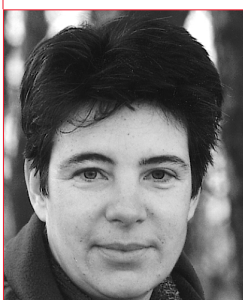


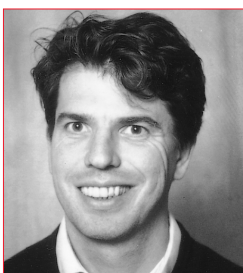
Prof. mr J.E.J. Prins, mr M. de Vries

Een andere overheid vraagt om een andere aanpak van de identificatie-infrastructuur



Corien Prins is redacteur van dit blad en als hoogleraar verbonden aan het Centrum voor Recht, Bestuur en Informatisering, Universiteit van Tilburg.

Sluipend maar gestaag wordt in Den Haag gewerkt aan de uitbouw van een identificatie-infrastructuur. De uiteindelijke consequentie van deze ontwikkeling kan zijn dat de overheid de beschikking krijgt – of denkt te hebben – over een compleet beeld van het doen en laten van haar burgers. Het op eigen initiatief aanvragen van voorzieningen hoeft niet meer. Bezwaar aantekenen heeft weinig zin. De overheid beschikt immers over alle informatie. Hieronder wordt een aanzet gegeven tot een fundamenteel en open debat.



Marc de Vries werkt als senior onderzoeker bij het Centrum voor Recht, Bestuur en Informatisering, Universiteit van Tilburg en is tevens partner bij ZENC BV.

* Deze bijdrage is deels gebaseerd op een rapport dat de auteurs schreven in opdracht van het Rathenau Instituut (*ID or not to be? Naar een doordacht stelsel voor digitale identificatie*, Rathenau Instituut, april 2003 beschikbaar in pdf via <http://www.rathenau.nl/nl/index4.html?publicaties/>>). De auteurs danken Margot Schoenmaker (Rathenau Instituut) voor haar inbreng.

Eind 2003 verscheen de kabinetsnota 'Een andere overheid'.¹ In samenhang met het daarbij gevoegde actieprogramma heeft de nota onder meer tot doel een publiek debat te entameren over de nieuwe rol van de overheid in relatie tot burgers en hun organisaties. Een van de thema's in het actieprogramma is het verbeteren van de dienstverlening aan burgers, waarbij de nadruk sterk ligt op stroomlijning van gegevensbestanden en overheidsbrede identificatie- en authenticatievoorzieningen. Binnen de kaders van het publieke debat over de rol van de overheid is het van groot belang dat er een fundamentele en geïntegreerde discussie over de toekomst van de identificatie-infrastructuur plaatsvindt. Kijkend naar de reeds ontplooiden initiatieven op dit gebied lijkt het kabinet zich namelijk onvoldoende te realiseren dat het bezig is met een belangrijke infrastructurele operatie die onze samenleving in vele opzichten kwetsbaar lijkt te maken. Als het kabinet waarlijk serieus werk wil maken van het moderniseren van de overheid en zijn ambities op tal van beleidsterreinen wenst waar te maken, moeten er wezenlijke keuzes worden gemaakt bij het scheppen van onze identificatie-infrastructuur.

I. Identificatie: wondermiddel voor beleidsambities?

Sluipend maar gestaag wordt in Den Haag gewerkt aan de uitbouw van een identificatiecultuur en -infrastructuur. Het motto van het beleid lijkt daarbij te zijn: uniek identificeren, centraal uniformeren en volledig digitaliseren. De algemene identificatieplicht wordt gezien als een cruciaal onderdeel van criminaliteits- en terrorismebestrijding. Een centraal en eenduidig identificerend nummer, het Burger Service Nummer, is het antwoord op de identiteitsfraude.² De digitale vingerafdruk als identificatiemiddel als dé oplossing voor 100% zekerheid. Ruimere toepassing van DNA technieken, meer cameratoezicht, het bewaren en koppelen van (verkeers)gegevens en een nieuw met biometrie uitgerust paspoort: de overheid lijkt bij het realiseren van alle ambities een welhaast absoluut vertrouwen te hebben in de techniek. Kortom, in het overheidsbeleid wordt (digitale) identificatie in stelling gebracht bij vrijwel alle actuele beleidsthema's: veiligheid, rechtshandhaving, doeltreffende opsporing³ en een efficiënte

1. Zie hierover NjB 2003, p. 2374-2376.

2. Zie hierover: J.E.J. Prins, 'Het BurgerServiceNummer en

de strijd tegen de Identiteitsfraude', *Computerrecht* 2003/1, p. 2-3.

