

Vergaderjaar 2011–2012

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 211

**BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN
KONINKRIJKSRELATIES**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 25 oktober 2011

De Wetenschappelijk Raad voor het Regeringsbeleid heeft mij op 15 maart 2011 haar rapport «iOverheid» aangeboden. Hierbij bied ik u namens het kabinet de kabinetsreactie op dit rapport aan. De kabinetsreactie gaat in op de ontwikkeling van de iSamenleving en iOverheid in den brede en niet op individuele casussen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,
J. P. H. Donner

Kabinetsreactie op WRR-rapport iOverheid: de rol van de overheid in de iSamenleving

Samenvatting

Het kabinet ziet in het rapport van de WRR waardevolle aanknopingspunten om zijn visie op de voortgaande digitalisering en de gevolgen hiervan voor burgers en voor de overheid uiteen te zetten. De iSamenleving en de iOverheid nopen tot een herbezinning. Het kabinet kondigt in zijn visie aan welke initiatieven het neemt om de hiermee gepaard gaande ontwikkelingen het hoofd te bieden. Het kabinet zet in op het verinnerlijken van het besef bij bestaande overheidsinstituties, een iOverheid te zijn. Die benadering volgt niet primair de suggestie van de WRR om te komen tot het inrichten van een iCommissie, een iPlatform en een iAutoriteit om de uitdagingen van de iSamenleving het hoofd te bieden. Het kabinet verwelkomt evenwel de *functionele* betekenis die schuilgaat achter deze suggesties van de WRR. Het vraagstuk dat aan de orde is in de iSamenleving wordt naar de mening van het kabinet niet opgelost met het instellen van nieuwe instituties op nationaal noch op internationaal niveau. Een gevaar bij het instellen van dergelijke instituties is dat het mogelijk suggereert dat het kabinet overheidssturing en regie heeft geregeld, en dat daarmee het vraagstuk is afgedaan. Het verinnerlijken van het bewustzijn een iOverheid te zijn, sluit aan bij de functionaliteiten die de WRR voorstelt. De overheid moet aldus zelf vanuit het door de WRR geschetste perspectief gaan handelen. Het gaat veeleer om het streven naar een zichtbare en effectieve transformatie binnen de bestaande instituties en om het besef een iOverheid te zijn, dan om instituties die dat van buitenaf zouden moeten bewerkstelligen. Het kabinet wenst de iSamenleving zoveel mogelijk te betrekken bij de duurzame uitbouw van de iOverheid.

Het kabinet deelt de analyse van de WRR dat met een transformatie van een eOverheid naar een iOverheid zowel nieuwe kansen als uitdagingen ontstaan. Kansen en uitdagingen voor beheer en beleidsvorming, zowel op rijksniveau als binnen de andere lagen van de overheid. Naar aanleiding van het WRR-rapport zijn op onderdelen al eerste stappen gezet om de iOverheid vorm te geven. Het kabinet ziet een belangrijke taak in het verder equiperen van de rijksoverheid om aan de nieuwe uitdagingen tegemoet te kunnen treden. Voorop daarbij staat dat de overheid in al haar lagen verantwoordelijk is voor het eigen informatiebeheer. Het ligt op de weg van de overheid, en binnen de verantwoordelijkheid van elk van de overheidslagen, om slechts na een zorgvuldige afweging te besluiten tot uitwisseling van persoonsgegevens. Daarnaast moeten de datastromen die de overheid beheert zo goed mogelijk worden onderhouden en beveiligd. Hiervoor moeten blijvend passende structuren worden gecreëerd. Het kabinet wenst bovendien de burger en ondernemer beter in staat te stellen problemen met de verwerking of uitwisseling van (persoons)gegevens in de iSamenleving zelf aan te pakken.

Het kabinet wil evenwel benadrukken dat de nationale overheid niet in staat is of zal zijn over datastromen in de informatiesamenleving (hierna: iSamenleving) in den brede regie te voeren, of die naar zich toe te trekken. Bovendien acht het kabinet het wenselijk noch noodzakelijk om te streven naar een regierol in de iSamenleving. De overheid heeft niet tot taak alle risico's te beheersen; zij heeft echter wel tot taak de burger in de iSamenleving optimaal te voorzien van mogelijkheden om zelf (mede) sturing te geven aan de iSamenleving, bijvoorbeeld met behulp van effectieve correctie- en inzagerechten. Datastromen zijn steeds vaker grensoverschrijdend en bewegen zich langs veelsoortige actoren. De rol van de overheid bij het in goede banen leiden van digitale datastromen in en het

beteugelen van kwalijke gevolgen van de iSamenleving zal mede om die reden noodzakelijkerwijs eerder faciliterend moeten zijn. Bij het faciliteren van de bescherming van de burger zullen de arrangementen eerder worden gezocht in het civiele recht dan in het publiekrecht, omdat laatstgenoemde in grensoverschrijdende context beduidend minder impact heeft. In het zoeken naar de optimale rol in de iSamenleving stuit de overheid bovendien op een dilemma. Aan de ene kant wordt verwacht dat de overheid het eigen handelen aan banden legt met het oog op de bescherming van de privacy en keuzevrijheid. Aan de andere kant wordt een effectieve en efficiënte overheid verwacht die juist meer armslag nodig heeft om burgers waar deze zich ook bevinden, te beschermen tegen gevaren en de risico's. Het kabinet streeft naar een evenwichtige balans tussen «ruimte laten» en «bescherming bieden». Gegeven dit dilemma en de beperkte sturingsmogelijkheden die de overheid heeft, kiest het kabinet voor inzet langs twee lijnen:

- het op orde brengen en houden van het overheidshandelen in de iOverheid en iSamenleving
- het equiperen van burgers om zichzelf te beschermen en eventuele problemen of misstanden recht te zetten.

Opzet van de kabinetsvisie

In deel I zet het kabinet zijn visie op de iOverheid in de iSamenleving uiteen. In deel II schetst het kabinet, welke kansen en perspectieven op dit moment worden onderzocht voor het verder versterken van een effectieve iOverheid. De opvattingen van de WRR zullen voorafgaand aan de visie van het kabinet steeds recursieerd worden weergegeven.

Deel I

Visie op de rol van de overheid in de iSamenleving

• Kern van de analyse van de WRR

Op 15 maart 2011 bracht de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) zijn rapport «iOverheid» uit. De alomtegenwoordige inzet van informatie- en communicatietechnologie (ICT) door de overheid heeft ervoor gezorgd dat deze niet langer meer als een elektronische overheid, gericht op dienstverlening en gebruikmakend van techniek, kan worden gekarakteriseerd. In de dagelijkse praktijk is veeleer een informatie-Overheid of iOverheid ontstaan, gekenmerkt door informatiestromen en -netwerken en gericht op niet alleen dienstverlening, maar ook controle en zorg. Uitgangspunt in de analyses van de WRR is de vaststelling dat digitale datastromen een steeds belangrijker rol spelen in de samenleving. Deze ontwikkeling duidt de WRR aan als iSamenleving. Ook worden in steeds grotere mate door de overheid digitale datastromen gebruikt bij de uitvoering van diverse taken zoals zorg, dienstverlening en veiligheid. Het koppelen, bewerken en hergebruiken van persoonsgegevens wordt onder invloed van technologische ontwikkeling steeds gemakkelijker en goedkoper. In de dagelijkse praktijk van politiek en bestuur wordt volgens de WRR evenwel onvoldoende nagedacht over het groeiend gebruik hiervan. Het overgrote deel van de overheidsinitiatieven voor digitalisering en informatiestromen die daaruit volgen, worden geïsoleerd bepleit, beoordeeld en ingevoerd. In dit proces loopt de overheid, aldus de WRR, waar het gaat om datastromen tussen overheden onderling en datastromen tussen overheid en burgers echter wel het risico stapje voor stapje de beleidsmatige greep en regie in de iSamenleving kwijt te raken.

