, maatschappelijke en de operationele functies, en deze van zowel middelen als doorzettingsmacht voorzien, heeft de prioriteit. Tegen deze achtergrond worden vier voorstellen voor institutionele innovatie voor de iOverheid gedaan. De strategische functie wordt belegd bij een permanente commissie voor de iOverheid die rapporteert aan de Eerste en Tweede

Kamer. De maatschappelijke functie wordt uitgewerkt in een nationaal iPlatform en een iAutoriteit die verantwoordelijk zijn voor de transparantie respectievelijk de opname en afhandeling van problemen van burgers met de iOverheid. De operationele functie wordt uitgewerkt in een organisatie waarin het opdrachtgeverschap van de overheid professioneel belegd kan worden.

3.1 Permanente commissie voor de iOverheid

Het besef van de iOverheid moet centraal belegd worden, omdat dit perspectief anders dreigt weg te zakken tussen de specialismen van de verschillende actoren en organisaties die zich met informatisering en gevolgen daarvan bezighouden.

Stel een permanente commissie voor de iOverheid in die jaarlijks aan het parlement rapporteert over de 'staat van informatie'.

De centrale taak van deze commissie is om ontwikkelingen te signaleren, met elkaar in verband te brengen, en te doordenken vanuit het perspectief van de iOverheid, dat wil zeggen over grenzen van departementen en overheidslagen heen en in het perspectief van de mogelijke toekomstige ontwikkelingen. Daarbij gelden de eerder gepresenteerde waarschuwingsvlaggen – bij netwerken, samengestelde informatie en preventief en proactief beleid – als specifieke aandachtspunten bij de advisering. Het jaarlijkse rapport is openbaar en doet aanbevelingen over de voorgenomen plannen van de overheid bezien vanuit het licht van informatie (in tegenstelling tot techniek) en tevens bezien vanuit het bredere perspectief van ontwikkelingen binnen de iOverheid en de iSamenleving. Waar daar aanleiding toe is, moeten internationale ontwikkelingen expliciet in de advisering betrokken worden. Met name op het internationale en het Europese vlak geldt dat beslissingen worden besproken en genomen die pas veel later zichtbaar worden in de Nederlandse politieke en maatschappelijke arena. Omdat deze beslissingen echter wel bepalend zullen zijn voor de verdere ontwikkeling van de iOverheid en haar vertakkingen over de grenzen van Nederland heen, is het van groot belang deze te tijdig te signaleren, bespreken en doordenken. De commissie kan in de advisering tevens invulling geven aan de ambitie van het kabinet-Rutte om voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens al bij de voorbereiding nadrukkelijk te toetsen aan effectiviteit (Regeerakkoord 2010: 42). Het zal daarbij juist de opdracht van de commisssie moeten zijn om deze taak op te vatten vanuit het bredere perspectief van ontwikkelingen binnen de iOverheid en de iSamenleving. Ook zal de toets meer omvatten dan effectiviteit, maar een afweging zijn van de stuwende, verankerende en procedurele beginselen.

Maar de agenda van de commissie zal breder moeten zijn dan uitsluitend advisering over voorgenomen maatregelen. Een regelmatig terugkerend agendapunt is de evaluatie van lopende, gestrande en afgeronde ICT-projecten in het licht van informatiestromen en de verhouding tussen service, care en control. Juist omdat de iOver-

heid zich kenmerkt door doorlopende processen van verknoping en vertakking, is het van groot belang om projecten en koppelingen van informatie kritisch te volgen, lessen uit het verleden te trekken en het debat daarover te faciliteren. Dat debat zou dan onder meer moeten gaan over *function creep*. Daarbij moet aandacht zijn voor *function creep* als inherent kenmerk van innovatie en voor function creep in problematische zin, waarbij beide zijden van de medaille overigens soms vervelend dicht bij elkaar kunnen liggen. Ook zou de commissie, op basis van de jaarverslagen van het iPlatform en de iAutoriteit (zie verderop) situaties en systemen waarin burgers (maar ook bedrijven) in moeilijkheden komen, moeten inventariseren om daar op een meer algemeen niveau lessen uit te kunnen trekken en verbeteringen of verslechteringen te kunnen monitoren. Een expliciet aandachtspunt bij de evaluatie van ICT-projecten is het voorkomen van de – maar al te gebruikelijke – blikvernauwing naar de technische en financiële kant van ICT-projecten. De commissie zou zich veel sterker moeten richten op het faciliteren en toetsen van de vraag of een nieuwe applicatie ook daadwerkelijk dat levert, in termen van informatie, wat vanuit de achterliggende beleidsdoelstelling was gevraagd. Vanuit de doelstelling te komen tot een verankering van het 'besef een iOverheid te zijn', is lessen willen trekken vooralsnog belangrijker dan verantwoording laten afleggen.