3. Rondom de thema's veiligheid, rechtshandhaving en

doeltreffende opsporing liggen wetsontwerpen op tafel op onder meer het gebied van: algemene identificatieplicht, ruimere toepassing

van DNA- technieken, meer cameratoezicht, uitbreiding van controlebevoegdheden van de politie, uitbreiding van de mogelijkheid van

overheid.⁴ De consequentie van alle plannen is dat belangrijke stappen worden gezet richting stroomlijning, coördinatie en integratie van digitale identificatie en we meer en meer in de buurt van één uniforme (nationale) infrastructuur voor digitale identificatie komen.

Maar er is ook een andere zijde van de medaille: fraude met identiteiten. In december 2003 stuurde Minister Donner van Justitie het rapport *Identiteitsfraude en (reis)documenten* naar de Tweede Kamer.⁵ Het rapport – van de hand van de Koninklijke Marechaussee – spitst zich toe op identiteitsfraude met gestolen en vermiste identiteitsdocumenten. Begin 2004 zal het kabinet met een standpunt over deze problematiek komen. De Koninklijke Marechaussee is niet de eerste die wijst op de kwetsbare kanten van de huidige identificatieprocessen en -documenten. Al eerder had het kabinet in de Nota Bestrijding Fraude en Financieel-economische criminaliteit laten weten dat identiteitsfraude een onderwerp van toenemende zorg is en daarbij aangegeven te komen met maatregelen om de fraude- en criminaliteitsproblemen aan te pakken.⁶ Ook in een rapport van het Rathenau Instituut en de literatuur is inmiddels herhaalde malen gewezen op de kwetsbare kanten van de huidige werkwijze en instrumenten bij identiteitscontrole.⁷

Zoals bij zoveel toepassingen van ICT, geldt ook voor digitale identificatie dat we ons met de inzet van techniek kwetsbaar maken. Inmiddels is veel identiteitsgerelateerde informatie vrij beschikbaar. Niet alleen namen en (e-mail) adressen zijn op het Internet te achterhalen. Eenieder die zich wat moeite getroost, zal vaststellen dat foto's, creditcard- en andere nummers en vele andere identiteitsgegevens vrij beschikbaar dan wel te koop zijn op het Internet. Ervaringen in de Verenigde Staten laten zien dat de drang naar uniforme identificatie, in combinatie met onder meer de groei van de grensoverschrijdende elektronische communicatie via de open netwerkstructuur van het Internet, identiteitsfraude juist in de hand werkt. Identiteitsfraude is daar tot een probleem van inmiddels gigantische omvang uitgegroeid: het is de snelst groeiende vorm van criminaliteit, waar jaarlijks tussen de 500 000 en 700 000 mensen het slachtoffer van worden.⁸ Het Amerikaanse ministerie van Justitie maakte in 2002 melding van een geval waarin iemand had geprobeerd om via eBay duizend *social security*-nummers te verkopen tegen een prijs van \$ 1 per stuk. Kortom, de virtuele wereld biedt eenieder van ons de mogelijkheid om nieuwe en zelfs meervoudige identiteiten en dus persoonlijkheden aan te nemen. Maar de gevallen van fraude met zorgpassen en Sofi-nummers in ons land laten zien dat identiteitsfraude niet alleen met Internet te maken heeft.

Het lijkt geen twijfel: een goede en op technologie gebaseerde infrastructuur voor identificatie en authenticatie van mensen en processen komt er en moet er ook komen. Een scala aan nieuwe – elektronische – identificatiemiddelen heeft zijn intrede gedaan en daarmee ontstaan welhaast ongekennde mogelijkheden en voordelen van unieke identificatie, koppeling, stroomlijning en pro-actieve dienstverlening. Kortom, er zijn belangrijke voordelen op het terrein van eenduidigheid, transparantie en efficiën-

tie te behalen. Maar de cruciale vraag is wel of we ons voldoende realiseren welke consequenties de nu te nemen stappen uiteindelijk voor het totaalplaatje zullen hebben. Voor de komst van wat we veelal de informatiemaatschappij noemen, was de identiteit van een persoon en het proces van identificeren een redelijk beheersbaar proces. ICT heeft daarin echter grote veranderingen gebracht. Met de keuze voor stroomlijning en integratie maken we ons namelijk tegelijkertijd afhankelijker van het adequaat functioneren van een uniform en overheidsbreed identificatiesysteem en daarmee dus ook kwetsbaarder, niet alleen voor identiteitsfraude, maar ook voor bijvoorbeeld *cybercrime* en terrorisme.

