

Corien Prins en Dennis Broeders

De iSamenleving de maat meten

over de consequenties van het WRR-rapport
voor de informatie-samenleving

1. In de beperking toont zich de meester

Een willekeurige dag, juni 2011. De ochtendbladen melden dat het kinderlijk eenvoudig is via de website van de Dienst Uitvoering Onderwijs (DUO, voorheen: IB-groep) privégegevens van studenten te stelen. Ook blijkt het mogelijk, gebruik makend van het feit dat oud-studenten een studieschuld moeten aflossen, hen geld afhandig te maken via het betalingssysteem iDeal. Zoals eerder bij de ov-chipkaart, blijkt een beveiligingslek de boosdoener. Het voorbeeld illustreert wederom de kwetsbare kanten van digitalisering, ditmaal het lekken van grote hoeveelheden persoonsgegevens. Maar dat toont het niet alleen. Evenzeer laat het zien hoe digitale diensten van de overheid (in dit geval die van DUO) zijn verweven met die van de private sector (het online betalingssysteem iDeal).

Een andere willekeurige dag, december 2020. Via diverse sociale media verspreidt zich het nieuws dat de Europese wetgever heeft besloten stringente voorwaarden te stellen aan het gebruik door de private sector van consumentprofielen die zijn opgesteld aan de hand van informatie over de genetische predispositie van individuen. De laatste jaren bleken niet alleen verzekeraars, maar ook werkgevers in een toenemend aantal situaties gebruik te maken van dergelijke profielen (premiëdifferentiatie bij arbeidsongeschiktheidsverzekeringen, aannemen van personeel, et cetera). De noodzakelijke informatie wisten de bedrijven veelal te achterhalen via hun al dan niet nauwe contacten met online diensten die zich begeven op de markt voor het voorspellen van – aanleg tot – ziekten aan de hand van genetisch materiaal. Consumenten behoeven bij deze diensten enkel wat wangslim afgewomen met een wattenstaafje op te sturen om enkele weken later een volledig genetisch profiel en melding van de daarmee verband houdende risicofactoren te ontvangen. De Europese Commissie is van mening dat sprake is van een ongezonde ontwikkeling en gaat paal en perk stellen aan het verwerven en uitwisselen van genetische informatie door de private sector alsmede het werken met informatie die is gebaseerd op dergelijke profielen. Ook volgen forse boetes bij overtreding van de regels.

De twee voorbeelden uit heden en toekomst vertonen in veel opzichten sterke overeenkomsten. Beide laten zien dat in de informatiesamenleving schotten steeds diffuser worden. Op een digitaal niveau is sprake van een toenemende verwevenheid tussen allerhande partijen en sectoren. Op een informatieniveau valt de grens tussen de publieke sector en de private sector nauwelijks meer te ontwaren (voorbeeld 1). Op een informatieniveau lijkt het lang gekoesterde uitgangspunt van doelbinding uit de Wet bescherming persoonsgegevens (Wbp) nog slechts een papieren tijger (voorbeeld 2). Het is deze verwevenheid van informatiestromen die toont tot welk een complex samenstel de informatiehuishouding van onze samenleving inmiddels is uitgegroeid.

De twee voorbeelden verschillen echter in één belangrijk opzicht: *grenzen durven te stellen*. Waar in 2011 op politiek en bestuurlijk niveau nauwelijks iemand wakker bleek te liggen van de kwetsbare verwevenheid die het DUO-voorval toonde, is dat besef er in 2020 wel degelijk en is de Europese Commissie bereid met strenge maatregelen te komen om de noodzakelijke digitale grenzen te stellen en, belangrijk, deze ook te bewaken.

De constatering dat digitalisering een totaal andere, te weten vernetwerkte informatieomgeving heeft gecreëerd, geeft alle aanleiding om het complexe karakter van de iSamenleving te doordenken en op zoek te gaan naar aanknopingspunten voor een andere wijze waarop organisaties zich tot de nieuwe realiteit kunnen en hebben te verhouden. Hoe paradoxaal het ook moge klinken, deze aanknopingspunten lijken gezocht te moeten worden in *beredeneerde begrenzingen van digitalisering*. Niet in de laatste plaats om actoren binnen de iSamenleving houvast te geven in het bepalen van wat een juiste omgang is met informatie en het delen daarvan met andere partijen.