Het rapport van de commissie wordt in beide Kamers van de Staten-Generaal plenair en in aanwezigheid van de voorzitter van de commissie besproken. Het is aan de Tweede Kamer om conclusies te verbinden aan de aanbevelingen. Het bureau van de Rijkscio zou het secretariaat van de Commissie moeten voeren om zo een institutionele verbinding te creëren tussen het besef van de iOverheid in de regering en in het parlement. Ook zou zo de strategische en toekomstgerichte functie van de CIO binnen de rijksoverheid versterkt kunnen worden.

Het bureau van de Rijks-CIO zou tevens ondersteuning kunnen bieden aan een ten behoeve van de commissie op te richten breed maatschappelijk forum. Dit forum moet vanuit een adviserende rol de verbinding tussen de permanente commissie voor de iOverheid en de iSamenleving faciliteren. Naar voorbeeld van het reeds bestaande – breed samengestelde – Forum Standaardisatie dat momenteel het College Standaardisatie ondersteunt, dient dit op te richten forum de commissie voor de iOverheid te voeden met ideeën, aandachtspunten en oplossingen. In het forum zal een breed scala aan stakeholders en deskundigen moeten deelnemen. Behalve vertegenwoordigers van de verschillende departementen, uitvoeringsorganisaties en gemeenten dient dit forum ook deskundigen vanuit de private sector (niet als vertegenwoordiger van een specifiek bedrijf, maar vanuit de specifieke kennis die daarmee aan tafel wordt gebracht), wetenschappers, toezichthouders en 'burgers', in de vorm van maatschappelijke organisaties als de Consumentenbond en mensenrechtenorganisaties te participeren. De commissie-Doctors van Leeuwen stelde al in 2001 een dergelijk orgaan voor onder de noemer 'Platform voor de Elektronische Samenleving' die ten dienste zou staan van een regeringscommissaris (Eenmalige

Adviescommissie ICT en Overheid 2001). De regering wees de voorstellen van de commissie indertijd af onder verwijzing naar de coördinerende rol voor ICT van de minister van Grote Steden en Integratie. Die zou een betere verankering bieden, concludeerde de regering in haar officiële reactie. Met die redenering kan echter niet meer worden volstaan. Het perspectief van de iOverheid is een breuk met een overheidstraditie van denken in termen van de eOverheid en vereist een ander geluid dan wat een coördinerend minster kan en vaak ook wil brengen. Bovendien vormen de netwerken van de iOverheid, zowel intern als met externe partijen, en de bewustmaking van de effecten daarvan een agenda die niet tot één departement en zelfs niet uitsluitend tot de overheid beperkt moet worden. De iOverheid kan pas een kwestie van coördinatie worden als dat besef daadwerkelijk en duurzaam verankerd is.

3.2 Het iPlatform en de iAutoriteit

Eén ontwikkeling die sterk uit de empirie naar voren komt is het ontstaan van een enorme 'backoffice' van informatiestromen bij de overheid, die deels ook tot buiten de grenzen van de overheid reikt. De informatie in deze netwerken is, zoals eerder gesteld, in termen van verantwoordelijkheid vaak 'verweesd'. Voor burgers is het soms nagenoeg onmogelijk om incorrecte informatie te corrigeren, terwijl ze in hun interactie met de overheid wel met de gevolgen daarvan worden geconfronteerd. Achter de extreme gevallen van identiteitsfraude die de voorpagina's van de kranten halen gaan vele gevallen schuil van burgers die de bestandsvervuiling van de overheid moeten zien te corrigeren en daarvoor geen eenduidige ingang vinden. Het netwerk van organisaties dat zich het lot van deze burgers aantrekt is noch dekkend noch berekend op die taak. Sommige initiatieven zijn slechts tijdelijk, voor andere vallen individuele problemen buiten de taak, velen hebben nauwelijks personeel en middelen en geen enkele organisatie heeft daadwerkelijk de doorzettingsmacht om fouten in het achterliggende netwerk te corrigeren. Ook de Nationale Ombudsman moest, in de meest gemediatiseerde zaak van identiteitsfraude, de zaak-Kowsoleaa, constateren dat een daadwerkelijke correctie van foutieve informatie onmogelijk bleek.