Het incident rond het bedrijf DigiNotar illustreert de vaststelling van de WRR dat digitale datastromen een steeds belangrijker rol spelen in de samenleving. In deze kabinetsreactie zal echter niet op de DigiNotar-casus worden ingegaan. Hierover is en wordt de Tweede Kamer separaat geïnformeerd¹.

Het kabinet deelt de vaststelling van de WRR dat de digitalisering en de grootschalige informatiestromen leiden tot fundamentele en onomkeerbare maatschappelijke ontwikkelingen, die nopen tot een herbezinning op de rol van de overheid in al zijn gelaagdheden.² Het kabinet wenst evenwel te benadrukken dat de nationale overheid niet in staat is of zal zijn over datastromen in de iSamenleving in de brede regie te voeren. Bovendien acht het kabinet het noch wenselijk, noch noodzakelijk om te streven naar een regierol in de iSamenleving. De overheid heeft niet tot taak alle risico's te beheersen; zij heeft echter wel tot taak de burger in de iSamenleving optimaal te voorzien van instrumenten om zelf regie te kunnen voeren.

• *Transformatie naar een iSamenleving*

Volgens de WRR zijn wij in het afgelopen decennium niet alleen een informatiesamenleving binnengestapt, maar is in wezen ook een nieuwe samenleving gecreëerd. De WRR duidt in dit verband op de «iSamenleving». Cruciaal in de iSamenleving is de vaststelling dat digitale datastromen een centrale rol zijn gaan vervullen in het verkeer tussen burgers, overheid en private partijen.

Deze iSamenleving heeft vele positieve gevolgen. Het uitwisselen van gegevens en verkrijgen van informatie kan sneller en goedkoper plaatsvinden dankzij de almaar voortschrijdende technologische ontwikkeling. De iSamenleving vormt op een aantal andere terreinen ook een nieuwe uitdaging. Het biedt ook kansen om bij de overheid aanwezige informatie beter te delen met burgers en bedrijven en de kwaliteit van gegevens en de opslag ervan te verhogen. Er is naar het oordeel van het kabinet een bredere vraagstuk aan de orde. Dat betreft niet alleen vraagstukken van privacy en informatiebeveiliging. Nieuwe communicatie- en verwerkingstechnieken hebben vergaande implicaties voor hoe de overheid haar taken vervult, diensten vormgeeft, hoe de overheid communiceert met burgers, maar ook hoe burgers onderling met elkaar in contact kunnen treden. Deze verandering is niet minder ingrijpend dan destijds de uitvinding van de boekdrukkunst.³ Het belangrijkste verschil is dat de veranderingen van toen enkele eeuwen in beslag namen, en nu binnen enkele jaren plaatsvinden. Mede daardoor zijn ze meer ingrijpend en meer zichtbaar.⁴ Destijds speelde eveneens de vraag naar de regie. Geprobeerd werd deze op centraal niveau te behouden met verstrekking van vergunningen aan boekdrukkers. Algehele centrale controle bleek echter al snel niet alleen onwenselijk maar ook onmogelijk. Het is belangrijk van deze les te leren. De uitdaging waar de nationale overheid nu voor staat is niet het proberen eenzijdig alle dataverkeer te beheersen en controleren, maar het garanderen van de juistheid, zorgvuldigheid en veiligheid van digitale datastromen waarvan de overheid zelf gebruikt maakt, het beheersbaar houden van de bredere gevolgen van digitalisering in de iSamenleving binnen en buiten de nationale grenzen, en het bieden van goede waarborgen tot correctie aan burgers en bedrijven als er iets fout gaat als gevolg van de inzet van digitalisering, en het (samen met burgers en bedrijven) bijdragen aan de beheersbaarheid van de bredere gevolgen van digitalisering in de iSamenleving binnen en buiten de nationale grenzen. De overheid zit bovendien, zoals destijds bij de boekdrukkunst, met een dilemma. Aan de ene kant wordt verwacht dat de overheid het eigen handelen aan banden legt met het oog op de bescherming van de

¹ Zie o.a. de brieven d.d. 5 en 16 september jl. Kamerstuk 26 643 nrs. 188 en 189.

² Het Rathenau Instituut werd bracht in november 2010 het rapport Databases Over ICT-beloftes, informatiehonger en digitale autonomie uit; de aanbevelingen van het Rathenau Instituut tonen grote gelijkenis met de bevindingen van de WRR.

³ Deze vergelijking wordt eveneens gemaakt in het onlangs verschenen rapport van het Europees Parlement, DG External Policies of the Union: «Information and Communication Technologies and Human Rights», 2010, p. 7: «Digital communications have empowered people to communicate directly with each other, rather than having to go through gatekeepers such as government spokespeople and the mass media. The changes that they have wrought on society are comparable to the impact of the invention of the Gutenberg press».

⁴ Tegelijkertijd zijn de veranderingen onzichtbaar – de wijze waarop techniek werkt en waar informatie «blijft» is voor veel burgers en ondernemingen een «black box».

privacy en keuzevrijheid. Aan de andere kant wordt juist een effectieve en efficiënte overheid verwacht die juist meer armslag nodig heeft om burgers waar deze zich ook bevinden, te beschermen tegen gevaren en de risico's. Om de uitdagingen van de iSamenleving het hoofd te bieden is dan ook een gezamenlijke inspanning nodig van overheden, burgers en bedrijfsleven.

• *Regie en verantwoordelijkheid van de overheid voor het eigen handelen*

De WRR wijst er in haar rapport op dat het voor de overheid in de huidige vorm steeds moeilijker wordt om regie te blijven voeren. De feitelijke ontwikkelingen naar een iSamenleving en de toenemende digitale uitwisseling en verwerking van data door de overheid, en tussen burgers onderling, zijn hier debet aan.

Het kabinet deelt deze observatie met de WRR. Uitgangspunt is dat de overheid de regie en verantwoordelijkheid behoudt voor wat betreft het eigen handelen. De eerder genoemde uitdaging – niet het proberen eenzijdig alle dataverkeer te beheersen en controleren, maar het garanderen van de juistheid, zorgvuldigheid en veiligheid van digitale datastromen waarvan de overheid zelf gebruikt maakt, het beheersbaar houden van de bredere gevolgen van digitalisering in de iSamenleving – speelt op alle overheidsniveaus, ook internationaal. Zo hebben gemeenten en uitvoeringsorganisaties op onderdelen autonome bevoegdheden, maar dat neemt niet weg dat de Rijksoverheid het als haar rol ziet om het bewustzijn van de hoedanigheid, een iOverheid te zijn ook op andere overheidsniveaus te promoten wanneer dat nodig mocht blijken. Met betrekking tot de private sector heeft de Rijksoverheid vooral een faciliterende rol. Indien het op dat niveau mis dreigt te gaan, kan met regelgeving worden ingegrepen.