Dat is nu vaak onbepaald. Vermenging van informatiestromen, onder meer tussen publiek en privaat, is ongemerkt heel gewoon geworden. Maar bij nadere beschouwing (en zoals we in paragraaf twee nader zullen bespreken), blijkt deze vermenging ook z'n problematische kanten te kennen. Vanuit deze constatering beoogt dit hoofdstuk een aanzet te geven voor de wijze waarop de iSamenleving zich in 2020 zou moeten verhouden tot digitalisering.

Centrale noemer anno 2020 is wat ons betreft, nogmaals, *begrenzing*. Niet langer is dan de huidige digitale grenzeloosheid leidend. Begrenzing zal uiteindelijk wezenlijk blijken te zijn, zowel omwille van de kwaliteit van individuele informatiehuishoudingen als de zorgvuldigheid van de informatieprocessen die deze huishoudingen tot een omvattende iSamenleving met elkaar verbinden. Het denken over begrenzing resulteert over een decennium in een hernieuwde *balans* tussen informatie-vrijheid, geheimhouding en beveiliging. Sommige informatie wordt dan helemaal niet meer opgeslagen of gebruikt, andere informatiebronnen zijn juist transparanter in plaats van vertrouwelijk en geheim, en sommige informatie is veel beter beveiligd. En daar waar actoren in de iSamenleving de verantwoordelijkheid voor het stellen van grenzen onvoldoende oppakken, is het de overheid die vanuit een soort van restverantwoordelijkheid de grenzen soms alsnog blijkt te stellen. En, zoals voorbeeld 2 ons als toekomstbeeld toont, ook bereid is het overschrijden van deze grenzen te sanctioneren met flinke boetes (vergelijkbaar met de boetes die de Europese Commissie in het verleden voor het verstoren van marktwerking heeft opgelegd).

Wat exact blijken de komende jaren de belangrijke motieven om van het huidige klimaat van vrijwel onbegrensde digitaliseringsslagen over te stappen op het besef dat begrenzing soms noodzakelijk is? Nadat paragraaf 2 allereerst kort de kwetsbare kanten van de toenemende verwevenheid heeft neergezet, schetst paragraaf 3 de omslag en duidt het belang van begrenzing nader. Paragraaf 4 brengt vervolgens aan het licht om welke redenen exact de Europese Commissie in 2020 besluit in te grijpen en vanuit haar systeemverantwoordelijkheid zelf de grenzen gaat stellen omdat blijkt dat ten aanzien van genetische informatie marktpartijen – de samenleving – het belang van begrenzing niet of onvoldoende zelf oppakken.

2. Kwetsbare verwevenheden

Anno 2011 gaan veel instanties zowel binnen de overheid als in de private sector nog immer van de veronderstelling uit dat het met de eigen informatiehuishouding gaat om een semigesloten systeem in plaats van een volledig open systeem zoals het Internet. Anders gezegd, men handelt vanuit de assumptie zelf nog het heft in handen te hebben en voor 100% te kunnen sturen op de eigen informatiestromen. Beide voorbeelden laten echter goed zien dat die *maakbaarheid* en *stuurbaarheid* van informatieprocessen onder druk zijn komen te staan. Zowel het vernetwerken van informatie als het laten vervloeien van informatiestromen over de grenzen van het publiek-private heen, maken dat de semigesloten informatiehuishouding van individuele instanties *intern* steeds meer op het Internet gaat lijken. Informatie is meer en meer van iedereen, in plaats van toebehorend aan één organisatie. Dat betekent ook dat het in goede banen leiden van informatiestromen binnen individuele organisaties op dezelfde grenzen stuit als binnen het model van het Internet. Naarmate die ontwikkeling zich doorzet, wordt het problematischer voor de samenleving als geheel om informatie te kanaliseren, te verifiëren en voor de betrouwbaarheid in te staan.

Behalve het risico dat de internetlogica bij individuele organisaties 'naar binnen slaat,' wijst het genoemde voorbeeld van DUO op een tweede risico, namelijk dat (semi-)gesloten systemen ongewild deel worden van het Internet. Illustratief is de WikiLeaks-affaire, zoals die in het najaar

van 2010 in alle hevigheid losbarstte en als een voorbode kan gelden van wat in de toekomst ongetwijfeld vaker gebeurt. Door WikiLeaks kwam de interne informatiehuishouding van overheden ineens digitaal op straat te liggen: oncontroleerbaar door het vele kopiëren en de snelle migratie van de informatie van server naar server, van cloud naar cloud. Alleen Chinese methoden zouden de geest wellicht terug in de fles kunnen krijgen, maar zelfs dat is de vraag. Om van wenselijkheid daarvan nog maar te zwijgen.