Maar het 'verweesde' beeld betreft niet alleen incorrecte informatie. Het geldt, zo laat de empirie zien, evenzeer de informatie die de overheid via een rijkgeschakeerd landschap aan websites, e-loketten en webportals naar burgers toe communiceert. Meer en meer is bij deze initiatieven een veelheid aan – soms ook private – partijen betrokken en blijken ze zonder een expliciete democratische legitimatie en besluitvorming te zijn ontstaan. Bij veel van deze nieuwe genetwerkte communicatiemodellen is de formele verantwoordelijkheid voor de beschikbare informatie en communicatie bovendien allesbehalve eenduidig belegd. Het goed organiseren van transparantie en accountability zodat de burger niet de dupe wordt van die elementen van de iOverheid waarop hij noch zicht heeft, noch invloed kan uitoefenen, geeft uitvoering aan de maatschappelijke functie.

Transparantie en accountability van de iOverheid moeten van een duidelijk 'adres' worden voorzien. Er dient daarom voor burgers één platform te komen waar de transparantiefunctie invulling krijgt en één autoriteit waar de accountability wordt belegd.

Net zoals de overheid bij haar dienstverlening streeft naar een één-loketgedachte, zou de overheid ook bij de functies van transparantie en correctie naar één ingang moeten streven. Daarmee zouden ook de her en der over internet verspreidde en sterk applicatie- of probleemgerichte overheidsfora zoals burgerservicenummer.nl (voor het bsn), infobsnzorg.nl (voor het EPD), lastvandeoverheid.nl, mijnoverheid.nl, mijnprivacy.nl (van het CBP) en het meldpunt ID-fraude voor burgers onder één digitaal dak gebracht worden. Het iOverheidsplatform moet een interactief informatiepunt zijn over informatisering in de relatie tussen de burger en de overheid: dit is de transparantiefunctie. Door deze informerende functie moet het burgers allereerst via één eenduidige ingang duidelijk worden hoe zij in de gekoppelde systemen van de iOverheid staan geregistreerd en wie en waarom daar toegang toe hebben. Naar voorbeeld van de toeslagenportal van de Belastingdienst moet de burger hier bovendien zijn gegevens zelf via een beveiligde omgeving kunnen muteren en corrigeren – waarbij gewaarborgd moet worden dat ze in het gehele netwerk worden aangepast. Het versterken van de transparantiefunctie met interactiviteit als kenmerkend uitgangspunt dient ook de emancipatie van burgers. De interactieve gedachte achter het platform sluit daarmee aan bij de bredere tendens in de iSamenleving waarin digitalisering de emancipatoire mogelijkheden van burgers versterkt en van nieuwe impulsen voorziet.

De tweede maatschappelijke functie, die van accountability, heeft een actief karakter en is al eerder bepleit door de Nationale Ombudsman (2009). De iAutoriteit moet ervoor zorgen dat misrepresentaties van burgers in de backoffice en overige systemen daadwerkelijk worden gecorrigeerd. Hier moet het probleem letterlijk uit handen van de burger genomen worden om het in de ketens en netwerken van de iOverheid recht te zetten en op te lossen. Dit is een radicale centralisatie van het beginsel van accountability. De huidige mogelijkheden om decentraal en via verschillende instanties en toezichthouders fouten te corrigeren die in het netwerk zijn opgenomen, zijn door de jaren heen onvoldoende gebleken. Bij deze iAutoriteit moeten expertise en een persoonlijke behandeling worden gecombineerd met een stevige doorzettingsmacht ten opzichte van de organisaties die het netwerk van de backoffice van de iOverheid bevolken. Die doorzettingsmacht is van groot belang, want als deze ontbreekt, neemt de iAutoriteit simpelweg de gemankeerde positie van de burger over wanneer deze door de verschillende organisaties van het kastje naar de muur wordt gestuurd. Dan is het probleem slechts verplaatst, maar niet opgelost. Overigens moet goed worden doordacht in welke mate burgers toegang hebben tot de iAutoriteit. Enerzijds moet het herkenbaar en laagdrempelig zijn, maar anderzijds zou een te lage drempel het voor bepaalde burgers wellicht te gemakke-

lijk maken om zand in de machinerie van de iOverheid te strooien,v aangezien dit model relatief grote inspanningen aan de kant van het bestuur veronderstelt.