• *Regie van de overheid in de iSamenleving*

Daar waar het gaat om ontwikkelingen buiten het publieke domein is de situatie wezenlijk anders. De overheid is slechts één van de spelers in de iSamenleving, die de Nederlandse grenzen ver te buiten gaat. Processen zoals bijvoorbeeld «cloud computing» en de grensoverschrijdende vernetwerking van gegevens, zijn niet effectief te beheersen met nationale wetgeving en nationaal beleid. Het is in de optiek van het kabinet dan ook onjuist om te denken dat de Nederlandse overheid in staat is om alle risico's die de iSamenleving met zich meebrengt, in de toekomst volledig te beheersen of daarop vooraf controle uit te oefenen. Het inspelen op de iSamenleving vereist een samenspel van nationale, internationale en private initiatieven.

• *Kwetsbaarheden en risico's van de iOverheid en de burger*

De noodzaak tot samenspel vloeit in essentie ook voort uit de analyse van de WRR. Wij, overheid, burgers en bedrijven, zijn gezamenlijk in een iSamenleving beland. Door het almaar toenemende gebruik van digitale verwerking en uitwisseling van (persoons)gegevens op grote schaal komen de verantwoordelijkheid en de kwetsbaarheid van zowel de overheid als van de burger in een ander licht te staan. De privacy en keuzevrijheid van burgers kunnen ernstig in het gedrang komen bij overheidsbesluiten die te eenzijdig zijn genomen vanuit de optiek van efficiëntie en effectiviteit, aldus de WRR. Overheden kunnen volgens de WRR in de iSamenleving op hun beurt kwetsbaar worden omdat de verantwoordelijkheid voor kwaliteit, betrouwbaarheid en beveiliging van informatie niet geheel in overheidshand kan worden gehouden, en de juistheid van de gegevens in hun context daarmee niet altijd meer kan

worden gegarandeerd. Het WRR-rapport plaatst om die risico's nader te duiden, bij drie typen van verwerking van gegevens zogenaamde waarschuwingsvlaggen. Indien informatie door de overheid wordt verrijkt, vernetwerkt of uitgewisseld over organisatiegrenzen heen, of indien informatie wordt gebruikt ten behoeve van proactief of preventief beleid, moet een waarschuwingsvlag worden geplaatst bij het proces van gegevensverwerking. De overheid dient dan zeer alert te zijn omdat de eerder genoemde kwetsbaarheid in die gevallen aanzienlijk wordt vergroot. Het risico bestaat dat informatie «vervuild» raakt, dat onduidelijk is wie verantwoordelijk is voor bepaalde gegevens en raken burgers, bedrijven en overheidsinstanties verstrikt in het gegevensverkeer.

Het kabinet deelt de opvatting van de WRR dat in zulke situaties extra alertheid bij die verwerkingen aangewezen is. Hierna zal in deel II worden uitgewerkt, op welke wijze aan deze alertheid gestalte wordt gegeven in de afwegingskaders en in institutionele arrangementen.

• *Nieuwe conventies in de iSamenleving*

De WRR constateert dat informatie een steeds belangrijker rol speelt in de samenleving; overheid, burgers en bedrijven maken veel en graag gebruik van de mogelijkheden en voordelen die de laagdrempeligheid en schaalvergroting met zich meebrengen. Daarbij treedt geleidelijk ook een andere ontwikkeling op in de omgang met en opvattingen over het gebruik van informatie. Opvattingen over welke informatie met wie gedeeld mag en kan worden veranderen steeds, bijvoorbeeld onder invloed van «sociale media». Technologische mogelijkheden scheppen nieuwe omgangsvormen tussen actoren – de overheid, burgers en bedrijfsleven – in de iSamenleving: soms ontstaan zij direct na het ontstaan van een nieuwe ICT-toepassing, en soms pas na verloop van tijd.

Het kabinet constateert met de WRR dat met de opkomst van de iSamenleving sprake is van een fundamentele en onomkeerbare ontwikkeling. Welke gevolgen daarvan blijvend zullen zijn is nu nog niet te voorzien. Het kabinet wil op een passende manier inspelen op de geschetste ontwikkeling. Het gaat erom te transformeren naar een robuuste iOverheid die geen regie zal voeren in de iSamenleving, maar wel tot taak heeft de bestaande arrangementen te herijken en zonodig aan te passen om kwalijke gevolgen van zich wijzigende informatiemiddelen te beperken. Dat geldt evenzeer voor de mogelijkheden die de burger zelf heeft, zich tegen inbreuken op zijn rechten te beschermen. Omdat informatiestromen zich vaak over landsgrenzen uitstrekken, zullen maatregelen of aanpassingen van het recht ook vaak een internationaal karakter moeten hebben.

• *Tekenen van bewustwording een iOverheid te zijn*

De WRR oordeelt positief over de nieuwe mogelijkheden binnen de iOverheid voor het verbeteren van de dienstverlening aan burgers en bedrijven en de samenwerking binnen de overheid, nationaal en internationaal. Een doorgroeiende iOverheid, die uit betrouwbare bronnen informatie verzamelt en gegevens koppelt en uitwisselt met publieke en private partijen, hoeft geen schrikbeeld te zijn. Een ongecontroleerde, als het ware organisch doorgroeiende iOverheid kan echter wel gevaren met zich meebrengen. Het verbinden van informatie met andere informatie bijvoorbeeld, waardoor de informatie een heel andere functie verkrijgt dan oorspronkelijk bedoeld, mag niet sluipenderwijs plaatsvinden. Opdrachtgevers en gegevensverantwoordelijken binnen de overheid moeten zich van de risico's scherp bewust zijn. Dat geldt temeer voor processen waarin informatie wordt verrijkt, vernetwerkt, of wordt gebruikt

ten behoeve van proactief en preventief beleid – het betreft hier de eerder genoemde waarschuwingsvlaggen van de WRR.

Het kabinet oordeelt met de WRR positief over de nieuwe mogelijkheden voor het verbeteren van de dienstverlening aan burgers en bedrijven, en voor de samenwerking binnen de overheid. In de optiek van het kabinet is het bewustzijn ter zake binnen de iOverheid voor een deel doorgedrongen in de besluitvormingsprocessen. Zo is naar aanleiding van het WRR-rapport een programma gestart (iBelastingdienst) dat aanbevelingen van het WRR-rapport gaat vertalen voor deze dienst en kan bijvoorbeeld worden gewezen op de brief van het kabinet aan de Eerste Kamer over het privacybeleid.¹ Daarin kondigde het kabinet onder meer aan dat voorgenomen maatregelen op informatiegebied nadrukkelijker moeten worden getoetst aan effectiviteit en transparantie. Ook zet de overheid in op het verder versterken van het intern toezicht met behulp van Functionarissen gegevensbescherming. Het kabinet zal het bewustzijn, een iOverheid te zijn, verder verbreden, en de eerder genoemde waarschuwingsvlaggen bij relevante processen binnen de overheid, verankeren. Hierbij dient onderscheid gemaakt te worden tussen het uitwisselen en hergebruiken van openbare overheidsinformatie en niet-openbare overheidsinformatie zoals persoonsgegevens. Dit kabinet streeft naar vrij hergebruik van openbare overheidsinformatie door burgers, bedrijven en overheden zelf om innovatie in de markt en efficiëntie binnen de overheid te stimuleren.² Niet-openbare overheidsinformatie komt niet in aanmerking voor hergebruik door partijen buiten de overheid. Wel kan uitwisseling van dergelijke gegevens binnen de overheid de dienstverlening aan burgers verbeteren door eenmalige verstrekking en meervoudig gebruik. Hierbij dienen de eerder genoemde waarschuwingsvlaggen in acht te worden genomen.