De huidige sluipende infrastructurele operatie heeft daarom een fundamenteel en open debat. We zullen op zoek moeten gaan naar uitgangspunten voor een identificatie-infrastructuur waarmee diverse beleidsaspiraties kunnen worden aangepakt, die daarbij aansluit bij de technologische en maatschappelijke ontwikkelingen in onze samenleving en tevens oog heeft voor de veelheid aan – vaak tegengestelde – belangen die bij het regelen van deze materie in het geding zijn.

2. Afwegingen bij het scheppen van een identificatie-infrastructuur

Hoe nu zo'n infrastructuur te scheppen? Waar moeten we op letten? Wat zijn de keuzes waar we voor staan en wat moeten we doen (en niet doen) en in welke volgorde? Welke belangen staan op het spel, waar liggen de spanningen en welke uitruil van belangen moet plaatsvinden? Bij het antwoord op deze vragen lijken vier verschillende afwegingen gemaakt te moeten worden. Ze liggen op het terrein van de infrastructuur, de zwaarte van het identificatiemiddel, de plaats van regie en de belangen.

a. De infrastructuur: eenheid versus diversiteit

Kijkend naar het scala aan beleidsinitiatieven waarin digitale identificatie een rol speelt, lijkt het erop dat al deze initiatieven tamelijk autonoom en los van elkaar functioneren.⁹ Toch is er ook een zekere tendens van ontkokering zichtbaar. Waar voorheen de inspanningen primair gericht waren op digitale identificatiemiddelen die voor de eigen specifieke context noodzakelijk zijn, ligt nu het accent meer op de verbetering van de dienstverlening en verhoging van de efficiëntie. Daaruit vloeit de behoefte voort de verschillende initiatieven te coördineren en waar mogelijk op elkaar af te stemmen of te integreren. Een eenvormig systeem van digitale identificatiemiddelen heeft immers als voordeel dat meerdere gegevensbronnen op een zinvolle manier kunnen worden ontsloten. De initiatieven op het terrein van stroomlijning basisgegevens en eenmalige gegevensverstrekking zijn daar duidelijke voorbeelden van.¹⁰

De uiterste variant van integratie is dan een uniform stelsel voor digitale identificatie, waar bij de uitgifte, de keuze voor het type identificatie-instrument en alle overige onderdelen van het stelsel rekening wordt gehouden met de afgesproken standaard. De identiteitsgegevens worden centraal beheerd, de ver-

- ▶ koppeling en uitwisseling van informatiebestanden en het vormgeven van het nieuwe met biometrie beveiligde paspoort.
- 4. Hierbij valt vooral te denken aan de initiatieven voor stroomlijning van onderlinge gegevensuitwisseling, de modernisering van de Gemeentelijke Basisadministratie en de introductie van het Burger Service Nummer.
- 5. Rapport *Identiteitsfraude en (reis)documenten*, Koninklijke Marechaussee, 1 juni 2003. Zie ook het persbericht van het Ministerie van Justitie van 15 december 2003 www.justitie.nl/pers/persberichten.
- 6. *Kamerstukken II* 2001/02, 17 050, nr 234.
- 7. Rathenau Instituut (*ID or not to be? Naar een doordacht stelsel voor digitale identificatie*), genoemd in de sternoote op p. 114; J.E.J. Prins, 'Identiteitsinflatie', *JAVI*, december 2002, p. 98; J.H.A.M. Grijpink, 'Identiteitsfraude als uitdaging voor de rechtsstaat', *Privacy & Informatie*, augustus 2003, p. 148-153.
- 8. Sedert 1998 zijn in de VS diverse pogingen ondernomen om identiteitsfraude aan te pakken. Tot op heden hebben de maatregelen afgekeurd middels onder meer de 'Identity Theft and Assumption Deterrence Act', 'Social Security Number Misuse Prevention Act', 'Identity Theft Protection Act' en de 'Reclaim Your Identity Act' echter weinig effect gesorteerd. Momenteel werkt men aan een zogenaamd *Identity Theft Clearinghouse Database*. Wanneer men het vermoeden heeft slachtoffer te zijn geworden van een vorm van identiteitsfraude kan dat worden gemeld bij een centraal punt, waarna de desbetreffende informatie wordt doorgegeven aan de voor dat specifieke geval relevante overheidsinstanties.
- 9. Zie voor een uitgebreid overzicht de eerdergenoemde studie van het Rathenau Instituut.
- 10. *Kamerstukken II* 2003/04, 26 387, nr 21.