Het iPlatform zou op digitaal vlak een uitbouw kunnen zijn van het huidige mijnoverheid.nl. Organisatorisch moet de iAutoriteit als een onafhankelijke partij met doorzettingsmacht worden opgezet. Alle bestaande informerende platforms en operationele organisaties, waaronder ook het meldpunt id-fraude, dienen in deze organisaties opgenomen te worden dan wel samen te komen. Het iPlatform en de iAutoriteit publiceren jaarlijks een gezamenlijk rapport waarin verslag wordt gedaan van de werkzaamheden, de resultaten daarvan alsmede de belangrijkste ontwikkelingen en trends.

3.3 Opdrachtgeverschap geprofessionaliseerd

Het besef van de iOverheid moet uiteindelijk ook belegd worden op het technische niveau van de ontwikkeling van standaarden, applicaties en koppelingen van informatie. Dit is de operationele functie. Op de tekentafels van de techniek en in de (internationale) gremia van de standaarden wordt immers bepaald hoe de iOverheid er in de praktijk uit komt te zien. Het besef dat dit in essentie politieke en beleidsmatige keuzes zijn valt in de praktijk vaak weg tegen de gedachte dat techniek niet meer dan een instrument is. Wie de informatiestromen volgt – zoals in dit rapport is gedaan – weet dat via de techniek categorieën ontstaan en *categories have politics*. Dat betekent dat ontwerpkwesties, standaardisaties en interoperabiliteit allemaal van bepalend belang zijn voor de ontwikkeling van de iOverheid als geheel en niet alleen voor individuele applicaties en beslissingen. Een van de cruciale momenten in de ontwikkeling van de iOverheid is het opdrachtgeverschap van de overheid. Het uitwerken en vaststellen van de eisen aan en de functies van nieuwe systemen en applicaties is bepalend voor de (toekomstige) mogelijkheden van nieuwe toepassingen en hun plaats in het bredere kader van de iOverheid. De overheid hinkt daarbij sterk op twee gedachten; enerzijds wil zij de ontwikkeling vaak zelf ter hand nemen, bijvoorbeeld via de ontwikkelorganisatie ICTU, anderzijds blijkt het onmogelijk en onpraktisch om de benodigde technische kennis zelf in huis te hebben. Het overgrote deel van de technici 'in dienst' van de overheid zijn externe adviseurs en technici. Het resultaat is een overinvestering in technische kennis, en te weinig aandacht voor de interactie tussen beleid, uitvoering en techniek waarin informatiestromen centraal staan.

Het opdrachtgeverschap van de overheid zou daarom over een geheel andere boeg gegooid moeten worden door te investeren in kennis op het snijpunt van beleid, uitvoering en techniek in plaats van investeren in technische kennis. Wil de overheid het oplossen van de ICT-problemen structureel aanpakken, zoals het kabinet-Rutte ambieert (Regeerakkoord 2010: 42), dan zal het de aandacht moeten verleggen van technische ontwikkeling naar de professionele opdracht. Dat betekent dat de technische realisatie primair aan partijen buiten de overheid wordt overgelaten

(door applicaties daar te laten ontwikkelen dan wel op de markt in te kopen). De overheid zelf dient te investeren in de kennis om de opdracht te formuleren, het pakket van eisen en de juridische context en randvoorwaarden scherp te krijgen, een en ander in een bredere context te doordenken en de ontwikkeling vakkundig te begeleiden. Dat de techniek werkt is de taak van de ontwikkelaar. Dat de techniek de 'juiste' informatie genereert en informatieprocessen faciliteert binnen de categorieën en bandbreedten die in het beleid en in overleg met de uitvoering zijn geformuleerd is de controlerende en begeleidende taak van de opdrachtgever. Dit betekent dat een organisatie ingericht moet worden die een andere invulling geeft aan het opdrachtgeverschap en daarbij niet gebonden is aan de grenzen van departementen en individuele uitvoeringsorganisaties. Deze organisatie zou een kleine kern hebben van eigen ICT'ers en ICT-juristen met kennis van de iOverheid die per project aangevuld kan worden met de CIO van het betreffende beleidsdepartement, ambtenaren van het beleidsdepartement en medewerkers vanuit uitvoeringsorganisaties die met het uiteindelijke systeem moeten werken. Het structureel betrekken van de ketenpartners of de netwerkpartners bij de ontwikkeling van applicaties lijkt een open deur, maar is in de praktijk relatief zeldzaam. Ook hier lopen de informatiestromen in de regel vooruit op de betrokken organisaties.

De iOverheid dient werk te maken van goed opdrachtgeverschap, waarbij investeren in eigen kennis op het snijpunt van beleid, uitvoering en techniek prioriteit heeft boven het in huis hebben van zuiver technische kennis en ontwikkelcapaciteit.