• *Voornemens van dit kabinet*

Het kabinet ziet in deze ontwikkelingen een rol voor zichzelf weggelegd, die in twee aspecten uiteenvalt. Het kabinet zet in op het waar noodzakelijk aanpassen van de eigen overheidsorganisatie om zo goed mogelijk op uitdagingen in te spelen die komen kijken bij gebruik van digitale datastromen door de overheid. Het bewustzijn van de gevolgen van de toegenomen digitalisering en schaalvergroting van gegevensverwerking binnen de overheid zelf zal moeten worden versterkt. Daarnaast zal het kabinet verder gaan met het nemen van maatregelen om binnen het juridische en beleidsmatige instrumentarium duurzaam tot een evenwichtige afweging te komen van legitieme belangen bij besluitvorming over grootschalige dataverwerking door de overheid. Daarbij is het van belang te bedenken dat ieder onderdeel van de overheid verantwoordelijk is voor het eigen beleid. Het kabinet zal zich inspannen om deze met de transformatie naar een iSamenleving noodzakelijk geworden overheidsmaatregelen tevens in internationaal en Europees verband aan te kaarten. Het kabinet zal maatregelen nemen om burgers zo goed mogelijk toe te rusten tegen problemen die voortvloeien uit verwerking van hun persoonsgegevens in digitale datastromen in de publieke sector, opdat deze daadwerkelijk en effectief voor zichzelf kunnen opkomen. De weerbaarheid van burgers zal worden vergroot door versteviging van het inzage- en correctierecht. Mede hierdoor zal ook het bewustzijn van burgers, dat zij deel uitmaken en medeverantwoordelijk zijn voor de iSamenleving, worden vergroot.

• *Verdere bewustwording van het zijn van een iOverheid*

Het vraagstuk dat aan de orde is in de iSamenleving wordt naar de mening van het kabinet niet opgelost met het instellen van nieuwe

¹ Brief van het kabinet aan de Eerste Kamer van 29 april 2011 inzake het privacybeleid.

² Brief van het kabinet aan de Tweede Kamer van 30 mei 2011 inzake *Hergebruik en Open Data: naar betere vindbaarheid en herbruikbaarheid van overheidsinformatie*.

instituties op nationaal noch op internationaal niveau. Een gevaar bij het instellen van dergelijke instituties is bovendien dat het mogelijk suggereert dat het kabinet overheidssturing en regie heeft geregeld, en dat daarmee het vraagstuk is afgedaan. Het kabinet ziet daarentegen een meerwaarde in het verankeren van een innerlijke bewustwording van de verantwoordelijkheden die bij een iOverheid horen binnen de bestaande overheidsstructuren. Het antwoord op de iSamenleving ligt, voor zover het gaat om dat deel van de iSamenleving waarop de overheid nu geen sturing heeft, niet in het streven naar volledige regie door de overheid, maar in het verbeteren van het besluitvormingskader en de besluitvormingsstructuur en het mondiger maken van de burger in de iSamenleving. In het tweede deel wordt uiteengezet op welke wijze het kabinet hierbij gebruik zal maken van de inhoudelijke en procesmatige aanbevelingen van de WRR (Onderdeel I). Vervolgens wordt ingegaan op de WRR-aanbevelingen die betrekking hebben op de opzet en uitvoeringspraktijk van de iOverheid (Onderdeel II).

Deel II

Acties gericht op het realiseren van de visie binnen de Rijksoverheid

1. Concrete maatregelen op het inhoudelijke vlak

- *Het cluster van stuwende, verankerende en procesmatige beginselen*

Volgens de WRR is de afweging tussen beginselen enerzijds privacy en keuzevrijheid en anderzijds de beleidsdoelen die de overheid met een bepaald beleidsdoel nastreeft, in de praktijk een minder evenwichtige en openbare aangelegenheid dan de theorie doet vermoeden. De uitkomsten van de afzonderlijke afwegingen zelf zijn volgens de WRR niet altijd evenwichtig. De belangen en beginselen die een rol spelen bij het bewerken van gegevens, worden bij de afweging in concrete situaties zelden expliciet gemaakt en zijn bovendien ongelijksoortig, zo stelt de WRR vast. Ook valt er volgens de WRR in sommige omstandigheden politiek en bestuurlijk veel te winnen bij een onevenwichtige voorstelling van zaken.¹ De huidige toetsing resulteert hierdoor vaak in een disbalans tussen de verschillende betrokken beginselen zoals gegevensbescherming, veiligheid, verantwoordelijkheid, efficiency en transparantie. De WRR beveelt in dit verband het gebruik van drie clusters van beginselen aan, te weten die van de stuwende, de verankerende en procesmatige beginselen, met het oog op herstel van de balans tussen alle beginselen die in de afweging bij gegevensverwerking zouden moeten worden meegenomen.² Onder stuwende beginselen verstaat de WRR veiligheid, effectiviteit en efficiëntie. De verankerende beginselen omvatten privacy en keuzevrijheid. De procesmatige beginselen zien tot slot op het waarborgen van accountability en transparantie. In de transformatie van de eOverheid naar de iOverheid wordt in de besluitvorming volgens de WRR vaak eenzijdig gestuurd door de stuwende beginselen. De andere beginselen raken hierdoor in de verdrukking. De clusters van beginselen moeten op alle niveaus van besluitvorming meer met elkaar in evenwicht worden gebracht, aldus de WRR.³ Behoedzaamheid is vooral geboden wanneer besluitvorming plaatsvindt waarin vernetwerking van informatie, het samenstellen en verrijken van informatie of het voeren van preventief beleid op basis van informatie aan de orde is – of in termen van de WRR de waarschuwingsvlaggen aan de orde zijn.

¹ WRR-rapport, p. 210.

² Voor nadere uitwerking zie WRR-rapport, p. 73 e.v.

³ WRR-rapport, p. 15.

• *Huidig kader voor afweging bij besluitvorming*

Met de WRR constateert het kabinet dat door het karakter en de intensiteit van digitalisering van de samenleving een duurzame versteviging van het huidige afwegingskader voor de toekomst gewenst is waar het gaat om gegevensverwerking door de overheid zelf. Aan de basis van het afwegingskader zelf zijn volgens het kabinet geen veranderingen noodzakelijk. De aanbeveling van de WRR die ziet op het hanteren van de clusters van beginselen is voor het kabinet een belangrijke aanleiding om te bezien of het tot nu toe gehanteerde kader in de praktijk voldoet. Het huidige afwegingskader voor een voorgenomen gegevensverwerking is neergelegd in de Wet bescherming persoonsgegevens (Wbp), en meer algemeen in het grondrechtelijke kader in artikel 10 Grondwet, artikel 8 EU-Handvest, artikel 8 EVRM, art. 17 IVBPR en EG-Richtlijn 95/46/EG.¹ Deze artikelen strekken tot bescherming van de persoonlijke levenssfeer en liggen ten grondslag aan Wbp. Veiligheid, effectiviteit en efficiency zijn vaste onderwerpen in het afwegingsproces en onderdeel van de proportionaliteitstoets. De vereisten van transparantie en accountability vinden hun weerslag onder meer in het vereiste dat een wet kenbaar en voorzienbaar moet zijn zoals is vastgelegd in artikel 8 lid 2 EVRM. Veiligheid is één van de legitieme doelstellingen uit artikel 8 lid 2 EVRM ten behoeve waarvan de overheid maatregelen kan treffen. De WRR reikt met het oog op de vigerende wetgeving volgens het kabinet geen nieuw normenkader aan. De voorgestelde clusters met beginselen in het WRR-rapport hebben reeds een zelfstandig bestaan of worden geabsorbeerd in de concrete afweging met betrekking tot de vereisten van proportionaliteit en subsidiariteit van voorgenomen maatregelen.