De virtuele wereld biedt eenieder van ons de mogelijkheid om nieuwe en zelfs meervoudige identiteiten en dus persoonlijkheden aan te nemen.

Het Microsoft-paspoort – ruim 350 miljoen abonnees! – is een duidelijk signaal dat op het Internet het bedrijfsleven voorop loopt in het ontwikkelen van grootschalige identificatie-initiatieven.

antwoordelijkheden met betrekking tot het stelsel liggen op een centraal niveau, de identificatiemiddelen zijn gestandaardiseerd en er zijn centrale afspraken gemaakt over eenvormig gebruik van identificatiesleutels, zoals nummers en andere unieke kenmerken. Met een dergelijke, geïntegreerde identificatie-infrastructuur zijn grote voordelen te behalen op het terrein van eenduidigheid, transparantie en efficiëntie. Dat het ontwikkelen van een dergelijk stelsel zeker niet ondenkbaar is, wordt duidelijk als alle initiatieven die inmiddels lopen in onderling verband worden gezien. Iedere volgende stap – hoe klein ook – is een stap in de richting van stroomlijning, coördinatie en integratie van digitale identificatie en zo komen we steeds meer in de buurt van een uniform (nationaal) stelsel.

Maar er kleven, zoals we hiervoor reeds stelden, ook nadelen aan een geïntegreerd systeem van digitale identificatie. Met iedere verdere stap die we in die richting zetten, maken we ons tegelijkertijd ook afhankelijker van het adequaat functioneren van dat ene stelsel. Clustering maakt het systeem kwetsbaar in de zin dat de zwakste schakel de betrouwbaarheid en veiligheid van de gehele keten bepaalt. De kwetsbaarheid neemt nog verder toe als we de controle met traditionele systemen gaan verwaarlozen. Als we de corrigerende werking van fysieke identificatie niet meer laten doorwerken, ontstaan (juridische) ficties die vervolgens realiteit worden ('het staat zo in de computer, dus het klopt'). Daarom is het van groot belang na te denken over de vraag hoe lang we de fysieke reserve van onze digitale identificatiemiddelen willen (en zouden moeten) bewaren en welke (juridische) waarde we daaraan hechten, en vooral ook wat de consequenties kunnen zijn als we deze reserve verwaarlozen.

b. De zwaarte van het middel: absoluut of relatief

Een tweede afweging betreft de vraag hoe sterk het identificatiemiddel moet zijn. Er lijkt sprake van een 'identificatielif': steeds meer wordt identificatie vereist en wordt daarbij het zwaarste middel ingezet. Biometrie en DNA zijn daar duidelijke voorbeelden van. Vraagt de overheid (en het bedrijfsleven) echter niet meer dan waar zij recht op heeft? Weegt het belang van 100% zekerheid op tegen de offers (privacy, kosten, moeite) die de burger en het bedrijfsleven zich moeten getroosten? Dient het uitgangspunt te zijn dat individuen altijd identificeerbaar moeten zijn, waarbij centralisatie en stroomlijning van registraties het mogelijk maken (indien nodig en omkleed met wettelijke waarborgen) zoveel en zo snel mogelijk gegevens over een individu te verzamelen? Of moet het uitgangspunt eerder zijn dat in rechtsrelaties een gedifferentieerd en contextgebonden stelsel van bevoegdheidsvaststelling heerst, waarbij zo mogelijk een pseudoniem en niet een identiteit wordt gebruikt, en waarbij contextafhankelijke gegevens niet per se zijn te relateren aan één en dezelfde persoon?¹¹