4 DE iOVERHEID IN UITVOERING

Om zowel aan te sluiten bij de realiteit van de iOverheid als in staat te zijn de verdere ontwikkeling daarvan in werkbare banen te leiden zal de Nederlandse overheid in woord en daad de transformatie van een eOverheid naar een iOverheid moeten maken. Wil de overheid in de toekomst het pad van digitalisering met vertrouwen kunnen vervolgen, dan zal het besef een iOverheid te zijn in alle lagen van de overheid verankerd dienen te worden. Daarbij schuilt de belangrijkste inhoudelijke opdracht in de bereidheid en het vermogen het debat niet langer te voeren via de band van technieken en individuele applicaties, maar dit te debat aan te gaan vanuit het besef van samenhangende informatieprocessen en verknoopte informatie. Van wezenlijk belang daarbij is allereerst dat er ruimte en aandacht is voor een open afweging tussen de drijvende, verankerende en de procedurele beginselen. Een zorgvuldige ontwikkeling van de iOverheid kan niet zonder een dergelijke afweging, waarbij het van groot belang is dat deze afweging wordt gemaakt in het licht van de iOverheid als geheel. Hiernaast geldt dat van de overheid bij zowel deze afweging als de verdere inrichting van beleid en uitvoering, extra behoedzaamheid verlangd mag worden wanneer sprake is van een drietal in dit rapport gesignaleerde processen van informatieverwerking. Deze processen – die in symbolische zin zijn voorzien van waarschuwingsvlaggen – houden verband met a) het vernetwerken van

informatie, b) het samenstellen en verrijken van informatie, en c) het voeren van preventief beleid op basis van informatie. De specifieke gevolgen die deze processen hebben voor de uitvoering van beleid, de positie van burgers, de kwaliteit van de overheidsinformatiehuishouding en de interne en externe aanknopingspunten voor aansprakelijkheid en verantwoording, noodzaken tot behoedzaamheid en een kritische houding ten opzichte van nut, noodzaak en maatschappelijke consequenties van digitaliseringsinitiatieven.

Om deze inhoudelijke opdracht van pleitbezorgers te voorzien en daarmee zorg te dragen voor de noodzakelijke institutionele verankering formuleert dit rapport een agenda voor institutionele transformatie. De instituties die in het kader van deze transformatie worden voorgesteld moeten garanderen dat de iOverheid de instrumenten in handen heeft om bewustwording, bescherming en innovatie te faciliteren. Daarbij moet het overigens helder zijn dat de institutionele transformatie als zodanig vele malen belangrijker is dan de in dit rapport voorgestelde (naambordjes van) instituties. Op een drietal niveaus zal de noodzakelijke transformatie gestalte moeten krijgen. Op het strategische niveau (via de installatie van een permanente commissie voor de iOverheid), op het maatschappelijke niveau (via een iPlatform ten behoeve van transparantie en een iAutoriteit ten behoeve van accountability) en op het operationele niveau (via professionalisering van het opdrachtgeverschap en prioritering van kennis op het snijvlak van techniek en beleid in plaats van kennis van de techniek zelf). Ten slotte, voor zowel de inhoudelijke opdracht als de noodzakelijke institutionele transformatie geldt dat de ontwikkeling van de iOverheid niet los gezien kan worden van het pad dat de bredere iSamenleving volgt.

NOTEN

1 Uiteindelijk is dat uiteraard ook een collectief belang, omdat een samenleving die niet vergeet en vergeeft een fundamenteel andere is dan een samenleving waarin men opnieuw kan beginnen.

2 Senator Joseph Lieberman had in een statement laten weten dat providers als Amazon (die WikiLeaks had gehost) al hun banden met WikiLeaks dienden te verbreken. “I will be asking Amazon about the extent of its relationship with WikiLeaks and what it and other web service providers will do in the future to ensure that their services are not used to distribute stolen, classified information”, zie het artikel Banishing WikiLeaks van Amy Davidson in the New Yorker, http://www.newyorker.com/online/blogs/closeread/2010/12/banishing- wikileaks.html, opgevraagd 10.12.2010.

3 Gesprek met dhr. P. Wijntje en dhr. S. Peereboom (Financiën/Belastingdienst), 19 oktober 2010.

4 ljn: BK6331, Hoge Raad, 08/04524 B.

