

Het bestuur als de tovenaarsleerling van ICT

Egbert Dommering¹

De WRR heeft in het rapport *i-Overheid* een belangrijk onderwerp op de agenda gezet. Het Rathenau Instituut ging hem daarin in 2010 al voor. ICT is een instrument waarmee de nationale en Europese bestuurlijke bureaucratieën en organisaties in het middenveld steeds meer macht over de burgers krijgen, maar ook steeds meer privacyrisico's creëren. ICT blijkt geen 'neutraal' instrument, maar één dat een voortgaande verschuiving van de macht richting bestuur binnen de trias politica versterkt. De reactie van de regering is wat lauw gezien de urgentie van het probleem.

Het WRR-rapport *iOverheid*

De Wetenschappelijke Raad voor het Regeringsbeleid heeft in 2011 een stevig rapport uitgebracht, ondersteund door een kloeke gebundelde reeks voorstudies.² De studie heet *iOverheid*: informatie-overheid, bedoeld als contrast van het meer gebruikelijke *eGovernment*: elektronische overheid. Het gaat inderdaad om informatie (volgens bepaalde conventies geïnterpreteerde data). Kennis is macht. Het rapport analyseert de door ICT ondersteunde groeiende macht van een vernetwerkte overheid over de burger. Inmiddels heeft het kabinet zijn standpunt naar aanleiding van het rapport bepaald.³ In het navolgende zal ik rapport en reactie bespreken. Het rapport moet worden geplaatst tegen de achtergrond van de langzaam eroderende trias politica waarin de 'uitvoerende macht' nationaal en Europees komt bovendien. ICT is een multiplier in dit proces. Eerst iets over de trias politica en de 'machtsvrije' sfeer van de burger.

Van een analytisch model der gescheiden machten naar (een mede door ICT) vernetwerkte overheid

Democratische constituties zijn wereldwijd gebaseerd op het van Montesquieu afkomstige model dat er een scheiding moet zijn tussen drie machten: de wetgevende (die de wetten maakt), de uitvoerende (die de wetten uitvoert) en de rechterlijke (die wetten toepast). Alleen bij die scheiding is gewaarborgd dat er geen tirannie zal ontstaan, waarin alle macht is samengebondeld. Het is gebaseerd op de veronderstelling dat de uitvoerende macht politieke verantwoording aflegt aan de wetgevende macht voor daden van uitvoering. Als dat verantwoordingsproces in de ogen van de burgers niet goed verloopt, kunnen zij in rechtstreekse verkiezingen de politieke machtsverhoudingen binnen de wetgevende macht trachten te veranderen. De verantwoording van de rechterlijke macht is gelegen in het feit dat zij geen poli-

Er is eigenlijk geen moment meer waarop wij niet geregistreerd, geïdentificeerd en in een bestand opgeslagen worden

tieke beslissingen, maar juridische beslissingen neemt. Het model trekt ook een scheidslijn tussen overheid en de burgers. Die scheidslijn is gebaseerd op de veronderstelling dat er een vrije sfeer is waarin de burgers in vrijheid zonder overheidsinmenging (dus inmenging van één van de machten) kunnen leven. Die sfeer wordt beschermd door grondrechten. Het privacyrecht vindt zijn oudste oorsprong in die vrijheid. Omdat dit artikel voor een belangrijk deel over privacy zal gaan is het goed om een formulering uit de klassieker van Allan Westin, *Privacy and freedom* hier te herhalen omdat daarin de kern in staat waar het bij privacy om draait:

'Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (...) Privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude

Auteur

1. Prof. mr. E.J. Dommering is emeritus Hoogleraar Informatierecht aan de Universiteit van Amsterdam. De schrijver dankt Frank Kuitenbrouwer en Frederik Zuiderveen Borgesius voor waardevolle opmerkingen bij een eerdere versie van dit artikel.

Noten

2. WRR-rapport nr. 86, *iOverheid* en WRR-verkenning nr. 25 *De staat van informatie*, Amsterdam: Amsterdam University Press 2011.
3. Brief van 25 oktober 2011 (*Kamerstukken II 2010/11*, 26 643, 211) p. 4.

or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve.⁴

Het trias politica model is op allerlei manieren onder druk komen te staan. Allereerst is de scheiding tussen wetgeving en bestuur in een complexe samenleving met een complex bestuur minder duidelijk. Al sinds de jaren zestig van de vorige eeuw discussieert de rechtswetenschap over het probleem van de 'vage norm' en de 'getrapte normstelling' in de wetgeving die tal van concrete normstellende vragen delegeert aan het bestuur en aan de rechterlijke macht. Het maatschappelijk middenveld oefent met haar lobby's via bestuur en parlement rechtstreeks invloed uit op de inhoud van de wetgeving en bestuursbeslissingen. Bovendien is het middenveld door privatiseringsprocessen of publiek-private samenwerkingsvormen nauw betrokken geraakt bij 'uitvoering' van wetgeving. Controle op uitvoering is in gespecialiseerde maatschappelijke sectoren te ingewikkeld geworden, zodat daarvoor speciale zelfstandige bestuursorganen zijn ingesteld. In de afgelopen twintig jaren zijn er flink wat 'Autoriteiten' opgericht die een mengsel van uitvoering, toepassing en normstelling in zich verenigen. De Europese Unie heeft de nationale bestuursbureaucratieën versmolten met een Europese bureaucratie: ver achter de horizon van de nationale wetgever en zeker ook van de burger. Maar ook de vrije sfeer van de burger is ingekrompen. De burger werd in de verzorgingsstaat overgoten met welzijn dat alleen aan hem op maat kan worden afgeleverd als 'de instanties' veel over hem weten. Na 9/11 is de burger bovendien een potentiële vijand geworden die voortdurend in de gaten moet worden gehouden. Dit heeft geleid tot een netwerk van welzijns- en controledatabanken waarin duizelingwekkende hoeveelheden persoonsgegevens worden opgeslagen.