Voordat een 'lek' van overheidsinformatie gebeurt, is het risico veelal beschouwd als een kwestie van beveiliging van data en van techniek en beleid om dat te bewerkstelligen. Zodra een lek resulteert in het verspreiden van gevoelige informatie op het Internet, is er echter geen beleid meer voorhanden, gaan instanties improviseren om de controle terug te winnen, wat uiteindelijk veelal een weinig verheffende aanblik biedt. Toch zijn dergelijke lekken juist door digitalisering nagenoeg onvermijdelijk (in feite inherent aan de technologie) en laat ook het voorbeeld van DUO zien hoe kinderlijk eenvoudig het blijkt te zijn om de interne informatiehuishouding van individuele organisaties ineens publiekelijk te dumpen.

3. Begrenzing anno 2020

In 2020 toont de Europese Commissie duidelijk dat ze bereid en in staat is grenzen te stellen aan het groeiende gebruik van informatie en profielen alsmede de toenemende verwevenheid van informatiestromen. De noodzaak tot het stellen van dergelijke grenzen werd ook reeds in 2011 op de agenda gezet. In dat jaar bood de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) het rapport *iOverheid* aan de regering aan. Het rapport handelt over de inzet van ict-applicaties door de overheid en concludeert dat met deze inzet een achterliggend complex geheel van informatiestromen is ontstaan waar politiek en bestuur zich ogenschijnlijk niet of nauwelijks van bewust lijkt te zijn. Deze onbewuste *iOverheid*, die eerder in de praktijk is ontstaan dan dat deze door de overheid is ontworpen, heeft de natuurlijke neiging om onbekommerd door te groeien. *Grenzen aan de groei* komen pas in zicht als er zich een bewustzijn ontwikkelt van wat die *iOverheid* is en doet. Zo ook ontwikkelt de samenleving zich met een grootschalige en welhaast allesomvattende inzet van ontelbare digitaliseringsinitiatieven tot een *iSamenleving*.

In vergelijking met de *iOverheid* is deze *iSamenleving* nog veel grenzenlozer. De *iSamenleving* is een conglomeraat van ongelijksoortige actoren die met elkaar in vernetwerkte verhoudingen staan en waartussen informatie rijkelijk vloeit en vermengt: burgers, overheden, NGO's, media, bedrijven, sociale media, cybercriminelen, et cetera. Waar men zich in 2011 nog verbaast over de snelle ontwikkelingen op het gebied van de informatisering – de komeetachtige opkomst van Facebook (die en passant de Nederlandse variant Hyves leegzoo), de reeds genoemde Wikileaks-affaire die overheden in grote verlegenheid bracht, de snelle tamtam via sociale media die een RIVM vaccinatieprogramma deed mislukken en de manier waarop YouTube and Twitter carrières maakten en braken – zal 2020 nog veel meer in petto hebben. Het voorbeeld van het benutten en uitnutten van genetische informatie is daar slechts een kleine illustratie van. Het merendeel zullen we niet hebben zien aankomen.

Hoewel het meeste dat de revue passeert in de *iSamenleving* de overheid in eerste instantie niet aangaat, moet de overheid meer dan ooit nadenken over waar zij haar rol als begrenzer dient te spelen. Centrale regie is onmogelijk in de geïnformatiseerde netwerksamenleving van 2011, laat staan die van 2020, maar de idee dat overheden niets meer vermogen in een informatiesamenleving is voor beide jaren eveneens een naïef beeld. In het rapport *iOverheid* benadrukt de WRR een aantal punten waarop de overheid scherp zou moeten letten om de eigen informatiseringambities op een goede

manier vorm te geven. Een aantal van deze punten is ook van groot belang om te bepalen wanneer begrenzings in de iSamenleving in beeld moeten komen. Uiteraard zijn de afwegingen voor de overheid zelf enerzijds en de afwegingen voor de vrije markt en samenleving als geheel anderzijds niet hetzelfde. Het gaat eerder om *informatieordening* in de zin van marktordening; net als de markt is informatisering een autonome kracht en de informatiesamenleving een vrije sfeer die toch, en om goede redenen, begrensd en bijgestuurd wordt door overheden.