5 Vgl. de discussies over (m.n.) milieuorganisaties en hun toegang tot de bestuursrechter.

III EPILOOG: DE IOVERHEID EN DE ISAMENLEVING

In de kern gaat dit rapport over de verantwoordelijkheid van de overheid voor haar eigen gebruik van ICT. Maar de rol en verantwoordelijkheid van de overheid in de informatiesamenleving reiken natuurlijk verder. Behalve de verantwoordelijkheid voor de iOverheid, berust bij de overheid ten principale ook een zekere verantwoordelijkheid voor het functioneren van de iSamenleving. Die bredere verantwoordelijkheid is in de volgende vragen te vatten. 'Wat dient de overheid zich in de ontwikkeling van de informatiesamenleving aan te trekken, en (hoe) heeft zij daarin te interveniëren?' Toenmalig premier Kok kaartte de kwestie al eens aan in een toespraak op het Infodrome-congres op 11 april 2001: "Toch moeten wij ons thans de vraag stellen welke verantwoordelijkheden, in de jaren die voor ons liggen, op de weg van de overheid komen in verband met aan de informatiesamenleving inherente gevolgen." Deze verantwoordelijkheid kan worden gedefinieerd als de systeemverantwoordelijkheid van de iOverheid voor de iSamenleving. Uiteraard zijn de interventies in de iSamenleving altijd politiek gekleurd en omstreden, maar er kan toch worden geprobeerd een soort common ground te formuleren voor de zaken waar een overheid garant voor moet staan. De systeemverantwoordelijkheid van de iOverheid kan niet zonder meer terzijde geschoven worden.

Allereerst omdat de overheid moet opkomen voor haar burgers wanneer private partijen het belang van deze burgers onvoldoende garanderen. Zo stelt de groeiende informatiemacht van mondiale spelers als Google, Facebook en Apple de (Europese) overheid voor de vraag of en op welke wijze deze macht om redenen van publieke belangen beteugeld dient te worden. Op een aantal dossiers zijn al eerste bewegingen in die richting waar te nemen. Voormalig minister van Economische Zaken, Van der Hoeven, deed in reactie op Kamervragen begin augustus 2010 de toezegging het College Bescherming Persoonsgegevens (CBP) te vragen om een nieuwe clausule in de privacyvoorwaarden van Apple te beoordelen.[1] Sommige kwesties die aan de systeemverantwoordelijkheid van de overheid raken, zullen echter op Europees niveau en via een Europese actor (*lead authority*)[2] geadresseerd moeten worden, omdat alleen daar de noodzakelijke massa en doorzettingsmacht gevonden kunnen worden. Maar ook de populariteit van interactieve communicatie via sociale netwerken en web 2.0 roept de vraag op of er een verantwoordelijkheid voor de overheid ligt om de gedragingen van burgers te sturen en te beperken en/of burgers te beschermen tegen marktpartijen. Tot op zekere hoogte geldt bovendien dat de systeemverantwoordelijkheid van de overheid voor bovenstaande en andere ontwikkelingen juridisch afdwingbaar is op grond van de mensenrechten (De Hert 2011).

"De aanname dat de Europese rechtspraak te weinig concrete handvatten geeft voor overheden is onterecht. Op het gebied van de bescherming van persoonsgegevens heeft het Hof algemene beginselen ontwikkeld, die in steeds meer zaken toegepast worden. Hetzelfde is in iets mindere mate waar voor de strijd tegen identiteitsfraude en de bescherming van het mediapluralisme. Nederland kan met die beginselen aan de slag" (De Hert 2011).

De vraag *hoe* de iOverheid zijn systeemverantwoordelijkheid in moet vullen is in die zin wellicht prangender dan de vraag *of* ze die in moet vullen.

Ten tweede kan systeemverantwoordelijkheid ook aan de orde zijn wanneer ontwikkelingen in het private domein te zeer interfereren met (vitaal) beleid van de overheid. Illustratief hier zijn de ontwikkelingen op het terrein van identiteitsmanagement. Zoals deel 2 van dit rapport laat zien, investeert de overheid veel in digitale middelen om de identiteit van burgers vast te stellen, bijvoorbeeld via applicaties als het (biometrisch) paspoort, DigiD en mogelijk in de toekomst het eRijbewijs. Juist omdat de overheid veel investeert in die identiteitsbepaling – en de accuratesse daarvan claimt – moet ze ook aandacht hebben voor identiteitsbepaling in het semipublieke en commerciële domein, in het bijzonder voor de risico's op verwatering van de kwaliteit daarvan. Wat bijvoorbeeld is de waarde van een streng beveiligde centrale opslag van biometrische gegevens in het kader van de Paspoortwet, als dezelfde gegevens ook buiten het domein van de overheid breed beschikbaar zijn? De invoering van een biometrisch paspoort roept vragen op over het gebruik van biometrie in de private sector. Momenteel is nauwelijks sprake van regulering of zelfs maar politieke aandacht en experimenteren zwembaden, supermarkten, werkgevers en computerfabrikanten volop met nieuwe toepassingen van deze technologie.