'Function creep' is een intrinsieke eigenschap van een 'slim, innovatief en efficiënt' ICT-systeem

De vernetwerking van nationaal en internationaal bestuur veroorzaakt een afname van politieke legitimiteit: binnen het politieke systeem is de burger vervaagd. De drang tot herstel van rechtstreekse invloed vindt zijn weerslag in Europa brede populistische partijen. De vernetwerking heeft tegelijkertijd geleid tot vergroting van de macht van de overheid over de burger. Buiten het politieke systeem is de burger scherp in het vizier: een doelwit van welzijn en controle.

Het WRR-rapport *iOverheid*: hoe het complexe vraagstuk aan te pakken en te beschrijven?

De WRR heeft kennelijk moeite gehad met de vraagstelling rond dit bijzonder complexe probleem. De onderzoekers in de voorstudies waren op pad gestuurd met de aanwijzing dat het zou moeten gaan over twee typen van verantwoordelijkheid van de overheid: 'In de eerste plaats

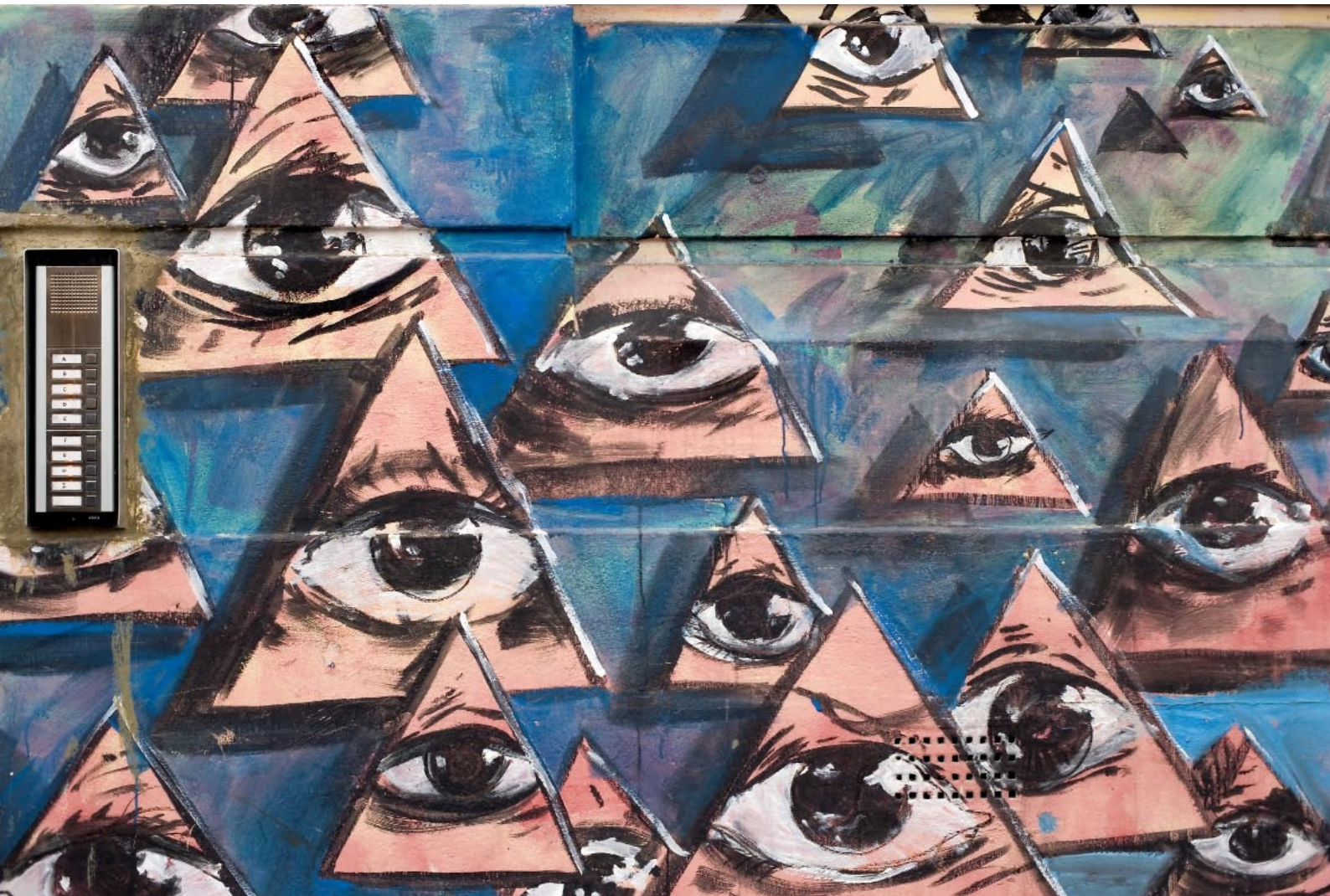
verantwoordelijkheid vanuit de rol van overheid als gebruiker van ICT, vooral voor de uitvoering van beleid dat de burger (direct) raakt. In de tweede plaats vanuit de rol van de overheid als "systeembeheerder" of regulator voor kwesties met betrekking tot technologie, informatie en informatieprocessen in de samenleving, in het bijzonder "private" ontwikkelingen die de positie van de burger raken.'⁵ Het is duidelijk dat in de eerste categorie de verantwoordelijkheid voor het eigen ICT-gebruik (lees: de voortdurend bij de overheid uit de hand lopende 'automatiseringen') en het opzetten van databanken en verzamelen van persoonsgegevens door elkaar lopen. Het is ook duidelijk dat de tweede verantwoordelijkheid overlapt met de eerste. Ook de relatie met 'private' ontwikkelingen is nogal ruim. In het rapport zelf wordt het object van de studie geconcentreerd op de relatie overheid-burger en hoe die door digitaliseringsprocessen ingrijpend is veranderd:

'De facto en bijna ongemerkt heeft zich een praktijk ontwikkeld, waarin samenhangende informatiestromen het karakter van de overheid domineren. En daarmee bepalen deze informatiestromen ook het functioneren, de afhankelijkheid en de kwetsbaarheid van zowel de overheid als haar burgers.'⁶

Dit is een overzichtelijke beperking, maar het tweede aspect (de verantwoordelijkheid naar de samenleving) krijgt toch nog een ondergeschikte plaats in het rapport.

De casuïstiek over de 'informatiestromen' waarin burgers verknoot raken in machts- en welzijnssystemen die door de overheid worden aangestuurd is omvangrijk. De voorstudies brengen de bekendste gevallen in beeld. Het Schengenakkoord beoogt de mobiliteit en het vrije verkeer van personen te verbeteren, maar heeft van Europa een digitale kooi (het Schengen Information System, dat wordt aangeduid met de lugubere afkorting SIS) gemaakt waarin de bewegingen van de 'vrije' EU burgers nauwgezet worden geregistreerd.⁷ Het elektronisch patiëntendossier strandde in 2011 in de Eerste Kamer. De hemel en hel overstijgende doelstelling van dit dossier (EPD) was *eHealth*, een informatiesysteem 'dat in staat is om alle gegevens van een patiënt van wieg tot graf te bevatten en toegankelijk te maken.'⁸ En dan is er het 'Kinddossier' (EKD) dat alle risicofactoren van jongeren al in een vroeg stadium vastlegt, in de voorstudies gekarakteriseerd als 'een spin in een digitaal vangnet'.⁹ Dit zijn een paar bekende probleemdossiers (overigens niet erg 'ehealthy'). Het Rathenau Instituut schrijft al jaren rapporten over deze problematiek.¹⁰ Alarmerend is het rapport *Check in/Check out* uit 2010 over de 'digitale ruimte'.¹¹ Het brengt alle controleapparatuur in de ruimte, die zich daar bevindt of door de burger wordt meedragen, in beeld: poortjes, camera's, pasjes, mobiele telefoons, radiofrequenties, i-phones, enzovoort. Er is eigenlijk geen moment meer waarop wij niet geregistreerd, geïdentificeerd en in een bestand opgeslagen worden.

Wat al deze dossiers gemeen hebben is dat het opzetten van het systeem gevoed wordt door een onbegrensd vertrouwen in ICT en dat deze systemen worden ontworpen met dikwijls onduidelijke doelstellingen of dat er gaandeweg allerlei doelstellingen aan toe worden gevoegd. Dat laatste noemen we *function creep*, de niet expliciete functie die stilzwijgend in het systeem kruip



als het er één keer staat. Het is van groot belang dat de WRR deze problematiek centraal op de beleidsagenda heeft geplaatst.

De aanpak van de WRR

De WRR meent de problematiek in kaart te hebben gebracht door een model te ontwerpen dat bestaat uit 'sturende, verankerende en procesmatige beginselen'. De Raad noemt dit een 'analytisch drieluik van beginselen'. Die 'sturende' beginselen zijn 'veiligheid, effectiviteit en efficiency'. De 'verankerende' beginselen zijn 'privacy en keuzevrijheid'. En de procesmatige beginselen zijn 'transparantie en accountability'.¹² Hoewel ik de analyse wel kan volgen, vind ik het gebruik van 'beginselen' om verschillende redenen

verwarrend. 'Beginsel' vat ik op als normatief, terwijl ik bij het sturende deel eerder aan stuwende krachten denk dan aan een normatief kader, hoewel hier ook sprake kan zijn van een normatief beginsel van systeemveiligheid (waarover hierna). Beginsel stel ik normatief lager (ook al hang je er een anker aan) dan een subjectief (grond)recht, en aan dat laatste zou ik bij privacy en keuzevrijheid toch eerder denken. Wellicht dat in de benoeming van 'veiligheid' en 'privacy' als ogenschijnlijk gelijkwaardige beginselen, nog het rapport van de Commissie Brouwer-Korf, *Gewoon doen; van veiligheid en persoonlijke levenssfeer* waarin veiligheid en privacy aan elkaar worden gekoppeld, nawerkt.¹³ De plicht tot transparantie zie ik als onderdeel van het privacyrecht, en accountability acht ik van toepas-

4. Alan F. Westin, *Privacy and Freedom*, London: The Boldly Head 1967, p. 7.

5. *De staat van informatie*, p. 22-23.