• *Verduurzaming en zichtbaarheid van het kader en de te wegen beginselen*

Het huidige afwegingskader is evenwel niet vrijblijvend en is grotendeels gebaseerd op de Grondwet, het EVRM en de EU-regelgeving. Om die reden kan het bestaande afwegingskader niet zomaar worden herzien. Het kabinet streeft een optimale balans na tussen de in het geding zijnde beginselen binnen de marges die deze bepalingen bieden. Van belang bij het zoeken naar de optimale balans tussen de beginselen is dat in het concrete geval het juiste gewicht wordt toegekend aan de stuwende, verankerende en procesmatige beginselen. Het kabinet is om die reden van oordeel, dat het bestaande afwegingskader niet zozeer zou moeten worden aangevuld met, of getransformeerd in een geheel nieuw afwegingskader. De oplossing zoekt het kabinet veeleer in een versteviging en waar nodig herijking van het soortelijk gewicht van de af te wegen beginselen bij concrete afwegingen.

• *Versterking van inzage- en correctierechten en uitwerking van de rol van de Fg*

Volgens de WRR is aanpassing van de wetgeving die ziet op het inzage- en correctierecht niet noodzakelijk, maar aanpassing van bestaande institutionele structuren heeft wel een meerwaarde.

Met het oog op het voornemen de burgers toe te rusten met effectieve bescherming, wordt hieronder uitgewerkt met welke toegezegde maatregelen en vervolgens met welke nog te nemen maatregelen deze doelstelling wordt nagestreefd. Door het vergroten van de mogelijkheden van burgers om hun gegevens te controleren en te laten corrigeren kan een «countervailing power» op gang worden gebracht, een tegenkracht waarvan een preventieve werking richting gegevensbeheerders, -eigenaren en opdrachtgevers bij de overheid zal uitgaan. Zij worden dan

¹ Richtlijn 95/46/EG van het Europese Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

immers meer gedwongen de gegevensverwerking intern goed op orde te hebben. Er gaat een zelfreinigende werking uit van deze vorm van transparantie, zo verwacht het kabinet. Het kabinet wil hiervoor de bestaande inzage- en correctierechten verstevigen.

Het kabinet kiest er in lijn met de WRR voor om de bestaande structuren die zien op de uitvoering van het inzage- en correctierecht, alsmede verwerkelijking van het wissen van persoonsgegevens aan te passen. Nadere uitwerking van deze aanpassing wordt uiteengezet in onderdeel 2 onder «Effectieve instrumenten voor de burger». Met beide maatregelen, bestending van het gewicht van de beginselen en het bieden van effectieve inzage- en correctierechten, verwacht het kabinet dat er een verschuiving zal optreden in de «checks and balances» in de besluitvorming die ziet op gegevensverwerking en dat dit bijdraagt aan een optimale belangenafweging door de iOverheid.

Het beleid van het kabinet inzake bescherming van persoonsgegevens is ook gericht op het stimuleren van het gebruik van intern toezicht met behulp van Functionarissen gegevensbescherming (Fg). Dat is eveneens een maatregel die de proportionaliteit en subsidiariteit van de gegevensverwerking binnen de overheid ten goede komt. Onderzocht wordt hoe deze taak binnen de overheid verder kan worden versterkt.¹

• *Voorgenomen maatregelen*

In zijn brief aan de Eerste Kamer en de Tweede Kamer over het privacybeleid en gegevensverwerking kondigde het kabinet onlangs al een aantal voornemens aan die direct of indirect leiden tot een versterking van de beginselen in het hiervoor genoemde afwegingskader.² Zo zal de verantwoordelijke voor gegevensverwerking de bewaartermijn alsook het gebruik van de gegevens na afloop van de verwerking, bekend moeten maken. Er komt een afzonderlijke regeling met specifieke transparantieverplichtingen bij het toepassen van profileringen, met inbegrip van de explicitering van het doel van de verwerking. Met deze ingrepen wordt nadrukkelijk het beginsel van de transparantieplichting gediend. De zichtbaarheid van de afweging maakt ook de ijking van de beginselen die in het geding zijn, meer inzichtelijk. Daarnaast kondigde het kabinet in de brief aan dat voortaan een nadrukkelijker toetsing van voorgenomen maatregelen op informatiegebied aan effectiviteit en transparantie dient plaats te vinden. Bovendien moet steeds worden overwogen of evaluatie- of horizonbepalingen bij een maatregel moeten worden opgenomen.

De brief kondigde onderzoek aan naar de mogelijkheden van het gebruik van privacy-effectbeoordeling (Privacy Impact Assessments) bij een voorgenomen gegevensverwerking. Een dergelijke privacy-effectbeoordeling dient in te gaan op de mate waarin de privacy door de voorgenomen gegevensverwerking wordt of kan worden geraakt zodat maatregelen kunnen worden genomen om, waar mogelijk en gewenst, die effecten te mitigeren. Daarbij dient rekening te worden gehouden met de samenhang met al bestaande digitale systemen. Bovendien dient koppeling met andere gegevensbestanden eerst plaats te vinden als de eerste database voldoende kwaliteit heeft. Wat de privacy-effectbeoordelingen betreft, verkeert het kabinet nog in een onderzoekende fase. In het kader van enkele in voorbereiding zijnde wetsvoorstellen³ wordt dit najaar een privacy-effectbeoordeling uitgevoerd.

Alle genoemde maatregelen, zo verwacht het kabinet, komen de proportionaliteit en de subsidiariteit van de voorgenomen gegevensverwerking ten goede. In de besluitvorming moet immers expliciet aandacht worden

¹ Uit de evaluatierapporten van de Wbp blijkt dat wanneer een Functionaris gegevensbescherming is aangesteld, dit een belangrijk positief effect heeft op de kwaliteit van de gegevensbescherming binnen de desbetreffende organisatie. (Kamerstukken II, 2009–2010, 31 051, nr. 5, p. 29).

² Brief van 29 april 2011 van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Veiligheid en Justitie aan EK en TK inzake het privacybeleid.

³ Wetsvoorstel inzake de uitbreiding van het gebruik van biometrische kenmerken in de vreemdelingenketen, het conceptwetsvoorstel vastleggen en bewaren van kentekengegevens door de politie (ANPR) en wetgeving inzake het gebruik van passagiersgegevens in het kader van geïntegreerd grensbeheer (Pardex).

besteed aan de toekenning van het gewicht aan het beginsel bij een concrete maatregel. Met deze maatregelen komt het kabinet eveneens tegemoet aan de motie Franken¹ waarin wordt opgeroepen tot toetsing van wetsvoorstellen aan noodzaak, effectiviteit en hanteerbaarheid, alsmede aan proportionaliteit. Daarnaast roept de motie op tot het opnemen van horizon- en evaluatiebepalingen in de regelgeving ter zake, waaraan met bovenstaande gehoor is gegeven. Het kabinet zegt toe dat de strekking van motie-Franken zal worden opgenomen in het Integraal Afwegingskader voor beleid en regelgeving (IAK), en het zal deze ook als vaste toetssteen hanteren in de wetgevingskwaliteitstoets van voorstellen voor wetten en algemene maatregelen van bestuur. Ook dit voornemen dwingt tot een herijking van het soortelijk gewicht van de beginselen bij voorgenomen maatregelen. Voor wat betreft het Europees en internationaal perspectief zegt het kabinet toe dat Nederland zich in Europees en internationaal verband in zal zetten voor een grotere alertheid met betrekking tot de implicaties van de inzet van digitale systemen.