In de eerste plaats moet bij nieuwe ontwikkelingen goed nagedacht worden of verschillende belangen en beginselen voldoende met elkaar in evenwicht zijn. De WRR introduceert voor het zoeken naar dit evenwicht drie clusters van beginselen: drijvende, verankerende en procesmatige beginselen. Deze drie zullen met elkaar in evenwicht gebracht dienen te worden als het gaat om overheidsinformatisering. Daarbij zal de overheid soms andere partijen de maat moeten nemen om burgers en bedrijven te beschermen. Zo is winstmaximalisatie een *drijvende* kracht voor bedrijven. Daar is ook in een informatiesamenleving in het geheel niets mis mee, vooropgezet dat ook *verankerende* beginselen als privacy en keuzevrijheid gewaarborgd zijn. Een bedrijf als Facebook dat de persoonsgegevens van zijn gebruikers als grondstof heeft, had geen gebrek aan een privacy-beleid maar stopte het zo ver weg in de kleine lettertjes die na elke update opnieuw beoordeeld moesten worden dat *procesmatige* beginselen als transparantie alleen op 'papier' maar niet in de dagelijkse digitale praktijk van haar gebruikers recht werd gedaan. Gegevensbeschermingsautoriteiten en de Europese Commissie volgden op dit punt Facebook in 2010 dan ook met argusogen en kritiek.

In het WRR-rapport zijn ook drie waarschuwingsvlaggen gehesen die te maken hebben met de kwaliteit van informatie. Daarbij ging het niet om de soort informatie – er zijn voldoende kaders die bepalen hoe bepaalde vormen van persoonsinformatie beschermd moet worden – maar om de processen van informatieverwerking en gebruik. Een drietal processen heeft een grote invloed op de kwaliteit van informatie die op zijn beurt weer bepalend is voor de mogelijkheden en moeilijkheden voor burgers en bedrijven in de informatiesamenleving. Processen die we ook terugzien in de twee voorbeelden waarmee dit hoofdstuk begint. In de eerste plaats het *vernetwerken* van informatie, ofwel het gezamenlijk gebruik en beheer van informatie in een netwerk. Daarnaast gaat het om *samenstellen* en verrijken van informatie in digitale profielen. En als derde gaat het om *preventief* en proactief handelen op basis van risicocalculatie, profilering en datamining. Tot op zekere hoogte zijn deze ontwikkelingen belangrijke pijlers onder het gemak en het plezier van de informatiesamenleving; innovatie en function creep zijn naaste familie van elkaar. Het kan heel prettig zijn als amazon.com je op basis van je eigen koopgedrag en de gegevens van alle andere klanten boeken aanraadt. Dat Amazon die gegevens verkoopt aan andere bedrijven die ze opnemen in hun eigen profilering is ook niet per se een probleem. Toch wil je ook weer niet dat je gegevens overal terecht komen, of dat je afgerekend wordt op een profiel. Zeker niet als die gegevens informatie opleveren over de genetische predispositie van individuen en deze individuen daardoor van een bepaalde verzekering worden uitgesloten. Daarin is een bedrijf dat boeken verkoopt toch weer heel iets anders dan een verzekeraar of werkgever.

Juist met het oog op deze toenemende vernetwerking en daarmee welhaast onstuurbare verspreiding van informatie is begrenzing in de tijd van groot belang. Tot in de eeuwigheid herinnerd worden is in de informatiesamenleving niet langer voorbehouden aan beroemdheden. De informatiesamenleving heeft een goed geheugen, soms tot onze schade en schande zelfs een te goed geheugen. Veel wordt onthouden en opgeslagen, hoewel dat vaak niet geldt voor de context waarin zaken zich afspeelden.