6. *iOverheid*, p. 32.

7. Nauwkeurig in kaart gebracht door E. Brouwer in haar dissertatie, *Digital Borders and Real Rights*, Nijmegen: Van der Wolf 2007, en in de voorstudies geactualiseerd door Dennis Broeders, 'Grensoverschrijden-

de mobiliteit van personen en de digitale grenzen van Europa.'

8. De Minister van VWS, geciteerd in de voorstudie van Anne-Greet Keizer 'De digitale patiënt centraal- medische informatie in een digitale wereld.'

9. Esther Keymolen en Corien Prins, 'Jeugdzorg via systemen. De verwijzingsindex risicjongeren als spin in een digitaal vangnet'.

10. Laatste: Geert Munnichs, Mirjam Schuijff & Michiel Besters, *Databases. Over ICT belofes, informatiehonger en digitale autonomie*. Den Haag: Rathenau instituut 2010. Hierin ook beschrijving van de bekende casus en bovendien de Gemeentelijke Basis Administratie, afgekort tot GBA.

11. Christian van 't Hof, Rinie van Est en Floortje Daemen, Rotterdam: NAI uitgevers

2010.

12. *iOverheid*, p. 73 e.v.

13. Brief van de Minister van Justitie van 3 november 2009, Kabinetstandpunt advies Commissie Brouwer-Korf en evaluatie van de Wet bescherming persoonsgegevens, *Kamerstukken II* 2009/10, 31 051, nr. 5.

Een samenleving die de veiligheidsutopie in het vaandel schrijft heeft de neiging risicominderheden te stigmatiseren en uit te sluiten

sing op het hele proces (stuwend, verankerend en procesmatig) en niet alleen op het procesmatige. De regering neemt het model niet over, maar stelt er niets substantieels voor in de plaats. Hoewel ik het analytisch model anders invul, volg ik het hierna in grote lijnen.

Wat 'stuwt' databanken?

Techno-sociale systemen

De Raad gaat uit van de thans heersende opvatting dat het ontwerp en de functionaliteit van een technologie gemaakt wordt door een samenleving, maar dat, als de technologie er eenmaal staat, er een wisselwerking ontstaat met sociale relaties. Om het simpel te zeggen: In de Westerse wereld werd de uitvinding van de telecommunicatie gedaan, omdat er een sociale behoefte bestond aan vrije informatie-uitwisseling; de zakenwereld maakte de telefoon tot een belangrijke toepassing van telecommunicatie, omdat deze individuele vorm van communicatie voor het handelsverkeer van levensbelang was. Toen de telefoontechnologie op gang kwam ontstonden er rond die technologie nieuwe beroepen en ging zij het sociale communicatiegedrag van mensen beïnvloeden. Technologie is dus een techno-sociaal systeem.¹⁴ De trits: sociale behoefte, technische invulling van die behoefte en feedback van de techniek op de sociale verhoudingen, zien we ook in dit probleemveld.

Openbare registers voor het rechtsverkeer en toekenning van rechten

Sinds Napoléon de registers van de burgerlijke stand instelde, zijn openbare registers niet meer weg te denken als ondersteuning van het rechtsverkeer. Burgerlijke stand, kadaster, handelsregister, noem maar op: zonder die registers kan het rechtsverkeer en de uitoefening van rechten niet plaatsvinden. De Amerikaanse politicoloog James Scott heeft in zijn boek uit 1998 *Seeing like a State* laten zien dat staten er altijd op gericht zijn geweest om van de staatsburger een *leesbare eenheid* te maken.¹⁵ Die drang om de burger leesbaar en het openbare rechts- en maatschappelijke verkeer controleerbaar te maken is in de 21e eeuw uitgegroeid tot ongekende proporties. En hier zien we dus het zich elkaar versterkende effect van maatschappelijk controle – en registratiebehoefte die de ICT 'uitvindt' aan de ene kant, en de versterking en perfectie van sociale controlehandelingen die door ICT-gebruik worden opgeroepen. In de klassieke trias politica wordt uitvoering ingevuld met de juridische middelen van privaatrechtelijke, bestuurlijke en strafrechtelijke sancties. In de ICT-wereld is daar de sturing door middel van verzameling en bewerking van persoonsgegevens bijgekomen. Het is dit uitvoeringsinstrument dat de machtsverhoudingen binnen de trias politica en ten opzichte van de burgers steeds meer in onbalans brengt.