2. Concrete maatregelen op het institutionele en operationele vlak

• *Bewustwording bij overheden en bestuurders operationaliseren en verbeteren*

Het besef een iOverheid te zijn, is geen rustig bezit, maar een permanente opgave, aldus de WRR. De rijksoverheid dient zich daar in ieder geval als eerste van bewust te zijn en ernaar te handelen. Op alle niveaus in de besluitvorming worden nu al beleidsdoelen meegewogen met privacy- en informatiebeleidsbeginselen. Het maken van dit soort van afwegingen is voor de betreffende verantwoordelijke bestuurder of uitvoerder als zodanig niet nieuw. Maar de afweging tussen die beginselen zal bewuster, meer geëxpliciteerd en transparanter moeten plaatsvinden. Bovendien moeten bepaalde soorten van informatieverwerking meer aandacht krijgen, omdat ze in het bijzonder riskant zijn voor de kwaliteit en betrouwbaarheid van gegevens; namelijk als er sprake is van het «vernetwerken», het verrijken of het voeren van proactief beleid op basis van informatie. Die soorten verwerking moeten een «waarschuingsvlag» krijgen in de bestaande toetsingskaders.

Het kabinet deelt de suggestie van de WRR dat het bewustzijn een iOverheid te zijn, verder kan worden versterkt. De beoogde bewustwording van verantwoordelijken binnen de overheid vraagt in de optiek van het kabinet allereerst om het opnemen van de bovengenoemde nieuwe afwegingen in bestaande procedures bij de rijksoverheid. Het gaat daarbij om bestaande verantwoordelijkheden en toetsingsrollen die bij alle departementen aanwezig zijn; ten eerste bij juristen, die beleid toetsen aan het IAK, ten tweede bij Chief Information Officers (CIO's), die op strategisch niveau ICT-projecten beoordelen, en ten derde bij de Fg's die toezien op toepassing en naleving van de Wbp. Het kabinet wil meer samenhang aanbrengen in bestaande beheermaatregelen en tussen de (verplichte) oordelen van juristen, CIO's en Fg's.

In de Bestuurlijke Regiegroep Dienstverlening en e-Overheid, waarin alle overheden en grote uitvoeringsorganisaties vertegenwoordigd zijn, is afgesproken de bevindingen en aanbevelingen van de WRR op de agenda te houden en zo de bewustwording ook bij andere overheden te vergroten. Dit zal onder meer plaatsvinden door het uitwisselen van ervaringen over de toepassing van de maatregelen binnen NUP-verband en in de Programmaraad e-Overheid voor Burgers. Door deze programmaraad is inmiddels een onderzoek gestart naar de concretisering van de visie op dienstverlening en de voortgang van de realisatie hiervan. De

¹ Motie Franken, Eerste Kamer 2010–11, 31 051, D.

analyse van de WRR en dit kabinetsstandpunt worden hierbij uitdrukkelijk meegenomen. De onderzoeksresultaten worden begin 2012 opgeleverd.

De eigenlijke opdracht die de WRR meegeeft – het op alle lagen en in alle geledingen van overheid en uitvoeringsorganisaties alert houden van bestuurders en betrouwbaar houden van gegevens – strekt zich echter tot ver na 2012 uit. Vertegenwoordigers van uitvoeringsorganisaties hebben aangegeven de komende maanden met BZK en VNG te willen verkennen op welke wijze praktische invulling kan worden gegeven aan de belangen van burgers bij onder meer hergebruik en verrijking van informatie uit verschillende bronnen.

• *Nieuwe instituties: iCommissie, iPlatform en iAutoriteit*

De WRR adviseert een permanente commissie voor de iOverheid in te stellen, die jaarlijks aan de Eerste en Tweede Kamer zou moeten rapporteren. De commissie zou zich bezig moeten houden met het signaleren van ontwikkelingen en met het bezien ervan vanuit het perspectief van de iOverheid. Het secretariaat van de commissie zou bij de CIO-Rijk moeten worden belegd. Deze aanbeveling van de WRR is vooral functioneel van aard; het is geen doel in zichzelf om een nieuw instituut op te richten. De WRR onderstreept dat het van belang is dat de overheid zich realiseert dat nu het ogenblik aangebroken is om maatregelen te nemen om de koers van de iOverheid te verleggen.

Het vraagstuk dat aan de orde is in de iSamenleving wordt zoals eerder betoogd, niet opgelost met het instellen van nieuwe instituties. Het kabinet ziet daarentegen een meerwaarde in het verankeren van een innerlijke bewustwording van de verantwoordelijkheden die bij een iOverheid horen binnen de bestaande overheidstructuren. Het kabinet onderschrijft het door de WRR gesignaleerde momentum en wil dat vasthouden, en kiest met het oog op effectiviteit voor het waarborgen van een ontwikkeling van de iOverheid door de verbetering van de integrale verantwoordelijkheid en bewustwording van alle bestuurslagen en overheden zelf. De overheid moet aldus zelf vanuit het door de WRR geschetste perspectief gaan handelen. Het gaat veeleer om het streven naar een zichtbare en effectieve transformatie binnen de bestaande instituties en om het besef een iOverheid te zijn, dan om instituties die dat van buitenaf zouden moeten bewerkstelligen.

Ook stelt de WRR voor, een iAutoriteit en een iPlatform in te richten. Het kabinet omarmt de gedachte, dat er een virtuele plaats voor de burger moet zijn waar zijn door de overheid verwerkte gegevens terug te vinden zijn. Daarmee wordt niet alleen het belang van de burger bij de mogelijkheid tot beheer en correctie gediend, maar ook het belang van de overheid bij het op orde houden van het eigen gegevensbeheer. Het kabinet wenst hieraan uitwerking te geven door het onlangs ingerichte «www.MijnOverheid.nl» verder te ontwikkelen. Met de andere overheden is in het NUP afgesproken dat de rijksoverheid en medeoverheden zodanig gaan samenwerken bij hun dienstverlening dat zij door burgers als één overheid worden waargenomen. Deze gemeenschappelijke visie heeft nadrukkelijk ook betrekking op de zogenaamde front-office van de e-overheid voor burgers, waar MijnOverheid.nl onderdeel van uitmaakt.