Kortom, is de zwaarte van het middel een absolute, autonome grootheid of is het een variabele die, afhankelijk van de situatie waarin een vorm van 'bekendmaken' moet plaatsvinden, tot een bepaalde uitkomst leidt? Overigens moeten we daarbij ook

nog constateren dat de discussie zich zwaar lijkt te concentreren op het middel (document of biometrie), zonder dat men zich druk maakt over allerlei andere relevante overwegingen. We lijken namelijk te vergeten dat de sterkte van de identificatie van meer factoren afhangt dan alleen het middel dat wordt gebruikt. Juist de registratie en het beheer van identiteitsgegevens, alsmede het proces van authenticeren (dus de eerste registratie) en de organisatie van het gehele stelsel zijn cruciaal voor de betrouwbaarheid. Anders gezegd: er wordt veel waarde gehecht aan het middel en er is minder aandacht voor de context waarbinnen dat middel moet functioneren: zowel intern (ontwerp, beheer) als extern (de noodzakelijkheid van gebruik).

c. De regie: publiek versus privaot

Ook de private sector zet in op nieuwe vormen van identificatie, onder meer om cliënten te identificeren, hun autorisatie te verlenen voor bepaalde diensten dan wel op maat diensten aan te bieden. In sommige gevallen zullen overheid en bedrijfsleven samen willen (of moeten) optrekken bij het vormgeven van bepaalde initiatieven op het terrein van digitale identificatie (zoals bijvoorbeeld de uitbouw van een systeem voor digitale handtekeningen). Deze ontwikkelingen zullen ertoe leiden dat op een zeker moment de afweging gemaakt moet worden wie het initiatief en de regie rond de vormgeving van digitale identificatie op zich moet nemen. Waar en onder welke omstandigheden moet de overheid een monopolie hebben en waar mag (of zelfs moet) ze ruimte laten voor marktpartijen? Voor welke sectoren? Wie zetten de standaarden? Waar moet de overheid handelen en waar juist niet? Hierbij komt ook de vraag naar voren wat nu precies de wisselwerking is tussen markt en overheid. De overheid zal zich daarbij bewust moeten zijn van haar verschillende rollen en haar specifieke hoedanigheid. In sommige gevallen zal immers uitsluitend de overheid in staat zijn bepaalde maatregelen te nemen, voldoende vertrouwen te geven en waarborgen te scheppen die onmisbaar zijn om digitale identificatie en identificatiemiddelen vorm te kunnen geven.

Tegelijkertijd zal de overheid scherp moeten zijn op de positie van het bedrijfsleven in samenhang met de dynamiek van de technologie. Als zij dat niet doet, zal zij voor voldongen feiten komen te staan en nog maar moeilijk in staat zijn zichzelf en burgers te behoeden voor een te grote afhankelijkheid van het bedrijfsleven, hetgeen kan leiden tot een grotere kwetsbaarheid van burgers en overheid. Het Microsoft-paspoort – ruim 350 miljoen abonnees! – is een duidelijk signaal dat op het Internet het bedrijfsleven voorop loopt in het ontwikkelen (en dus ook sturen) van grootschalige identificatie-initiatieven. Opvallend is zeker ook dat Minister De Graaf voor Bestuurlijke vernieuwing en Koninkrijksrelaties afgelopen december, bij de presentatie van een proef in zes gemeenten met een vinger- en een gelaatsscanner op het paspoort, aangaf dat de keuze voor de gelaatsscanner mede is ingegeven vanwege het feit dat op een mogelijk alternatief, de iristechneek, een octrooi rust. De keuze voor de irisscanner zou de overheid te afhankelijk maken van één leverancier. Opvallend is deze ontwikkeling des te meer, nu blijkt uit een onderzoek

11. J.E.J. Prins, 'What's in a name? De juridische status van een recht op anonimiteit', *Privacy & Informatie*, augustus 2000, p. 148-152; Koops, B.J., 'Een nieuwe GBA, digitale kluis en identificatiedrang', *NJB* 2001, p. 1555-1561.

dat de minister heeft laten uitvoeren dat de gelaats-scan zeker niet de meest betrouwbare vorm van biometrie lijkt te zijn.¹²