Koppeldrang: van specifieke naar algemene ontsluiting. Hergebruik voor een ander doel. Inherente expansie en afnemende kosten

'De aard van de informatietechnologie is dat er een 'aandring' is gegevenskoppeling tot stand te brengen. (...) Kenmerkend voor automatisering is dat deze gegevens ontsluit van meer specifieke toepassing voor algemeen gebruik.'¹⁶ In de termen van het Rathenau Instituut van 2010 heet dit de intrinsieke drang tot efficiencyverhoging, profilering en hergebruik voor een ander doel.¹⁷ Aanvankelijk staat dat allemaal in het teken van verbetering van de service aan de burger. Het EKD en het EPD zijn opgezet om op het juiste moment alle gegevens met betrekking tot een patiënt of een moeilijk kind bij elkaar te hebben om de arme drommels beter te kunnen *helpen*. De 'open data'-discussie mondt uit in een transparante overheid met één loket waar de burger voor al zijn vragen terecht kan (het Burger Service Nummer).¹⁸ Ook in Brussel draait er een krachtige motor om ICT in te zetten om een 'slimme, duurzame en innovatieve' overheid te bevorderen: 'Het effectiever maken van e-overheid betekent dat diensten rond de behoeften van gebruikers worden ontworpen en flexibele en gepersonaliseerde manieren van interactie en verrichten van transacties met overheidsdiensten worden aangeboden.'¹⁹ Een van die projecten luistert naar (ook al weer) een lugubere afkorting SPOCS ('Simple Procedures Online for Cross-border Services'), het één-loketten-spook om administratieve belemmeringen voor grensoverschrijdend dienstenverkeer op te heffen. Maar één loket betekent gekoppelde loketten, dus gekoppelde bestanden.

Het hergebruik voor een ander doel is ingebakken in de IC-technologie. Een toegankelijk systeem van persoonsgegevens vraagt erom. Een kentekenregister is onontbeerlijk voor een geordend rechtsverkeer in auto's of de heffing van motorrijtuigenbelasting. Maar je kunt er ook auto's mee verkopen, autodieven mee vangen of er mee bijhouden waar auto's zich bevinden. 'Function creep' is een intrinsieke eigenschap van een 'slim, innovatief en efficiënt' ICT-systeem.

ICT-systemen zijn 'van nature' expansief in termen van uitbouw, centralisatie, en identificatie. Door de snel afnemende kosten van verzameling, opslag en bewerking van data is er ook geen economische prikkel meer het systeem beperkt te houden. Daardoor dreigt ook de band tussen verzamelen van data en informatie nodig voor besluitvorming doorgeknipt te worden.²⁰

De Veiligheidsutopie

De socioloog Boutellier heeft in navolging van Ulrich Beck, die de term 'risicomaatschappij' muntte, onze samenleving getypeerd als een 'veiligheidsutopie'. Dat is een samenleving die de paradoxale doelstelling heeft maximale individuele vrijheid én maximale veiligheid *tegelijk* te realiseren, dus totale egotistische vrijheid *naast*

maximale controle tegen dikwijls ongrijpbare risico's.²¹ Na 9/11 is de utopie overheersend geworden. De WRR spreekt van een 'dominant beleidsdoel'.²² De samenleving wil steeds meer controle ook als het eigenlijk zinloos is (bijvoorbeeld de veiligheidspoortjes op de luchthaven). Het is een bezweringsritueel dat burgers, bestuurders en politici een veilig gevoel geeft.

Maar de drang naar maximale vrijheid, wil dat de controle zo min mogelijk ingrijpt op individuele vrijheid. Dit zet druk op het systeem zo vroeg mogelijk risico's uit te selecteren aan de hand van voorspelbare persoonskenmerken, zodat de controlelast op de 'normale' vrije burgers vermindert.²³ Het EKD is er een voorbeeld van. Een ander voorbeeld is het recente plan van de IATA de controle-druk bij het instappen op luchthavens te verminderen, door op basis van analyse van persoonsgegevens die vooraf zijn verzameld uit gekoppelde databanken, de kleine groep te selecteren die een zware poortcontrole moet ondergaan en een groep die een lichte poortcontrole krijgt.²⁴ Een samenleving die de veiligheidsutopie in het vaandel schrijft heeft de neiging risicominderheden te stigmatiseren en uit te sluiten.

Privacy en veiligheid: is er controle op de ankers of zijn ze losgeslagen?

Twee soorten veiligheid

Veiligheid ziet op systeemveiligheid en maatschappelijke veiligheid. Systeemveiligheid houdt in dat systemen veilig functioneren en niet gemakkelijk gekraakt kunnen worden. De externe politieke druk om die veiligheid (en dus ook de privacy) zo veel mogelijk te garanderen is groot. Het lek bij DigiNotar veroorzaakt grote maatschappelijke opwinding en druk op de verantwoordelijke minister.²⁵ Deze systeemveiligheid dreigt alle andere aspecten in de discussie weg te drukken. Het is een 'handzame bliksemafleider'.²⁶

Maatschappelijke veiligheid gaat over de paradox van de veiligheidsutopie. De maatschappelijke druk werkt hier tegen privacybescherming, omdat de samenleving veel controle en veiligheid wil.

Beide vormen van veiligheid hebben te maken met het technisch ontwerp van het systeem, dus met een vroeg stadium van de besluitvorming.