Feit is wel dat het verleden vaak meespeelt in de manier waarop mensen nu benaderd worden, zowel in de digitale wereld van de dataprofielen als in de echte wereld. Vergeten is uitzonderlijk geworden op het web en in private en publieke databestanden (Buruma, 2011). Formele, wettelijk vastgelegde bewaartermijnen blijken in de regel in de dagelijkse praktijk niet of nauwelijks in acht te worden genomen. En soms staat de techniek zelf het vergeten in de weg; sommige technische systemen, zoals relationele databases, zijn zo ingericht dat absolute en volledige verwijdering van gegevens het systeem welhaast als een kaartenhuis in elkaar doet storten. Kortom, verwijderen is niet slechts een kwestie van op enig moment eens een keer stilstaan bij het weggooien van gegevens, maar zeker ook een aandachtspunt bij het ontwerpen en bouwen van systemen. In feite is het een kwestie van *privacy by design*, het in de techniek verdisconteren van gegevensbescherming, een optie die door de Tweede Kamer al ruim 10 jaar geleden enthousiast is omarmd, maar in de praktijk nauwelijks wordt ingevoerd.

Tenslotte zal het duidelijk zijn dat de ontwikkelingen ook eisen stellen aan het digitale individu, nu en zeker in 2020. Die zal zorgvuldiger met zijn digitale identiteit om moeten gaan en zich minder snel moeten laten verleiden om persoonsinformatie weg te geven, al dan niet in ruil voor een voordeel. Grenzen stellen is soms ook een collectieve mogelijkheid en verantwoordelijkheid: Facebook-gebruikers hebben het bedrijf meerdere malen wijzigingen in het privacybeleid terug laten draaien. Soms is het echter ook de overheid die grenzen moet stellen en daarbij de bovenstaande ontwikkelingen moet meewegen. Het is dan zaak om de juiste strijd aan te gaan op het juiste niveau en een duidelijk voorbeeld te stellen, niet in de laatste plaats omdat echte regie in de weidse uitgestrektheid van de informatiesamenleving geen optie is. In 2010/2011 was dat de Europese Commissie die – uit naam van jonge kinderen – het privacybeleid van Facebook onder de loep nam. In 2020 zullen de grote innovatoren van de informatiesamenleving andere namen hebben en nieuwe manieren gevonden hebben om informatie voor zich te laten werken. Maar ook dan zullen grenzen bepaald moeten worden door een evenwichtige weg van beginselen, een realistische kijk op de kwaliteit van informatie en het belang van vergeten.

4. Systeemverantwoordelijkheid anno 2020

Maar wat als bedrijven hun eigen verantwoordelijkheid toch niet op blijken te pakken? Vanuit de fundamenteën van onze rechtsstaat, rust ons inziens dan ten principale bij de overheid een zekere verantwoordelijkheid voor het functioneren van de iSamenleving. De overheid moet immers opkomen voor haar burgers wanneer private partijen het belang van deze burgers onvoldoende garanderen. Deze bredere verantwoordelijkheid voor de iSamenleving is in de volgende vragen te vatten: Wat dient de overheid zich in de ontwikkeling van de informatiesamenleving aan te trekken, en (hoe) heeft zij daarin te interveniëren?

Aan het begin van dit millennium kaartte toenmalig premier Kok de kwestie al eens aan in een toespraak op het Infodrome-congres op 11 april 2001:

Toch moeten wij ons thans de vraag stellen welke verantwoordelijkheden, in de jaren die voor ons liggen, op de weg van de overheid komen in verband met aan de informatiesamenleving inherente gevolgen.

Deze verantwoordelijkheid kan worden gedefinieerd als de systeemverantwoordelijkheid van de overheid voor de iSamenleving. Uiteraard zijn de interventies in de iSamenleving altijd politiek gekleurd en omstreden, maar er kan toch worden geprobeerd een soort *common ground* te formuleren

voor de aspecten, onderwerpen e.d. waarvoor een overheid garant staat. En een van de zaken waar ze verantwoordelijk voor heeft te staan is, daar waar nodig, *het stellen van grenzen* aan digitalisering dan wel het faciliteren dat deze grenzen worden gesteld.

De noodzaak tot handelen op basis van systeemverantwoordelijkheid tekent zich anno 2011 reeds af. De groeiende informatiemacht van mondiale spelers als Google, Facebook en Apple stelt de (Europese) overheid voor de vraag of en op welke wijze deze macht om redenen van publieke belangen beteugeld dient te worden. Op een aantal dossiers zijn de eerste bewegingen in die richting gezet. Voormalig minister van Economische Zaken, Van der Hoeven, deed in reactie op Kamervragen begin augustus 2010 de toezegging het College Bescherming Persoonsgegevens (CBP) te vragen om een nieuwe clause in de privacyvoorwaarden van Apple te beoordelen.¹ Illustratief is ook de opvatting van het Ministerie van Justitie over de toepassing van biometrie in de private sector (Ministerie van Justitie, 2010, p. 33):

de aspecten waar de overheid rekening mee houdt ten aanzien van biometrie in de publieke sector kan zij ook van toepassing verklaren op de private sector in haar rol als beschermer van de belangen van de burger en de maatschappij.