• *Effectieve instrumenten voor de burger: versteviging van het inzage- en correctierecht*

Door het groeiend gebruik van internet en sociale media wennen burgers er steeds meer aan dat zij niet alleen afnemers, maar ook producenten en beheerders van informatie zijn. Het kabinet wil van die ontwikkeling

gebruik maken. Het past bij een compacte overheid om burgers te faciliteren en te stimuleren zelf ook bij te dragen aan het op orde hebben en houden van de eigen gegevens. Daarmee wordt invulling gegeven aan het inzage- en correctierecht dat burgers volgens de Wbp hebben. De WRR bepleit dit verder faciliteren van het inzagerecht door burgers voor de eigen gegevens en verwijst daarbij naar Mijnoverheid.nl. Uitbreiding van de mogelijkheden van burgers kan alleen als de overheid tegelijkertijd de kwaliteit van gegevens en informatie waarborgt en veilige toegang biedt. Als gevolg van de door het kabinet in de brief over het privacy-beleid en gegevensverwerking aangekondigde maatregelen moeten opdrachtgevers en gegevensbeheerders bij de rijksoverheid en uitvoeringsorganisaties meer gegevens gaan expliciteren en bekend maken. In de motie Tan¹ werd het kabinet bovendien opgeroepen, het correctie- en inzagerecht van de burger ten opzichte van de overheid te versterken, en te komen tot een wet inzake identiteitsmanagement.²

Het kabinet wenst burgers inderdaad meer mogelijkheden te bieden voor inzage- en correctierecht op de gegevens die de overheid over hen heeft. In de hieronder geschetste nieuwe beleidslijn trekt het kabinet deze transparantie door naar het op een geleidelijke en beheersbare wijze delen van gegevens met degene die het aangaat. Dit versterkt de aanspreekbaarheid («accountability») van diegenen die voor de informatiehuishouding verantwoordelijk zijn. Het kabinet verwacht bovendien dat hiervan een preventieve werking uitgaat op het zuiver en betrouwbaar houden van gegevens en informatie door (overheids)organisaties. Uiteraard blijven gegevens waarop het inzage- en correctierecht niet van toepassing is, zoals in toezichtsprocessen of opsporingsdossiers in lopende opsporingsonderzoeken, hierbij buiten beschouwing. Door middel van nader onderzoek zal verkend worden op welke wijze de informatiepositie van de burger verder kan worden versterkt door verdere uitbreiding van de functionaliteit van MijnOverheid, onder meer met:

- inzage in de gegevens die de overheid over de burger heeft;
- inzage in het gegevensverkeer tussen overheidsorganisaties (welke gegevens over mij worden tussen welke organisaties uitgewisseld);
- een mogelijkheid tot verzoeken om correctie van onjuiste gegevens;
- een mogelijkheid om eigen gegevens op eigen verzoek actief te delen met derde partijen.

De beoogde doelstelling en werking van deze nieuwe functionaliteiten wordt hieronder verder toegelicht.

De implicaties van deze nieuwe functionaliteiten kunnen omvangrijk zijn, en zowel organisatorisch, technisch, juridisch, als financieel van aard. In de verkenning zal eveneens worden nagegaan of, en zo ja, op welke wijze, overheidsorganisaties verplicht kunnen worden om via MijnOverheid een of meer van de hierboven genoemde mogelijke functionaliteiten aan te bieden. De verkenning, af te ronden medio 2012, dient meer inzicht te geven in zowel de mogelijkheden als de implicaties van een dergelijke aanpak.

• Inzage in de eigen gegevens en het gebruik hiervan door overheidsorganisaties

Door voor de burger op elektronische wijze inzichtelijk te maken welke overheidsorganisaties van welke gegevens over deze burger gebruik maken, met welke andere organisaties zij deze gegevens delen, en welke wettelijke grondslag voor de deling bestaat, krijgen burgers de beschikking over informatie die hen in staat stelt zelf meer regie te voeren op en toezicht te houden op de gegevensuitwisseling met en door de overheid.³ Wanneer organisaties eigen gegevens en gegevens van andere organisaties combineren in een elektronisch dossier, zou dit elektronisch

¹ Motie Tan, Eerste Kamer 2010, 31 051, C.

² Het Rathenau Instituut beveelt in zijn rapport aan, de positie van de burger te verstevigen door de burger bijvoorbeeld de regie over de eigen gegevens te geven. Hiertoe dienen volgens het Rathenau het inzage- en correctierecht te worden verbeterd (Rathenau 2010, p. 11).

³ Dit sluit aan bij het EU-actieplan *E-Overheid 2011–2015. Benutten van de ICT om een slimme, duurzame en innovatieve overheid te bevorderen*, zoals aangekondigd in de Mededeling van de Europese Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's van 15 december 2010, p. 9.

dossier inclusief de herkomst van de van andere organisatie verkregen gegevens op elektronische wijze zichtbaar moeten zijn voor de betreffende burger. Als organisaties proactief handelen voor dienstverlening, zorg of handhaving, mede op basis van gegevens die van andere organisaties zijn verkregen, dan maken zij in hun besluit de herkomst van deze gegevens van derden zichtbaar.

Een eventuele verplichting voor overheidsorganisaties om bovenstaande inzagemogelijkheden te realiseren via MijnOverheid.nl, zal worden verkend.

• *Vergeten worden*

Voor allerlei gegevens bestaan al bepalingen over bewaartermijnen, maar deze worden niet altijd in acht genomen. Het is het voornemen van het kabinet dat bij het zichtbaar maken van de eigen gegevens geleidelijk eveneens zichtbaar gemaakt wordt wanneer de betreffende gegevens zullen worden gewist. Daarmee wordt de burger beter geëquipeerd om te controleren of het «recht op vergeten worden» wel wordt nageleefd en kan hij zich, indien dit niet het geval is, tot de langbewaarder wenden met een verzoek tot het verwijderen van de desbetreffende gegevens.

• *Verzoeken om correctie*

Met het zichtbaar maken van de herkomst van gegevens (zoals hierboven beschreven) is het voor burgers al een stuk eenvoudiger om de bron van eventuele onjuiste gegevens te vinden en zich tot deze bron te wenden met een verzoek om correctie. Verkend zal worden of, náást de mogelijkheid tot het indienen van correctieverzoeken direct bij de gegevenshouder, een uitbreiding van MijnOverheid met een correctievoorziening wenselijk, mogelijk en haalbaar is. Mochten er voor een bepaald gegeven meerdere bronnen zijn die inhoudelijk tot een verschillende conclusie over dat gegeven komen, en de burger met de verschillende gegevenshouders niet tot een bevredigende oplossing hiervan komt, dan is een vorm van geschilregulering noodzakelijk.¹ In principe staan de bestaande procedures via de Nationale ombudsman en de rechterlijke macht hiervoor al open en kan van een geschillenbeslechtingregeling ex art. 47 Wbp gebruik worden gemaakt. Omdat noch de aard noch de omvang van deze problematiek bekend zijn, is de inrichting van een formele procedure of nieuwe institutie vooralsnog niet aan de orde. Het kabinet wil voor dergelijke gevallen, naast de genoemde procedures, het digitale loket en de bestaande procedures van het Centraal Meldpunt Identiteitsfraude en Fouten (CMI) bij het Ministerie van BZK benutten. Aan de hand van de ervaringen die het komende jaar hiermee worden opgedaan zal worden bezien of hiermee afdoende mogelijkheid wordt geboden of dat aanvullende maatregelen noodzakelijk zijn.