Technisch ontwerp en grondrechten:

De eigenschap van een op ICT gebaseerde samenleving is dat fundamentele normatieve vragen die vrijheid van

communicatie en individuele privacy (zoals verwoord door Westin) raken, verweven zijn geraakt met de onderliggende IC technologie: we noemen dat tegenwoordig de 'computational turn' van de samenleving.²⁷ De beperking van de vrijheid zit steeds meer ingebakken in het technisch ontwerp. Waar wij ons vroeger op de 'informatielaag' concentreerden, moeten we ons voor het beschermen van de fundamentele rechten die bij informatieoverdracht en informatieopslag spelen, steeds meer op de onderliggende 'technische' lagen richten.²⁸

Iedereen is het er daarom over eens dat je in de ontwerpfase een heldere afweging moet maken tussen veiligheid en privacy. Iedereen: dat zijn de Europese en nationale toezichhouders, het Rathenau Instituut, de WRR en zelfs de Algemene Rekenkamer.²⁹ Als het gaat om systeemveiligheid, kan keuze voor de techniek en de vorm van groot belang zijn.

De beperking van de vrijheid zit steeds meer ingebakken in het technisch ontwerp

Bij privacy is de technische ontwerpfase ('privacy by design') ook van steeds groter belang. Dan gaat het immers om het (kunnen) anonimiseren van de handelingen van de gebruikers (bijvoorbeeld bij rekeningrijden met auto's en openbaar vervoer), transparantie en verantwoordelijkheid, die ook op systeemniveau gerealiseerd moeten kunnen worden. De politieke druk maatschappelijke veiligheid de voorrang te geven is groot. De maatschappelijke druk werkt hier dus tegen privacybescherming.

Keuzevrijheid; het recht om vergeten te worden

Keuzevrijheid

Het WRR-rapport noemt keuzevrijheid een van de ankers, maar relateert tegelijk de betekenis ervan, omdat de complexiteit van de samenleving het maken van keuzen door eenvoudige burgers niet bevordert. Wel noemt de Raad de kritische consument als parameter.³⁰ In het

14. *iOverheid*, p. 57.

15. James C. Scott *Seeing like a state, How certain schemes to improve the Human Condition Have Failed*, New Haven and London: Yale University Press 1998. Zie ook E.J. Dommering, *Gevangen in de waarneming*, Amsterdam: Otto Cramwinckel 2008.

16. F. Kuitenbrouwer, *Wanneer computers koppelen...*, (oratie Belle van Zuylen), Deventer: Kluwer 1990, p. 8.

17. *Databases. Over ICT beloftes, informatiehonger en digitale autonomie*. Den Haag: Rathenau instituut 2010, p. 16.

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

19. Het Europese actieplan inzake e-overheid 2011-2015. Mededeling van de Commissie aan het Europese Parlement, COM(2010)734, p. 6 en 10.

20. Zie de casestudy van James B. Rule, *Private Life and Public Surveillance*, New York: Shocken Books 1974, p.271 e.v.

21. H. Boutellier, *De veiligheidsutopie*, Den Haag: Boom Juridische uitgeverij 2002.

22. *iOverheid*, p. 77-78.

23. Het probleem van het geringe aantal 'deviants' in een massale controle werd al geanalyseerd door James Rule a.w., noot 19, p. 287 e.v.

24. *Het Financieel Dagblad* 19 november 2011, p. 22, 'Goeden van kwaden scheiden'.

25. Brieven van de Minister van Binnenlandse Zaken van 5 en 16 september 2011, 26 643, nr. 188 en 189.

26. F. Kuitenbrouwer 'De privacy voorbij', in: *Computerrecht* 2009/3, p. 99.

27. De term werd gemunt in Ch. Esser & R.

Hagengruber (eds.), *The Computational Turn*, Münster: Monenstein und Vannerdat 2011.

28. Zie voor een heldere analyse van het probleem: *Information and communication Technologies and human rights*, Brussel: Directorate-General for external policies of the Union 2010.

29. Zie De Expertmeeting van 20 maart 2011, *Kamerstukken I* 2010/11, 301 051, nr. B.

30. *iOverheid*, p. 80.

begrip keuzevrijheid bevinden we ons inderdaad op het snijpunt van de staatsburger en de consument, overheid en markt. Een vrije keuze hangt samen met het beschikken over voldoende informatie. De consument die in de relatie tot het bestuur moet kunnen kiezen, krijgt die keuze vaak niet, omdat hij niet op een eenvoudige en beknopte manier geïnformeerd wordt waarom de gevraagde persoonsgegevens nodig zijn en waarvoor ze worden gebruikt. Bovendien wordt hij als regel gedwongen om persoonsgegevens af te geven om de overheidsdienst geleverd te kunnen krijgen. Op de markt is het nog erger. Vrolijk neemt de burger allerlei zogenoemde gratis diensten af, en stort hij zich net 'huid en haar' in sociale netwerken. Om de burger keuzevrijheid te geven, moet hij het besef krijgen dat de persoonsgegevens 'van hem' zijn en economische waarde hebben, zodat hij bewust van wat hij 'prijs geeft' in informatietransacties kan stappen.³³ Anonimiteit is een andere grens. De vraag moet zijn of de burger/consument zich voor iedere economische of bestuurlijke transactie steeds moet identificeren.