Overigens zullen lang niet alle kwesties die aan de systeemverantwoordelijkheid van de overheid raken, op nationaal niveau geadresseerd kunnen worden. Inmiddels wordt ook gesproken over een Europese actor die op het hogere niveau de noodzakelijke massa en doorzettingsmacht kan genereren.² Illustratief is hier de mededeling van Europees commissaris Kroes dat het toezicht op *social networking sites* en de daarin gehanteerde *privacy settings* verscherpt gaat worden, in het bijzonder waar het gaat om jeugdigen (Kroes, 2010). Burgers moeten in bescherming worden genomen tegen een agressieve en competitieve informatiemarkt, zo lijkt de teneur.

Maar systeemverantwoordelijkheid voor de grenzen van de iSamenleving kan niet alleen aan de orde zijn wanneer burgers beschermd moeten worden. Ook kan de overheid grenzen hebben te stellen wanneer ontwikkelingen in het private domein te zeer interfereren met (vitaal) beleid van de overheid. Anno 2011 zijn illustratief de ontwikkelingen op het terrein van identiteitsmanagement. De overheid investeert veel in digitale middelen om de identiteit van burgers vast te stellen, bijvoorbeeld via applicaties als het (biometrisch) paspoort, DigiD en mogelijk in de toekomst het eRijbewijs. Juist omdat de overheid veel investeert in die identiteitsbepaling – en de accuraatheid daarvan claimt – moet ze ook aandacht hebben voor identiteitsbepaling in het semipublieke en commerciële domein, in het bijzonder voor de risico's op verwatering van de kwaliteit daarvan. Het voorbeeld waarmee we deze bijdrage begonnen – het gebruik van iDeal door studenten voor het aflossen van studieschuld – is wederom illustratief. Maar er zijn meer voorbeelden te geven. Wat was bijvoorbeeld de waarde geweest van een streng beveiligde centrale opslag van biometrische gegevens in het kader van de Paspoortwet, als dezelfde gegevens ook buiten het domein van de overheid breed beschikbaar zijn? De invoering van een biometrisch paspoort roept vragen op over het gebruik van biometrie in de private sector. Momenteel is nauwelijks sprake van regulering of zelfs maar politieke aandacht en experimenteren zwembaden, supermarkten, werkgevers en computerfabrikanten volop

¹ Brief van Minister van Economische Zaken, beantwoording vragen over nieuwe clause in de privacyvoorwaarden van Apple, 3 augustus 2010.

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

met nieuwe toepassingen van deze technologie. Vanwege de enorme toename van verzamelde informatie worden identificaties ook buiten de overheid steeds belangrijker als sleutels om informatie te kunnen koppelen en combineren. Het feit dat iDeal gebruikt kan worden voor een dienst van DUO laat zien dat bij het gebruik van identificaties de grenzen tussen de publieke en private sector steeds diffuser worden, hetgeen impliceert dat ook de effecten van dat gebruik over de grenzen heen spelen. Interventie door de overheid kan daarom ook ingegeven zijn door de prijs die de overheid zelf betaalt, bijvoorbeeld via de kosten van opsporing in geval van fraude met identiteiten. Daarnaast heeft de overheid de positie en verantwoordelijkheid om (technologische) onveiligheid aan te pakken. Net zomin als marktpartijen dat kunnen, kan de overheid identiteitssystemen en sleutels voor de volle 100 procent beveiligen, maar heeft wél, en hierin verschilt ze van marktpartijen, de doorzettingsmacht om de afwenteling van onveiligheid te reguleren (De Hert, 2011). De overheid kan, met andere woorden, voorschrijven welke schouders bepaalde risico's moeten dragen. Binnen deze arrangementen kunnen de kosten en baten van de onveiligheid worden afgewogen en verantwoordelijkheden aan de actoren worden toebedeeld. Burgers zijn dan niet langer uitsluitend op zichzelf aangewezen om eventuele problemen die voortkomen uit de onveiligheid van identiteitssystemen op te lossen. Zeker wanneer in de toekomst – voor dit hoofdstuk is dat anno 2020 – de economische en maatschappelijke potentie enorm blijkt te zijn van gegevens die mensen zeer dicht op de huid zitten (biometrie en genetische informatie), is een heldere en daadwerkelijk te handhaven verantwoordelijkheidsverdeling cruciaal voor risico's die met dit gegevensgebruik gemoeid zijn.