Vanwege de enorme toename van verzamelde informatie worden identificaties ook buiten de overheid steeds belangrijker als sleutels om informatie te kunnen koppelen en combineren. Het empirisch materiaal laat zien dat bij het gebruik van identificaties de grenzen tussen de publieke en private sector steeds diffuser worden, hetgeen impliceert dat ook de effecten van dat gebruik over de grenzen heen spelen. Zeker nu sommige actoren in de private sector een publiekrechtelijke taak hebben (notaris) dan wel de overheid van private partijen verlangt dat ze de identiteit van burgers vaststelt (Wet identificatieplicht dienstverlening; arbeidsrelatie) aan de hand van door de overheid uitgegeven identiteitsdocumenten. Het bsn bijvoorbeeld werd als identificatiesleutel bedacht voor overheidsdiensten, zonder er rekenschap van te geven dat het zich binnen de kortste keren tot een *universal* (pubiek-private) *unique identifier* zou ontwikkelen. Om deze en andere redenen moet de overheid alert zijn op ontwikkelingen buiten de overheid en overwegen of en wanneer het noodzakelijk is nadere kaders of regels te stellen.

Dat een zekere eindverantwoordelijkheid ten principale bij de overheid ligt wil overigens nog niets zeggen over de vraag of zij die ook zelf ter hand moet nemen (De Hert 2011) of daar zelfs maar de mogelijkheden en capaciteiten voor in huis heeft (Meijer 2011). De grondrechtelijke eindverantwoordelijkheid van de overheid is bovendien een lastige zaak, omdat er voor een aantal valkuilen gewaakt moet worden. In de eerste plaats moet er niet te gemakkelijk over sturing worden gedacht. Interveniëren in maatschappelijke en in dit geval informationele verhoudingen is weliswaar de bestaansreden van de staat, maar het is tegelijkertijd in zekere zin een waagstuk: interventies kunnen door allerlei factoren in hun tegendeel verkeren, en het is zaak daar vooraf bij stil te staan. In de tweede plaats is het een valkuil om interventies met een 'gebruikersmentaliteit' aan te vatten: de informatiesamenleving is niet 'van de overheid', en daarom dient er ten volle rekenschap gegeven te worden van de rechtsstatelijke voorwaarden die aan interventies gesteld worden. In de derde plaats zijn er verschillende manieren om te interveniëren, en zijn verkeerde keuzes snel gemaakt. Om met de meest traditionele modus te beginnen: de overheid kan zich dwingend regulerend mengen in de informationele verhoudingen. Zij kan zich echter ook helemaal aan de 'zachte' kant van het spectrum positioneren door zich enkel als gesprekspartner voor private spelers op te stellen. Daartussenin bevindt zich nog de specifieke modus van het faciliteren: randvoorwaarden scheppen voor het tot ontplooiing komen van maatschappelijke mogelijkheden. Bij deze verschillende modi horen steeds andere verantwoordelijkheidsoverwegingen.

Volgens Meijer (2011) wordt het echter steeds lastiger, en misschien wel fundamenteel onmogelijk, om vanuit systeemverantwoordelijkheid 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 uitkomsten, maar wel voor de kwaliteit van het proces. Vanuit een restverantwoordelijkheid 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 voorgestelde commissie voor de iOverheid kan in het denken over systeemverantwoordelijkheid van de overheid een belangrijke agenderende rol spelen. De kernvragen die de commissie vanuit deze rol kan adresseren zijn: welke ontwikkelingen in de bredere iSamenleving dienen ondersteund of juist beteugeld te worden en op welk niveau (nationaal of internationaal) kan normerend optreden het beste worden belegd? Van welke ontwikkelingen kan worden verwacht dat de effecten zullen doorsijpelen in de iOverheid en wat betekent dat voor eventueel regulerend (conditionerend) optreden?