Recht op vergetelheid

De Raad noemt in navolging van de voorstudie van Buruma³² het belang om vergeten te worden als versterking van de rechten van de consument op: de gebruiker moet van bepaalde elektronische schaduwen die hem dwars zitten, kunnen worden verlost. De gedachte is ooit gelanceerd door Viktor Mayer-Schönberger in zijn boek uit 2009 *Delete*.³³ Ik heb ook wel eens een recht geopperd om met een schone lei te kunnen beginnen: een *tabula rasa*-recht.³⁴ Hoe langer ik erover nadenk hoe complexer ik vergetelheid als recht vind. Voor heel veel technische systemen kun je je nog een 'privacy by default' (privacy is de regel) voorstellen, waarbij je na ommekomst van een termijn automatisch uit het systeem wordt verwijderd of eerst toestemming moet geven om erin te worden opgenomen. Veel ingewikkelder is dat met registers en archieven die historische waarde hebben. In het kader van perszaken is de vraag al gerezen of je bij een rectificatie het recht hebt van internet te worden verwijderd. Het privacyrecht moet dan worden afgewogen tegen het recht en belang dat de geschiedenis niet herschreven wordt.³⁵ Als er niet al vroeg in onze geschiedenis registers werden bijgehouden zouden we van heel veel belangrijke historische feiten of personen minder weten. Zonder politieregisters zouden we van de schilder Caravaggio nagenoeg niets weten. Holocaust-delicten zijn een verbod op vergeten.

Mayer-Schönberger neemt als vertrekpunt van zijn beschouwingen dat herinneren – ook op cognitief niveau – bestaat uit twee componenten: opslag en vindbaarheid. Beide zijn zo goedkoop geworden dat alle informatie opgeslagen en vindbaar blijft. Afgezien van een regeling van bewaartermijnen, valt daarom ook te denken aan een duidelijker scheiding tussen de archief functie en de zoekfunctie. Moeten archieven drempelloos ten eeuwigste online blijven? Je zou na een zekere tijd gekwalificeerde toegang kunnen inbouwen (met daarnaast de open papieren toegang).

De WRR en ook de Europese Commissie zijn voor vergeten geporteerd. De WRR ziet echter het probleem om het als een *recht* te definiëren, omdat ook de historische integriteit van registers in het geding is. Corien Prins bepleit

een aanscherping van art. 36 Wbp dat weliswaar een verwijderrecht kent, maar dat moeilijk is te effectueren.³⁶

De verantwoordelijkheid van de overheid voor de samenleving

In een voorstudie had De Hert de verantwoordelijkheid van wat er op ICT in de samenleving gebeurt herleid tot de positieve verdragsverplichting van de staat onder art. 8 EVRM de naleving van dit grondrecht ook in horizontale verhoudingen te waarborgen.³⁷ De richtinggevende arresten zijn *KU/Finland*³⁸ en meer recent de beslissing in de zaak *Köpke*.³⁹ De minister verschuilt zich in zijn reactie op het rapport achter het internationale karakter van de informatiesamenleving om de verantwoordelijkheid van de Nederlandse Staat te relativeren.⁴⁰ Dit is niet de benadering van het EHRM. Dit onderzoekt met name of voor privacyinbreuken in de private sfeer wel een voldoende wettelijke grondslag bestaat. De ICT-samenleving vergroot de verantwoordelijkheid. In de *Köpke*-beslissing stelt het Hof:

In het begrip keuzevrijheid bevinden we ons op het snijpunt van de staatsburger en de consument, overheid en markt

'The competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies.'

Structurele en afdwingbare controlemechanismen; de reactie van de regering op het WRR-rapport

Zowel WRR als het Rathenau Instituut bepleit een structurele aanpak. Beide denken aan een nieuwe autoriteit, maar dat voorstel ontving van de regering en tijdens de expertdiscussie in de Eerste Kamer weinig bijval.⁴¹ Los van het mechanisme: het gaat eigenlijk om een voortgezette machtscheiding binnen de uitvoerende macht om tot een herstel van het evenwicht tussen de machten onderling en tussen overheid en burger te komen.

In het kabinetsstandpunt over het WRR-rapport volstaat de regering met het bepleiten van een 'bewustwordingsproces'. Zij verwijst daartoe naar bestaande bestuurlijke praktijken. Hoewel er al veel gebeurt, lijkt het mij toch te weinig. De bestaande controlemechanismen zijn toegesneden op inspraak in de inhoud van de wetgeving en een politieke controle op afstand op de inhoud van gedelegeerde wetgeving. Het gaat er nu juist om dat steeds vaker aan wetgeving een ICT-instrument hangt dat ingrijpender gevolgen voor de burger kan hebben dan de inhoud van de regelgeving zelf. Zoals Mireille Hildebrandt het in haar oratie verwoordde:

'Het realiseren van de rechtsstaat in cyberspace vraagt om heroriëntatie op de manier waarop de rechts-

staat bestaat: geschreven recht zal niet altijd volstaan'.⁴²

De regering is na de reactie op het WRR-rapport toch iets verder gegaan. In de brief van 15 november 2011 waarin het de 'I-strategie' van het Rijk voor de komende jaren presenteert, gaat het aanvankelijk vooral over verbetering van systeemveiligheid en stroomlijning van automatiseringsprocessen, maar op p. 9 wordt voorgesteld om in de projectplannen voor ICT een *Privacy Impact Assessment* (PIA) op te nemen als onderdeel van de omschrijving van het risicoprofiel van het project.⁴³ De al bestaande Chief Information Officers (die vooral over de technische kant gingen) zullen een uitbreiding van hun takenpakket krijgen. Maar zal dat genoeg zijn? Is het meer dan nu al staat in de Aanwijzingen 161 en 162 voor de Regelgeving (die een motiveringsplicht opleggen als regelgeving implicaties heeft voor informatievoorziening en gegevensverwerking)? Waarom niet expliciet vastleggen dat een PIA moet gaan over doelbinding en de subsidiariteit en proportionaliteitsbeginselen van art. 8 EVRM?⁴⁴ En waarom geen evaluatieplicht van een systeem dat er enige tijd staat? De functie kruipt immers waar zij niet gaan kan.