Het is dus van groot belang dat de overheid steeds doorgronde wat de mogelijke toekomstige implicaties van private identificatie-initiatieven kunnen zijn voor de eigen vormgevingsactiviteiten. Men moet daarbij overigens niet vergeten dat de *toekenning* van digitale identificatiemiddelen (en het beheer van het identificatiesysteem) een andere zaak is dan het daadwerkelijke *gebruik* van die middelen. Door de overheid gecreëerde digitale identificatiemiddelen kunnen wel degelijk in de private sector een rol spelen. Het scheppen en toekennen van de bronidentiteit (met behulp van bijvoorbeeld biometrie) moet echter voorbehouden blijven aan de overheid, terwijl de private sector wel gebruik kan maken van de *templates*¹³, maar niet van de achterliggende gegevens. Hier zijn interessante publiekprivate samenwerkingsvormen denkbaar en misschien zelfs wel noodzakelijk.

d. De wens: gemak en resultaat versus vrijheid

De ontwikkelingen op het gebied van ICT hebben ons maatschappelijk en sociaal functioneren de afgelopen jaren in vele opzichten eenvoudiger gemaakt. Ook de publieke sector heeft haar voordeel kunnen doen met ICT. Zo zijn de afgelopen jaren diverse ICT-applicaties ontwikkeld en ingezet om bestuurlijke problemen aan te pakken, handhaving te verbeteren en de dienstverlening efficiënter te laten verlopen. De applicaties worden daarbij veelal als service aan de burger gepresenteerd (burgerservicekaart) of geïntroduceerd onder het motto: 'leuker kunnen we het niet maken, wel makkelijker'. Ook de plannen rondom identificatie en digitale identificatiemiddelen passen in dit beeld. Proactieve dienstverlening, eenmalige gegevensverstrekking, stroomlijning van gegevens: de plannen worden gelanceerd met als boodschap een verbeterde dienstverlening door de overheid. Ook de kabinetsnota 'Een andere overheid' is daar wederom een voorbeeld van.

De uiteindelijke consequentie van deze ontwikkelingen kan wel zijn dat de overheid de beschikking krijgt – of denkt te hebben – over een vrijwel compleet beeld van het doen en laten van haar burgers. Het op eigen initiatief aanvragen van bepaalde voorzieningen behoeft dan niet meer. Bezwaar aantekenen heeft weinig zin. De overheid beschikt immers over alle relevante informatie. Binnen dit kader passen kreten als: 'Uit onze gegevens blijkt dat u recht heeft op een tegemoetkoming. Nadere informatie hebben we niet nodig. We beschikken inmiddels over alle noodzakelijke gegevens.' 'Uit onze bestanden blijkt dat deze gegevens juist zijn.' 'Indien u het met de beslissing niet eens bent, kunt u bezwaar aantekenen, maar inmiddels blijkt uit andere bronnen dat ...' De fictie dat al deze informatie ook de *juiste* informatie is, en dat die in wetgeving wordt vastgelegd, geeft de overheid de garantie dat procedures vervolgens ook efficiënt en snel kunnen worden afgehandeld. Maar de vraag is hoe ver we optimalisatie (onder het mom) van 'gemak' willen doorvoeren?

De uiteindelijke consequentie van deze ontwikkelingen kan wel zijn dat de overheid de beschikking krijgt – of denkt te hebben – over een vrijwel compleet beeld van het doen en laten van haar burgers.

Waar trekken we de grens en waar laten we het initiatief en de regie aan de burger? Kortom: wanneer krijgt vrijheid voorrang boven gemak?

3. Enkele startpunten voor een debat

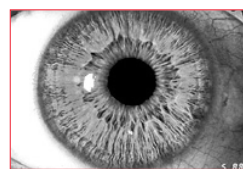
We gaven hiervoor aan dat de huidige sluipende ontwikkelingen op het terrein van (digitale) identificatie een fundamenteel en open debat vergen. Met de hiervoor geschetste afwegingen in het achterhoofd, willen we voor dat debat drie startpunten formuleren.

De regie moet bij de overheid liggen

Allereerst zal de overheid zich bewust moeten zijn van haar verantwoordelijkheid en monopoliepositie. Immers, het primaat van het scheppen van (een debat over) een infrastructuur ligt bij de overheid. Zij is de enige die in staat is voldoende vertrouwen te geven en waarborgen te scheppen. Met andere woorden *noblesse oblige*: burgers en bedrijven zijn afhankelijk van de overheid; sterker nog: ze zitten te wachten en kijken wat de overheid doet, simpelweg omdat ze het zelf niet kunnen. Om dat debat op gang te trekken, zal de overheid het belang helder moeten maken: ministeries en uitvoeringsorganisaties zullen ervan overtuigd moeten worden dat zij gezamenlijk aan deze discussie moeten deelnemen (zoals de ministeries van Justitie, Financiën, Binnenlandse Zaken en Koninkrijksrelaties, Sociale Zaken, Economische Zaken, en voorts vertegenwoordigers van koepelorganisaties (werkgevers, gemeentes, (privacybehoef-tige) burgers en consumenten). Om de vaart erin te houden is een sectoroverstijgend vehikel nodig: een 'Platform Identificatie', onder onverdacht voorzitterschap (bijvoorbeeld belegd bij het ICTU).