• *Regie over de eigen gegevens*

Naast het gebruik van gegevens door de overheid zelf kan het voor burgers, bedrijven en instellingen van belang zijn om de door de overheid vastgelegde en gebruikte gegevens te delen met derden. Voorbeelden hiervan zijn het uittreksel uit het GBA om de juistheid van bepaalde persoonsgegevens aan te tonen of de beschikking van de Belastingdienst op de inkomstenbelasting om de hoogte van het eigen inkomen aan te tonen. In de visie op dienstverlening is afgesproken de keuzemogelijkheid te gaan bieden aan burgers, bedrijven en instellingen dergelijke gegevens digitaal aan derden ter beschikking te stellen. De operationalisering van dit principe is onderdeel van het eerder genoemde onderzoek naar de

¹ Het gebruik van basisregistraties draagt bij aan het voorkomen van dit probleem doordat basisregistraties de enige bron vormen voor de betreffende gegevens.

concretisering van de visie op dienstverlening. Hierin zal verkend worden of de regie van burgers op de eigen gegevens kan worden versterkt door het burgers mogelijk te maken om door de overheid vastgelegde en gebruikte gegevens te delen met derden via een functionaaliteit in MijnOverheid.nl.

• *MijnOverheid.nl als kanaal*

De versterking van inzage, correctiemogelijkheden en regie voor burgers kan plaatsvinden via de eigen websites van overheidsorganisaties, maar kan ook via MijnOverheid.nl. Het gebruik van MijnOverheid.nl verdient de voorkeur met het oog op de verdere ontwikkeling van de daartoe benodigde ICT-functionaliteiten (MijnOverheid.nl en Digimelding) bij de rijksbrede beheerorganisatie Logius. Bovendien is in het kader van het NUP afgesproken dat rijk en medeoverheden samen werken aan die gemeenschappelijke overheidsbrede, toekomstbestendige informatie-infrastructuur waar MijnOverheid.nl onderdeel van uitmaakt.

Uitgangspunt van de overheidsbrede visie op dienstverlening is dat burgers, bedrijven en instellingen online inzicht hebben in de gegevens die de overheid van hen heeft en de mogelijkheid hebben een verzoek te doen om deze gegevens te laten wijzigen als ze onjuist zijn. In de verkenning zal derhalve tevens worden nagegaan of en zo ja, hoe overheidsorganisaties kunnen worden verplicht om genoemde functionaliteiten via MijnOverheid.nl te bieden.

• *Het opdrachtgeverschap van de (rijks)overheid*

De WRR oordeelt dat de rijksoverheid als opdrachtgever verantwoordelijk is voor het verbeteren van een weloverwogen aansluiting tussen beleid, uitvoering, technologie, informatiestromen en netwerken. De WRR bepleit professionalisering van opdrachtgevers in dit opzicht.

Sinds 2008 neemt het kabinet al maatregelen om de beheersing van grote, kwetsbare projecten te verbeteren, opdat er minder sprake zal zijn van overschrijdingen in kosten en tijd.¹ Hiertoe hebben de departementale CIO's al taken, bevoegdheden, verantwoordelijkheden en instrumentarium gekregen, dat hen in staat stelt om een sterkere, eigenstandige rol te kunnen spelen in het sturen en beheersen van dergelijke projecten. Daarnaast betreft de beheersing het selecteren en beheren van de juiste projecten via projectportfoliomanagement, het uitvoeren van tussentijdse reviews en het rapporteren over de projecten aan de Tweede Kamer, en het zorgen voor professionalisering van het opdrachtgeverschap.

De bestaande maatregelen hebben betrekking op het beperken van de risico's van ICT-projecten – in kosten en tijd – en (nog) niet op de door de WRR geschetste risico's in de informatie- en gegevenshuishouding. Door in het kader van goed projectportfoliomanagement ook deze aspecten op te nemen in de projectplannen worden op strategisch niveau alle risico's meegewogen. Op deze manier wordt ook een bijdrage geleverd aan de gewenste bewustwording van bestuurders die als opdrachtgevers in eerste instantie misschien vooral oog zullen hebben voor de beleidsdoelen van het informatiesysteem. De CIO's kunnen ook op dit punt hun rol breed invullen; niet alleen sturing en beheersing, maar ook advisering aan opdrachtgevers en de ambtelijke en politieke top.

Concreet betekent dit dat de eisen zoals die nu gelden ten aanzien van de inhoud van projectplannen voor grote ICT-projecten worden aangevuld met de eis om in het projectplan informatie op te nemen over de vraag of er bij het project sprake is van het opnemen van privacygevoelige gegevens of van het koppelen of verrijken van data. Daarnaast zal in het

¹ Brief aan de Tweede Kamer van 3 februari 2011 (TK 26 643, nr. 172)

projectplan beargumenteerd worden aangegeven of voor het project een Privacy-effectbeoordeling of een andere externe kwaliteitstoets gewenst is. Deze informatie wordt betrokken bij de verplichte bepaling van het risicoprofiel van projecten. Als dit resulteert in een hoger risicoprofiel is dat van invloed op een mogelijke rapportage aan de Tweede Kamer.

De CIO betreft, zoals gebruikelijk, alle informatie vanuit het projectplan bij het oordeel dat hij geeft bij de start van een project, of tussentijds bij de uitvoering. Wanneer dit oordeel betrekking heeft op het opnemen van privacygevoelige gegevens of van verrijkte of gekoppelde data, laat de departementale CIO zich bij het opstellen van dit oordeel adviseren door de functionaris gegevensbescherming, die bij elk ministerie is aangesteld en die toezicht houdt op toepassing en naleving van de Wbp. De opdrachtgevers van ICT-projecten zijn gehouden om wijzigingen in een systeem ten aanzien van het gebruik van privacygevoelige gegevens en koppelingen of verrijking daarvan te melden aan de departementale CIO. Deze kan op basis daarvan besluiten of een nieuw oordeel noodzakelijk is. Omdat de hier geformuleerde maatregelen zoveel mogelijk aansluiten bij al bestaande processen kan de hieruit voortvloeiende verhoging van de bestuurlijke last zo beperkt mogelijk gehouden worden.

• *Conclusies*

De overheid heeft een cruciale rol in de iSamenleving waar te maken als het gaat om het beschermen van de burger tegen de gevaren die de iSamenleving met zich meebrengt. Het is daarnaast noodzakelijk dat de overheid ervan doordrongen raakt, een iOverheid te zijn en de daarbij passende verantwoordelijkheid neemt voor de door de overheid tot stand gebrachte gegevensverwerking en informatisering. De eigen huishouding dient op orde te zijn en daartoe wordt onderzocht, welke prikkels en initiatieven hiertoe het meest passend zijn. Omdat de overheid niet op voorhand alle bedreigingen van de iSamenleving kan wegnemen, kiest het kabinet ervoor de burger zo goed mogelijk toe te rusten tegen de mogelijk schadelijke gevolgen die de iSamenleving met zich kan meebrengen. Inzage- en correctierechten dienen in dit verband te worden verstevigd. Het kabinet zet hiermee eveneens in op de eigen verantwoordelijkheid van de burgers. Zij merken in het dagelijks gebruik immers snel op waar de weeffouten in het systeem zitten. Het bewustzijn van de ingrijpendheid van de voortdurende dynamiek van de ICT bij hen die werken met en beslissen over het inrichten van ICT-systemen zal worden vergroot. Om die reden is een bewuste en transparante toepassing van het afwegingskader voor gegevensbescherming in de besluitvorming binnen de overheid voorwerp van voortdurende aandacht. Bij de transformatie naar een iOverheid past het inzicht dat de regie niet in zijn geheel kan worden gewonnen, maar dat op cruciale aanknopingspunten – daar waar de burger last ervaart – wel zoveel mogelijk effectief kan worden bijgestuurd.