De regering heeft in de reactie op het WRR-rapport ook een transparantieverkenning (gereed medio 2012) aangekondigd, die moet leiden tot versterking van de inzage- en correctierechten van de burger.⁴⁵ Maar wat zij als verkenning aankondigt, is mijns inziens niet meer dan reeds *als recht* uit de Wbp volgt. De verkenning beoogt alleen het aanbod van functionaliteiten te vergroten die de uitoefening van dit recht moeten vergemakkelijken. Dat kan feitelijk natuurlijk winst opleveren. De veel radicalere voorstellen van het Rathenau Instituut om feitelijke maatregelen te nemen die mogelijk moeten maken dat de burger zelf beheer over zijn gegevens krijgt ('identi-

Wat de regering als verkenning aankondigt is niet meer dan reeds als recht uit de Wbp volgt

teitsbeheer'), zie ik daarin niet terug, eerder een mogelijkheid het delen van gegevens te vergemakkelijken.

Slot

De WRR heeft in het rapport *i-Overheid* en de daarmee verbonden voorstudies een belangrijk onderwerp op de agenda gezet. Het Rathenau Instituut is hem daarin in 2010 voorgegaan met het rapport *Databases. Over ICT beloftes, informatiehonger en digitale autonomie*. ICT is een instrument waarmee de nationale en Europese bestuurlijke bureaucratieën en organisaties in het middenveld steeds meer macht over de burgers krijgen, maar ook steeds meer privacyrisico's creëren. ICT is niet een 'neutraal' instrument, maar een instrument dat een voortgaande verschuiving van de macht richting bestuur binnen de trias politica versterkt, en het bestuur allengs dichterbij de burger brengt met vermindering van het speelveld van diens grondrechten.⁴⁶ Die ICT-systemen hebben allemaal afkortingen: SIS, SPOCS, EPD, KPD enzovoort. Laten we niet vergeten dat dictaturen dol zijn op afkortingen. Het zijn afdelingen die de burgers 'besturen' en 'controleren' en daar houden dictaturen van.

De reactie in porties van de regering op dit WRR-rapport is wel een stap vooruit, maar toch te licht in relatie tot de urgentie van het vraagstuk. Welke macht zal daar nog eens een flinke duw tegen geven? •

31. E.J. Dommering, 'Recht op persoonsgegevens als zelfbeschikkingsrecht', in: Corien Prins e.a. (red.) '16 miljoen BN'ers? Bescherming van persoonsgegevens in het Digitale Tijdperk.', Leiden: NJCM-Boekerij (47) 2010, p. 83-99.

32. 'Het recht op vergetelheid. Politieke en justitiële gegevens in een digitale wereld', in: WRR verkenning nr. 25 *De staat van informatie*, Amsterdam: Amsterdam University Press 2011, p. 165-219.

33. Viktor Mayer-Schönberger, *Delete, The Virtue of forgetting in the Digital Age*, Princeton and Oxford: Princeton University

Press 2009.

34. E.J. Dommering, 'Ik surf, dus ik ben (er geweest)', in: Karin Spaink (red.) *Wie is U?*, Amsterdam: Nijgh & Van Ditmar/XS4All 2010, p. 56.

35. De zaak *Times/UK*, EHRM 10 maart 2009, appl.nr. 23676/03, NJ 2010/109, m.nt. E.J. Dommering.

36. C. Prins, 'Reen recht op vergeten. Vergeet het maar,' in: AA november 2011, p. 774-775.

37. P. de Hert, 'Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechtenverplichting', in:

De staat van informatie, Amsterdam: Amsterdam University Press 2011, p. 33-75.

38. *K.U./Finland* (EHRM 2 december 2008, appl.nr. 2872/02, NJ 2009/470, m.nt. E.A. Alkema).

39. Ontvankelijkheidsbeslissing: EHRM 5 oktober 2010, appl.nr. 420/07, NJ 2011/566, m.nt. E.J. Dommering.

40. Brief van 25 oktober 2011 (*Kamerstukken II* 2010/11, 26 643, nr. 211), p. 4.

41. A.w. noot 38, p. 10; zie ook de Expertmeeting van 20 maart 2011, *Kamerstukken I* 2010/11, 301 051, nr. B.

42. M. Hildebrandt, *De Rechtsstaat in cyberspace*, Nijmegen: Radboud Universiteit 2011, p. 23.

43. *Kamerstukken II* 2011/12, 26 643, nr. 216, p. 9.

44. In de kabinetsreactie op de WRR werd de PIA op p. 9 al genoemd onder verwijzing naar de motie Franken *Kamerstukken I* 2010/11, 31 051, nr. D. De PIA is beperkt tot effectrapportage.

45. Kabinetsstandpunt, p. 11-12.

46. *iOverheid*, p. 106.