Het debat moet gaan over de wezenlijke vragen, niet over de middelen

In de tweede plaats is momenteel het debat volledig gecentreerd rond de middelen: Wat voor biometrie moet er op het paspoort? Willen we één of meerdere chipcards in de relatie met de overheid? Hoe moet er aan de buitengrenzen geïdentificeerd worden? Over de implicaties van (het scheppen van) die middelen wordt daarentegen te weinig nagedacht. Dit heeft tot gevolg dat de achterliggende en veel fundamentele discussie over de consequenties van de inzet van deze middelen voor het identificatieproces niet aan bod komt. Het zou dan moeten gaan om vragen als: Wie moet het stelsel scheppen en beheren (één ministerie, meerdere)? Welke fundamentele belangen zijn in het geding en welke waarborgen moeten gelden? Hoe moeten onderhoud en beveiliging vorm krijgen en welke regels en *checks and balances* moeten er gemaakt worden om het ontstaan en voortbestaan van juridische ficties tegen te gaan? Leggen we de nadruk op de stem van de bestuurde of juist op die van het bestuur? Welke bestuurslagen moeten een rol hebben en wat willen zij? Gaan we voor duur of goedkoop? En wie moet dat betalen? De overheid moet er kortom voor zorgen dat er een discussie ontstaat over de fundamentele veranderingen die optre-



12. 'Proef biometrische kenmerken op paspoort', persbericht ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 29 december 2003 www.minbzk.nl.

13. Eenvoudig gesteld worden op de *template* de in technische code omgezette gegevens geplaatst.

Het sprookje moet overboord dat de overheid een identiteitsstelsel moet scheppen omdat burgers daar in de interactie met de overheid behoefte aan zouden hebben.

den bij de nieuwe invulling van identificatie en identificatieprocessen.

In het debat moeten axioma's op de helling of ontmythologiseerd worden

Het scheppen van een nieuw stelsel voor identificatie is een essentiële voorwaarde voor de modernisering van de overheid. Als dit debat gevoerd wordt vanuit de bestaande loopgraven zal het stelsel hopeloos verouderd zijn nog voordat we het kunnen invoeren. Welke stellingen moeten verlaten worden?

- I. In de eerste plaats moet in een moderne relatie tussen burger en – met name een presterende – overheid de overheid kunnen vragen (en zeker moet kunnen weten) met wie ze van doen heeft. Dit geldt vooral waar het gaat om maatwerk dienstverlening (zorg, onderwijs, inkomensoverdrachten); uiteindelijk is dit ook in het belang van de burger. Maar cruciaal is dat niet de technologie leidend is, maar dat de belangen van proportionaliteit en subsidiariteit voorop staan en concreet handen en voeten krijgen. En juist technologie biedt de mogelijkheid de handen en voeten vervolgens vorm te geven: technologie biedt immers de mogelijkheid te nuanceren tussen anonimiteit en identiteit.¹⁴
- II. Verder moet het sprookje overboord dat de overheid een identiteitsstelsel moet scheppen omdat burgers daar in de interactie met de overheid behoefte aan zouden hebben. De behoefte aan een overheid als proactieve dienstverlener is grotendeels een mythe. De contactmomenten met de overheid zijn in een mensenleven relatief beperkt en dikwijls dan ook nog verplicht. De transactiegedachte, zoals dat bij contacten in de private sector het geval is, kan hier (bijna) nooit opgeld doen.
- III. Bij het scheppen van het stelsel moet de overheid zich bewust zijn van de basale behoefte van burgers aan beschikkingsmacht over keuzes: daar gaat het veelal niet om de vraag óf persoonsgegevens verwerkt worden; het gaat erom wat er vervolgens mee gebeurt, hoe lang de gegevens worden bewaard, welke *checks en balances* er gelden en op welke wijze daarop controle is. Mensen willen de mogelijkheid houden zelf zaken in de hand te houden en deels te beslissen. Daarbij hoort een basaal recht geïnformeerd te worden, zodat burgers weten dat er een keuze is en waartussen. Immers, als het kabinet in haar visie op 'Een andere overheid' de wens uitspreekt tot een nieuw maatschappelijk contract te willen komen met meer gelijkwaardige verhoudingen tussen burgers en overheid, dan dienen burgers daartoe ook de noodzakelijke instrumenten in handen te krijgen. Openheid van zaken is daarbij cruciaal.
- IV. Het scheppen van een identiteitsstelsel is natuurlijk omgeven door tal van privacyrechtelijke vragen. Deze mogen echter niet leidend zijn in het debat. We hebben gezien dat ook andere belangen, zoals de behoefte aan efficiëntie, afhankelijk-