Bepaalde ontwikkelingen in de iSamenleving zullen de overheid echter in toenemende mate voor fundamentele vragen stellen waarop momenteel nog geen begin van een antwoord geformuleerd is. De snelheid waarmee informatie – ook als die de overheid onwelgevallig is – wordt verspreid en gekopieerd, maakt dat de overheid ook na zal moeten denken over haar eigen informatiemanagement. Dat heeft de WikiLeaks-affaire overtuigend laten zien. Transparantie wordt in de regel gezien als iets wat de overheid haar burgers gunt (passieve openbaarheid), veel minder als een actief na te streven belang (actieve transparantie) en al helemaal niet als iets wat door (enkele) burgers wordt genomen of afgedwongen. In de digitale wereld zullen overheden zich echter steeds vaker voor de vraag gesteld zien hoe ze met transparantie om willen gaan. John Naughton schreef in *The Guardian* dat overheden voor een keuze staan: "Live with the WikiLeakable world or shut down the net. It's your choice" (Naughton 2010b). Die laatste keuze zal niet snel gemaakt worden. Desalniettemin zal er wel naar een hernieuwde balans tussen informatievrijheid, geheimhouding en beveiliging van gegevens gezocht moeten worden, waarbij regulering mogelijk aan de orde is. Een deel van het antwoord zal gezocht en gevonden worden in regulering van partijen buiten de overheid (servers, clouds etc.), voor een ander deel moet de overheid wellicht bij zichzelf te rade gaan. Sommige informatie moet misschien helemaal niet opgeslagen worden, andere informatiebronnen moeten wellicht juist transparanter in plaats van vertrouwelijk en geheim en sommige informatie moet wellicht nog beter beveiligd worden.[3] Maar de onvoorspelbaarheid en onzekerheid van de samenleving en daarmee ook van de iSamenleving zal de overheid uiteindelijk nooit volledig buiten de deur kunnen houden, zoals de WRR (2008) al eerder betoogde (zie ook Van Asselt et al. 2010).

Als het gaat om de verantwoordelijkheid van de iOverheid voor de iSamenleving geldt eenzelfde soort afwegingskader als voor de het gebruik van ICT door de overheid zelf. Het definiëren van een systeemverantwoordelijkheid komt in essentie ook voort uit een afweging van stuwende, verankerende en procesmatige beginselen, zij het dat de stuwende beginselen nu veelal buiten de overheid liggen. Burgers en bedrijven worden voortgestuwd door enthousiasme voor nieuwe technische mogelijkheden en overwegingen van winstgevendheid. Waar deze structureel onvoldoende worden afgewogen tegen verankerende beginselen en onvoldoende in balans worden gebracht met een uitwerking van procesmatige beginselen die informatiestromen voor burgers transparant en, indien nodig, aanvechtbaar maken, dient de iOverheid zich af te vragen of ze aan zet is.

NOTEN

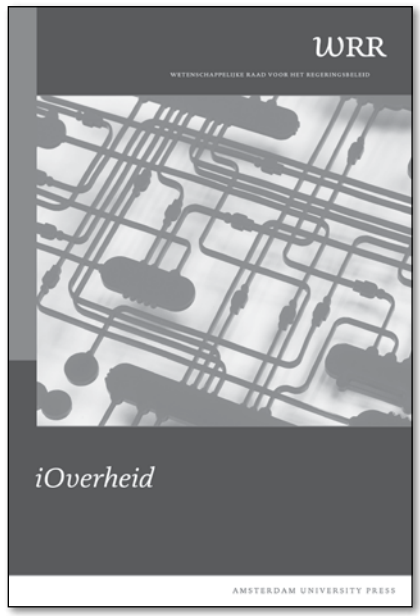
1 Brief van minister van Economische Zaken, beantwoording vragen over nieuwe clausule in de privacyvoorwaarden van Apple, 03-08-2010.

2 Binnen Europa wordt inmiddels gepleit voor een *lead authority* met voldoende bevoegdheden om dit soort zaken voor de 27 lidstaten op te knappen (gesprek J. Hennis-Plasschaert, vvd-fractie Tweede Kamer, 4 november 2010).

3 Zoals onder meer wordt gesuggereerd in de analyse van 'WikiLeaks – cable gate' door Bits of Freedom. Zie Ot van Daalen, De wereld na WikiLeaks' cable gate, op https://www.bof.nl/2010/12/10/de-wereld-na-wikileaks-cablegate/

IV BESTELINFORMATIE

Het WRR-Rapport *iOverheid* en de WRR-Verkenning *De staat van informatie* zijn te bestellen bij Amsterdam University Press, Herengracht 221, 1016 BG te Amsterdam (info@aup.nl). De teksten zijn te downloaden via www.wrr.nl of www.ioverheid.nu.



iOverheid, ISBN 978 90 8964 309 4

De staat van informatie, Dennis Broeders, Colette (M.K.C.) Cuijpers & Corien (J.E.J.) Prins, ISBN 978 90 8964 310 0

Amsterdam University Press