5. Slot

Wezenlijk is natuurlijk de vraag of het voor de overheid überhaupt nog wel mogelijk is om vanuit een systeemverantwoordelijkheid grenzen aan turbulente en complexe informatiestromen te stellen. De realiteit anno 2020 rondom systeemverantwoordelijkheid zal veeleer procesverantwoordelijkheid en restverantwoordelijkheid zijn dan een verstrekkende inhoudelijke verantwoordelijkheid. Dat betekent dat de overheid in veel situaties niet zozeer de verantwoordelijkheid neemt voor uitkomsten maar wel voor de kwaliteit van het proces. Vanuit een restverantwoordelijkheid waarborgt de overheid dat ze in sommige situaties taken op zich neemt die door andere partijen niet worden vervuld (zoals in het tweede voorbeeld waarmee we deze bijdrage begonnen). Institutioneel heeft deze ontwikkeling ook betekenis. De anno 2011 door de WRR voorgestelde, en in 2012 ingevoerde, Commissie voor de iOverheid zal namelijk in het denken over de – invulling van – systeemverantwoordelijkheid van de overheid een belangrijke agenderende rol blijken te spelen. Deze commissie (en haar tijdens het Nederlandse EU-voorzitterschap van 2016 ingevoerde Europese evenknie) richt zich op de strategische kernvragen voor de systeemverantwoordelijkheid voor de Nederlandse en Europese iSamenleving. Welke ontwikkelingen in de bredere iSamenleving dienen ondersteund of juist beteugeld te worden en op welk niveau (nationaal of internationaal) kan normerend optreden het beste worden belegd? Van welke ontwikkelingen kan worden verwacht dat de effecten zullen doorsijpelen naar de overheid en wat betekent dat voor eventueel regulerend (conditionerend) optreden? Waar moet en kan de iSamenleving begrensd worden en waar moet de overheid haar eigen grenzen kennen in de informatiesamenleving waarvan zij deel uit maakt? Juist met het agenderen van deze bredere en fundamentele vragen toont de nationale en Europese politiek anno 2020 dat ze digitalisering op een evenwichtige wijze de maat meet.

Literatuur

Buruma, Y., Het recht op vergetelheid. Politie en justitiële gegevens in een digitale wereld, in: *De staat van informatie*, D. Broeders, C. Cuijpers en J.E.J. Prins (samenstellers), WRR verkenning nr.25, Amsterdam University Press, 2011.

Hert, P. de, Systeemverantwoordelijkheid voor de informatiemaatschappij als positieve mensenrechten verplichting, in: *De staat van informatie*, D. Broeders, C. Cuijpers en J.E.J. Prins (samenstellers), WRR verkenning nr.25, Amsterdam University Press, 2011.

Kroes, N., Memo 10/33, date 09/02/2010, te raadplegen op www.europa.eu/rapid/searchAction.do, 2010.

Ministerie van Justitie, *Visie op biometrie in de identiteitsketen publieke sector*, Programma VIPS, juli 2010.

Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid*, WRR Rapporten aan de Regering nr. 86, Amsterdam University Press, 2011.

Corien Prins is lid van de Wetenschappelijke Raad voor het Regeringsbeleid en hoogleraar Recht en Informatisering aan de Universiteit van Tilburg. Zij was voorzitter van de projectgroep die het WRR-rapport *iOverheid* schreef dat op 15 maart 2011 aan het kabinet werd aangeboden (zie www.ioverheid.nu).

Dennis Broeders is senior wetenschappelijk medewerker bij de Wetenschappelijke Raad voor het Regeringsbeleid en als onderzoeker verbonden aan de vakgroep Sociologie van de Erasmus Universiteit Rotterdam. Hij was coördinator van de projectgroep die het WRR-rapport *iOverheid* schreef.