heid en kwetsbaarheid, aandacht vereisen. En wanneer de privacyrechtelijke vragen aan bod komen, zullen ze vooral niet bediscussieerd moeten worden op de wijze waarop dat nu vrijwel standaard gebeurt, namelijk vanuit de optiek van persoonsgegevensbescherming en de invloed van techniek. Als we de discussie op die manier voeren, hebben we het in feite over niet meer dan beveiliging en afspraken maken over de omgang met gegevens, de juistheid ervan, etc. Privacy is echter veel meer: zeker in het debat over de identificatie-infrastructuur gaat het om zaken als vrijheid en zelfbeschikkingsrecht.¹⁵

Kortom, het wordt tijd een aantal, voor identificatievraagstukken relevante grondslagen van het recht fundamenteel ter discussie te stellen. Het gaat erom uit te vinden wat de burger nu werkelijk wil en het onderhavige onderwerp biedt nu (eindelijk) bij uitstek eens de mogelijkheid om privacy 'politiek' te maken en het uit de abstracte, juridisch technische, hoek te halen. Daarbij zal de overheid vooral ook eens kritisch naar haar eigen optreden moeten kijken. De overheid heeft de privacyclaim welhaast gemonopoliseerd en overtreedt iedere dag het relativiteitsvereiste: tal van overheidsorganisaties treden ongevraagd op als hoeder van privacybelangen van burgers: ze is een rentmeester geworden, zonder dat ze zich ervan heeft overtuigd of daar wel voldoende steun voor is.

4. Conclusie

Het kabinet zet in de Nota 'Een andere overheid' de bijl in vele heilige huisjes. Ze spreekt van onrealistische verwachtingen over hetgeen de overheid vermag, een doorgeschoten subsidieverslaving van delen van de *civil society* en de noodzaak te komen tot een nieuw maatschappelijk contract. De paternalistische verzorgingsstaat moet plaats maken voor een participatiestaat die zich vooral kenmerkt door meer gelijkwaardige verhoudingen tussen burgers en overheid, aldus het kabinet. Wil de overheid de rol van 'albedil' inderdaad van zich afschudden dan zal ze daarin ook volledig de weg moeten lopen. Ze zal de troefkaarten op het terrein van identificatie die ze momenteel in handen heeft op tafel dienen te leggen en met burgers open kaart moeten spelen over de toekomst en inrichting van de identiteitsinfrastructuur. Dat vraagt om meer dan wat eenvoudige opmerkingen over eenmalige gegevensverstrekking en de inrichting van een overheidsbrede authenticatie-infrastructuur. Dat vraagt om een fundamenteel, open, gedemythificeerd en door de overheid gemodererd debat waarin de wezenlijke keuzes waar we voor staan en de daarmee gemoeide belangen aan de orde komen. Juist – en alleen door – de uitruil van deze belangen zal het mogelijk zijn een overheidsbreed gedragen en publiekelijk gewenst en geaccepteerd stelsel te scheppen. Dat moet gebeuren vóórdát we definitieve, onomkeerbare beslissingen hebben genomen, niet daarna. ■

14. Zo biedt biometrie de mogelijkheid specifieke rechten van een persoon te verifiëren (bijvoorbeeld of de persoon toegang tot bepaalde faciliteiten mag worden verleend) zonder te weten met wie men precies van doen heeft.

15. Zie hierover: J.E.J. Prins, 'Acht gesprekken over privacy en aanpalende belangen', in: *Zeven essays over informatietechnologie en recht*, Den Haag: Sdu uitgeverij 2003, p. 53-105.